Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.
# Table of Contents

What is Aurora? ................................................................................................................................. 1  
Aurora DB clusters ............................................................................................................................. 3  
Regions and Availability Zones .......................................................................................................... 5  
AWS Regions ................................................................................................................................. 5  
Availability Zones ............................................................................................................................ 9  
Local time zone for DB clusters ......................................................................................................... 9  
Supported Aurora features by Region and engine ........................................................................... 13  
  Backtracking in Aurora ................................................................................................................. 13  
  Aurora global databases .............................................................................................................. 14  
  Aurora machine learning ............................................................................................................ 16  
  Aurora parallel queries .............................................................................................................. 18  
  Amazon RDS Proxy .................................................................................................................. 19  
  Aurora Serverless v1 .............................................................................................................. 21  
  Data API for Aurora Serverless .............................................................................................. 23  
  Aurora connection management ............................................................................................... 24  
    Types of Aurora endpoints ...................................................................................................... 25  
    Viewing endpoints .................................................................................................................. 27  
    Using the cluster endpoint ...................................................................................................... 27  
    Using the reader endpoint ...................................................................................................... 27  
    Using custom endpoints ......................................................................................................... 28  
    Creating a custom endpoint .................................................................................................... 30  
    Viewing custom endpoints ..................................................................................................... 32  
    Editing a custom endpoint ...................................................................................................... 37  
    Deleting a custom endpoint ................................................................................................... 39  
    End-to-end AWS CLI example for custom endpoints ............................................................. 40  
    Using the instance endpoints ................................................................................................. 44  
    Endpoints and high availability ............................................................................................. 44  
  DB instance classes .................................................................................................................... 46  
    DB instance class types .......................................................................................................... 46  
    Supported DB engines ............................................................................................................ 47  
    Hardware specifications ......................................................................................................... 49  
  Aurora storage and reliability ....................................................................................................... 51  
    Overview of Aurora storage .................................................................................................... 51  
    Cluster volume contents ......................................................................................................... 52  
    How storage resizes .............................................................................................................. 52  
    Data billing ........................................................................................................................... 52  
    Reliability .............................................................................................................................. 53  
  Aurora security ............................................................................................................................ 54  
    Using SSL with Aurora DB clusters ...................................................................................... 55  
  High availability for Amazon Aurora .......................................................................................... 55  
    High availability for Aurora data ............................................................................................ 55  
    High availability for Aurora DB instances ............................................................................. 55  
    High availability across AWS Regions with Aurora global databases .................................. 56  
    Fault tolerance ...................................................................................................................... 56  
  Replication with Aurora ............................................................................................................... 57  
    Aurora Replicas ..................................................................................................................... 57  
    Aurora MySQL ....................................................................................................................... 58  
    Aurora PostgreSQL ................................................................................................................ 58  
  DB instance billing for Aurora ...................................................................................................... 59  
    On-Demand DB instances ...................................................................................................... 60  
    Reserved DB instances .......................................................................................................... 61  
Setting up your environment ............................................................................................................... 73  
Sign up for AWS ............................................................................................................................. 73  
Create an IAM user ........................................................................................................................... 73
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine requirements</td>
<td>75</td>
</tr>
<tr>
<td>Provide access to the DB cluster in the VPC by creating a security group</td>
<td>76</td>
</tr>
<tr>
<td>Getting started</td>
<td>78</td>
</tr>
<tr>
<td>Creating an Aurora MySQL DB cluster and connecting to it</td>
<td>78</td>
</tr>
<tr>
<td>Create an Aurora MySQL DB cluster</td>
<td>78</td>
</tr>
<tr>
<td>Connect to an instance in a DB cluster</td>
<td>85</td>
</tr>
<tr>
<td>Delete the sample DB cluster, DB subnet group, and VPC</td>
<td>87</td>
</tr>
<tr>
<td>Creating an Aurora PostgreSQL DB cluster and connecting to it</td>
<td>87</td>
</tr>
<tr>
<td>Create an Aurora PostgreSQL DB cluster</td>
<td>88</td>
</tr>
<tr>
<td>Connect to an instance in an Aurora PostgreSQL DB cluster</td>
<td>96</td>
</tr>
<tr>
<td>Delete the sample DB cluster, DB subnet group, and VPC</td>
<td>97</td>
</tr>
<tr>
<td>Tutorial: Create a web server and an Amazon Aurora DB cluster</td>
<td>99</td>
</tr>
<tr>
<td>Create a DB cluster</td>
<td>100</td>
</tr>
<tr>
<td>Create a web server</td>
<td>105</td>
</tr>
<tr>
<td>Configuring your Aurora DB cluster</td>
<td>117</td>
</tr>
<tr>
<td>Creating a DB cluster</td>
<td>118</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>118</td>
</tr>
<tr>
<td>Creating a DB cluster</td>
<td>119</td>
</tr>
<tr>
<td>Available settings</td>
<td>128</td>
</tr>
<tr>
<td>Using Aurora Serverless v1</td>
<td>134</td>
</tr>
<tr>
<td>Advantages of Aurora Serverless v1</td>
<td>134</td>
</tr>
<tr>
<td>Use cases for Aurora Serverless v1</td>
<td>135</td>
</tr>
<tr>
<td>Limitations of Aurora Serverless v1</td>
<td>135</td>
</tr>
<tr>
<td>Configuration requirements for Aurora Serverless v1</td>
<td>136</td>
</tr>
<tr>
<td>Using TLS/SSL with Aurora Serverless v1</td>
<td>137</td>
</tr>
<tr>
<td>How Aurora Serverless v1 works</td>
<td>138</td>
</tr>
<tr>
<td>Creating an Aurora Serverless v1 DB cluster</td>
<td>145</td>
</tr>
<tr>
<td>Restoring an Aurora Serverless v1 DB cluster</td>
<td>150</td>
</tr>
<tr>
<td>Modifying an Aurora Serverless v1 DB cluster</td>
<td>154</td>
</tr>
<tr>
<td>Scaling Aurora Serverless v1 DB cluster capacity manually</td>
<td>156</td>
</tr>
<tr>
<td>Viewing Aurora Serverless v1 DB clusters</td>
<td>158</td>
</tr>
<tr>
<td>Deleting an Aurora Serverless v1 DB cluster</td>
<td>159</td>
</tr>
<tr>
<td>Aurora Serverless v1 and Aurora database engine versions</td>
<td>161</td>
</tr>
<tr>
<td>Using the Data API</td>
<td>162</td>
</tr>
<tr>
<td>Logging Data API calls with AWS CloudTrail</td>
<td>186</td>
</tr>
<tr>
<td>Using the query editor</td>
<td>188</td>
</tr>
<tr>
<td>Using Aurora Serverless v2 (preview)</td>
<td>193</td>
</tr>
<tr>
<td>How Aurora Serverless v2 (preview) works</td>
<td>193</td>
</tr>
<tr>
<td>Limitations of Aurora Serverless v2 (preview)</td>
<td>196</td>
</tr>
<tr>
<td>Creating an Aurora Serverless v2 (preview) DB cluster</td>
<td>197</td>
</tr>
<tr>
<td>Creating a snapshot of an Aurora Serverless v2 (preview) DB cluster</td>
<td>200</td>
</tr>
<tr>
<td>Modifying an Aurora Serverless v2 (preview) DB cluster</td>
<td>201</td>
</tr>
<tr>
<td>Deleting an Aurora Serverless v2 (preview) DB cluster</td>
<td>203</td>
</tr>
<tr>
<td>Restoring an Aurora Serverless v2 (preview) DB cluster</td>
<td>204</td>
</tr>
<tr>
<td>Using Aurora global databases</td>
<td>206</td>
</tr>
<tr>
<td>Overview of Aurora global databases</td>
<td>206</td>
</tr>
<tr>
<td>Advantages of Amazon Aurora global databases</td>
<td>207</td>
</tr>
<tr>
<td>Limitations of Aurora global databases</td>
<td>207</td>
</tr>
<tr>
<td>Getting started with Aurora global databases</td>
<td>208</td>
</tr>
<tr>
<td>Managing an Aurora global database</td>
<td>227</td>
</tr>
<tr>
<td>Connecting to an Aurora global database</td>
<td>232</td>
</tr>
<tr>
<td>Using write forwarding in an Aurora global database</td>
<td>233</td>
</tr>
<tr>
<td>Disaster recovery for Aurora global databases</td>
<td>244</td>
</tr>
<tr>
<td>Monitoring an Aurora global database</td>
<td>248</td>
</tr>
<tr>
<td>Using Aurora global databases with other AWS services</td>
<td>251</td>
</tr>
<tr>
<td>Connecting to a DB cluster</td>
<td>253</td>
</tr>
<tr>
<td>Connecting to Aurora MySQL</td>
<td>253</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Adjusting the maintenance window for a DB cluster</td>
<td>393</td>
</tr>
<tr>
<td>Automatic minor version upgrades for Aurora DB clusters</td>
<td>394</td>
</tr>
<tr>
<td>Choosing the frequency of Aurora MySQL maintenance updates</td>
<td>395</td>
</tr>
<tr>
<td>Rebooting a DB instance</td>
<td>396</td>
</tr>
<tr>
<td>Deleting a DB cluster or DB instance</td>
<td>398</td>
</tr>
<tr>
<td>Deletion protection</td>
<td>398</td>
</tr>
<tr>
<td>Aurora clusters with a single DB instance</td>
<td>398</td>
</tr>
<tr>
<td>Deleting an empty Aurora cluster</td>
<td>398</td>
</tr>
<tr>
<td>Aurora MySQL clusters that are read replicas</td>
<td>399</td>
</tr>
<tr>
<td>Deleting a DB instance</td>
<td>399</td>
</tr>
<tr>
<td>Tagging RDS resources</td>
<td>401</td>
</tr>
<tr>
<td>Overview</td>
<td>401</td>
</tr>
<tr>
<td>Working with ARNs</td>
<td>406</td>
</tr>
<tr>
<td>Constructing an ARN</td>
<td>406</td>
</tr>
<tr>
<td>Getting an existing ARN</td>
<td>409</td>
</tr>
<tr>
<td>Aurora updates</td>
<td>413</td>
</tr>
<tr>
<td>Identifying your Amazon Aurora version</td>
<td>413</td>
</tr>
<tr>
<td>Backing up and restoring an Aurora DB cluster</td>
<td>414</td>
</tr>
<tr>
<td>Overview of backing up and restoring</td>
<td>415</td>
</tr>
<tr>
<td>Backups</td>
<td>415</td>
</tr>
<tr>
<td>Restoring data</td>
<td>415</td>
</tr>
<tr>
<td>Backtrack</td>
<td>416</td>
</tr>
<tr>
<td>Backup storage</td>
<td>417</td>
</tr>
<tr>
<td>Creating a DB cluster snapshot</td>
<td>418</td>
</tr>
<tr>
<td>Determining whether the snapshot is available</td>
<td>419</td>
</tr>
<tr>
<td>Restoring from a DB cluster snapshot</td>
<td>420</td>
</tr>
<tr>
<td>Parameter groups</td>
<td>420</td>
</tr>
<tr>
<td>Security groups</td>
<td>420</td>
</tr>
<tr>
<td>Aurora considerations</td>
<td>420</td>
</tr>
<tr>
<td>Restoring from a snapshot</td>
<td>421</td>
</tr>
<tr>
<td>Copying a snapshot</td>
<td>423</td>
</tr>
<tr>
<td>Limitations</td>
<td>423</td>
</tr>
<tr>
<td>Snapshot retention</td>
<td>423</td>
</tr>
<tr>
<td>Shared snapshots</td>
<td>423</td>
</tr>
<tr>
<td>Encryption</td>
<td>424</td>
</tr>
<tr>
<td>Copying snapshots across AWS Regions</td>
<td>424</td>
</tr>
<tr>
<td>Parameter groups</td>
<td>424</td>
</tr>
<tr>
<td>Copying a DB cluster snapshot</td>
<td>424</td>
</tr>
<tr>
<td>Sharing a snapshot</td>
<td>433</td>
</tr>
<tr>
<td>Sharing an encrypted snapshot</td>
<td>433</td>
</tr>
<tr>
<td>Sharing a snapshot</td>
<td>435</td>
</tr>
<tr>
<td>Exporting snapshot data to Amazon S3</td>
<td>439</td>
</tr>
<tr>
<td>Overview of exporting snapshot data</td>
<td>440</td>
</tr>
<tr>
<td>Setting up access to an S3 bucket</td>
<td>440</td>
</tr>
<tr>
<td>Exporting a snapshot to an S3 bucket</td>
<td>442</td>
</tr>
<tr>
<td>Monitoring snapshot exports</td>
<td>444</td>
</tr>
<tr>
<td>Canceling a snapshot export</td>
<td>446</td>
</tr>
<tr>
<td>Troubleshooting PostgreSQL permissions errors</td>
<td>447</td>
</tr>
<tr>
<td>Data conversion</td>
<td></td>
</tr>
<tr>
<td>Point-in-time recovery</td>
<td>454</td>
</tr>
<tr>
<td>Deleting a snapshot</td>
<td>457</td>
</tr>
<tr>
<td>Deleting a DB cluster snapshot</td>
<td>457</td>
</tr>
<tr>
<td>Monitoring an Aurora DB cluster</td>
<td>459</td>
</tr>
<tr>
<td>Overview of monitoring</td>
<td>460</td>
</tr>
<tr>
<td>Monitoring plan</td>
<td>460</td>
</tr>
<tr>
<td>Performance baseline</td>
<td>460</td>
</tr>
<tr>
<td>Performance guidelines</td>
<td>460</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Identify your objectives</td>
</tr>
<tr>
<td>2</td>
<td>Understand your workload characteristics</td>
</tr>
<tr>
<td>3</td>
<td>Practice with the console or CLI</td>
</tr>
<tr>
<td>4</td>
<td>Create your Aurora cluster</td>
</tr>
<tr>
<td>5</td>
<td>Set up your schema</td>
</tr>
<tr>
<td>6</td>
<td>Import your data</td>
</tr>
<tr>
<td>7</td>
<td>Port your SQL code</td>
</tr>
<tr>
<td>8</td>
<td>Specify configuration settings</td>
</tr>
<tr>
<td>9</td>
<td>Connect to Aurora</td>
</tr>
<tr>
<td>10</td>
<td>Run your workload</td>
</tr>
<tr>
<td>11</td>
<td>Measure performance</td>
</tr>
<tr>
<td>12</td>
<td>Exercise Aurora high availability</td>
</tr>
<tr>
<td>13</td>
<td>What to do next</td>
</tr>
<tr>
<td>14</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>15</td>
<td>Overview of an Aurora proof of concept</td>
</tr>
<tr>
<td>16</td>
<td>Best practices with Aurora</td>
</tr>
<tr>
<td></td>
<td>Basic operational guidelines for Amazon Aurora</td>
</tr>
<tr>
<td></td>
<td>DB instance RAM recommendations</td>
</tr>
<tr>
<td></td>
<td>Monitoring Amazon Aurora</td>
</tr>
<tr>
<td></td>
<td>Working with DB parameter groups and DB cluster parameter groups</td>
</tr>
<tr>
<td></td>
<td>Amazon Aurora best practices presentation video</td>
</tr>
<tr>
<td>17</td>
<td>Working with DB parameter groups and DB cluster parameter groups</td>
</tr>
<tr>
<td>18</td>
<td>Using Kerberos authentication</td>
</tr>
<tr>
<td></td>
<td>Overview of Kerberos authentication</td>
</tr>
<tr>
<td></td>
<td>Setting up</td>
</tr>
<tr>
<td></td>
<td>Managing a DB cluster in a Domain</td>
</tr>
<tr>
<td></td>
<td>Connecting with Kerberos authentication</td>
</tr>
<tr>
<td>19</td>
<td>Aurora PostgreSQL reference</td>
</tr>
<tr>
<td></td>
<td>Aurora PostgreSQL parameters</td>
</tr>
<tr>
<td></td>
<td>Aurora PostgreSQL events</td>
</tr>
<tr>
<td>20</td>
<td>Aurora PostgreSQL updates</td>
</tr>
<tr>
<td></td>
<td>Identifying your version</td>
</tr>
<tr>
<td></td>
<td>Engine versions for Aurora PostgreSQL</td>
</tr>
<tr>
<td></td>
<td>Extensions and modules for Aurora PostgreSQL</td>
</tr>
<tr>
<td>21</td>
<td>Best practices with Aurora</td>
</tr>
<tr>
<td></td>
<td>IAM database authentication</td>
</tr>
<tr>
<td></td>
<td>Password authentication</td>
</tr>
<tr>
<td></td>
<td>Kerberos authentication</td>
</tr>
<tr>
<td>22</td>
<td>Data protection</td>
</tr>
<tr>
<td></td>
<td>Data encryption</td>
</tr>
<tr>
<td></td>
<td>Internetwork traffic privacy</td>
</tr>
<tr>
<td>23</td>
<td>Identity and access management</td>
</tr>
<tr>
<td></td>
<td>Audience</td>
</tr>
<tr>
<td></td>
<td>Authenticating with identities</td>
</tr>
<tr>
<td></td>
<td>Managing access using policies</td>
</tr>
<tr>
<td></td>
<td>How Amazon Aurora works with IAM</td>
</tr>
<tr>
<td></td>
<td>Identity-based policy examples</td>
</tr>
<tr>
<td></td>
<td>IAM database authentication</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>24</td>
<td>Logging and monitoring</td>
</tr>
<tr>
<td>25</td>
<td>Compliance validation</td>
</tr>
</tbody>
</table>
Resilience ........................................................................................................................................ 1268
  Backup and restore ..................................................................................................................... 1268
  Replication ................................................................................................................................. 1268
  Failover ...................................................................................................................................... 1268
Infrastructure security .................................................................................................................. 1270
  Security groups ......................................................................................................................... 1270
  Public accessibility ...................................................................................................................... 1270
VPC endpoints (AWS PrivateLink) ............................................................................................ 1271
  Considerations .......................................................................................................................... 1271
  Availability ................................................................................................................................ 1271
  Creating an interface VPC endpoint .......................................................................................... 1272
  Creating a VPC endpoint policy ................................................................................................. 1272
Security best practices .................................................................................................................. 1273
Controlling access with security groups .................................................................................... 1274
  VPC security groups .................................................................................................................. 1274
  Security group scenario ............................................................................................................. 1274
  Creating a VPC security group ................................................................................................... 1275
  Associating with a DB instance ................................................................................................. 1275
  Associating with a DB cluster .................................................................................................... 1275
Master user account privileges .................................................................................................. 1276
Service-linked roles ..................................................................................................................... 1277
  Service-linked role permissions for Amazon Aurora ............................................................... 1277
  Creating a service-linked role for Amazon Aurora ................................................................. 1279
  Editing a service-linked role for Amazon Aurora ....................................................................... 1279
  Deleting a service-linked role for Amazon Aurora ................................................................. 1279
Using Amazon Aurora with Amazon VPC .................................................................................. 1281
  Creating a VPC for Aurora ....................................................................................................... 1281
  Scenarios for accessing a DB instance in a VPC ......................................................................... 1288
  Working with a DB instance in a VPC ...................................................................................... 1291
  Tutorial: Create an Amazon VPC for use with a DB instance .................................................. 1298
Quotas and constraints .................................................................................................................. 1303
  Quotas in Amazon Aurora ......................................................................................................... 1303
  Naming constraints in Amazon Aurora .................................................................................... 1304
  Amazon Aurora table size limits ............................................................................................... 1305
Troubleshooting ............................................................................................................................ 1306
  Can't connect to DB instance .................................................................................................... 1306
  Testing the DB instance connection .......................................................................................... 1307
  Troubleshooting connection authentication .............................................................................. 1308
Security issues ............................................................................................................................... 1308
  Error message "failed to retrieve account attributes, certain console functions may be impaired." .......................................................................................................................... 1308
  Resetting the DB instance owner password ............................................................................. 1308
  DB instance outage or reboot ..................................................................................................... 1308
  Parameter changes not taking effect ......................................................................................... 1309
  Aurora MySQL out of memory issues ....................................................................................... 1309
  Aurora MySQL replication issues ............................................................................................. 1310
  Diagnosing and resolving lag between read replicas ............................................................... 1310
  Diagnosing and resolving a MySQL read replication failure .................................................... 1311
  Replication stopped error .......................................................................................................... 1312
  No space left on device .............................................................................................................. 1312
Amazon RDS API reference .......................................................................................................... 1314
  Using the Query API .................................................................................................................. 1314
  Query parameters ..................................................................................................................... 1314
  Query request authentication ................................................................................................. 1314
Troubleshooting applications ....................................................................................................... 1315
  Retrieving errors ....................................................................................................................... 1315
  Troubleshooting tips .................................................................................................................. 1315
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document history</td>
<td>1316</td>
</tr>
<tr>
<td>AWS glossary</td>
<td>1345</td>
</tr>
</tbody>
</table>
What is Amazon Aurora?

Amazon Aurora (Aurora) is a fully managed relational database engine that’s compatible with MySQL and PostgreSQL. You already know how MySQL and PostgreSQL combine the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. The code, tools, and applications you use today with your existing MySQL and PostgreSQL databases can be used with Aurora. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

Aurora includes a high-performance storage subsystem. Its MySQL- and PostgreSQL-compatible database engines are customized to take advantage of that fast distributed storage. The underlying storage grows automatically as needed. An Aurora cluster volume can grow to a maximum size of 128 tebibytes (TiB). Aurora also automates and standardizes database clustering and replication, which are typically among the most challenging aspects of database configuration and administration.

Aurora is part of the managed database service Amazon Relational Database Service (Amazon RDS). Amazon RDS is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. If you are not already familiar with Amazon RDS, see the Amazon Relational Database Service User Guide.

The following points illustrate how Aurora relates to the standard MySQL and PostgreSQL engines available in Amazon RDS:

- You choose Aurora as a DB engine option when setting up new database servers through Amazon RDS.
- Aurora takes advantage of the familiar Amazon Relational Database Service (Amazon RDS) features for management and administration. Aurora uses the Amazon RDS AWS Management Console interface, AWS CLI commands, and API operations to handle routine database tasks such as provisioning, patching, backup, recovery, failure detection, and repair.
- Aurora management operations typically involve entire clusters of database servers that are synchronized through replication, instead of individual database instances. The automatic clustering, replication, and storage allocation make it simple and cost-effective to set up, operate, and scale your largest MySQL and PostgreSQL deployments.
- You can bring data from Amazon RDS for MySQL and Amazon RDS for PostgreSQL into Aurora by creating and restoring snapshots, or by setting up one-way replication. You can use push-button migration tools to convert your existing Amazon RDS for MySQL and Amazon RDS for PostgreSQL applications to Aurora.

Before using Amazon Aurora, you should complete the steps in Setting up your environment for Amazon Aurora (p. 73), and then review the concepts and features of Aurora in Amazon Aurora DB clusters (p. 3).

Topics

- Amazon Aurora DB clusters (p. 3)
- Regions and Availability Zones (p. 5)
- Supported features in Amazon Aurora by AWS Region and Aurora DB engine (p. 13)
- Amazon Aurora connection management (p. 24)
- DB instance classes (p. 46)
- Amazon Aurora storage and reliability (p. 51)
- Amazon Aurora security (p. 54)
- High availability for Amazon Aurora (p. 55)
• Replication with Amazon Aurora (p. 57)
• DB instance billing for Aurora (p. 59)
Amazon Aurora DB clusters

An Amazon Aurora DB cluster consists of one or more DB instances and a cluster volume that manages the data for those DB instances. An Aurora cluster volume is a virtual database storage volume that spans multiple Availability Zones, with each Availability Zone having a copy of the DB cluster data. Two types of DB instances make up an Aurora DB cluster:

- **Primary DB instance** – Supports read and write operations, and performs all of the data modifications to the cluster volume. Each Aurora DB cluster has one primary DB instance.
- **Aurora Replica** – Connects to the same storage volume as the primary DB instance and supports only read operations. Each Aurora DB cluster can have up to 15 Aurora Replicas in addition to the primary DB instance. Maintain high availability by locating Aurora Replicas in separate Availability Zones. Aurora automatically fails over to an Aurora Replica in case the primary DB instance becomes unavailable. You can specify the failover priority for Aurora Replicas. Aurora Replicas can also offload read workloads from the primary DB instance.
- For Aurora multi-master clusters, all DB instances have read/write capability. In this case, the distinction between primary instance and Aurora Replica doesn’t apply. For discussing replication topology where the clusters can use either single-master or multi-master replication, we call these writer and reader DB instances.

The following diagram illustrates the relationship between the cluster volume, the primary DB instance, and Aurora Replicas in an Aurora DB cluster.

**Note**
The preceding information applies to all the Aurora clusters that use single-master replication. These include provisioned clusters, parallel query clusters, global database clusters, serverless clusters, and all MySQL 5.7-compatible and PostgreSQL-compatible clusters. Aurora clusters that use multi-master replication have a different arrangement of read/write and read-only DB instances. All DB instances in a multi-master cluster can perform write operations. There isn't a single DB instance that performs all the write operations, and there aren’t any read-only DB instances. Therefore, the terms primary instance and Aurora Replica...
don't apply to multi-master clusters. When we discuss clusters that might use multi-master replication, we refer to *writer* DB instances and *reader* DB instances.

The Aurora cluster illustrates the separation of compute capacity and storage. For example, an Aurora configuration with only a single DB instance is still a cluster, because the underlying storage volume involves multiple storage nodes distributed across multiple Availability Zones (AZs).
Regions and Availability Zones

Amazon cloud computing resources are hosted in multiple locations world-wide. These locations are composed of AWS Regions and Availability Zones. Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones.

**Note**
For information about finding the Availability Zones for an AWS Region, see Describing your Regions, Availability Zones, and Local Zones in the Amazon EC2 documentation.

Amazon operates state-of-the-art, highly-available data centers. Although rare, failures can occur that affect the availability of instances that are in the same location. If you host all your instances in a single location that is affected by such a failure, none of your instances is available.

It is important to remember that each AWS Region is completely independent. Any Amazon RDS activity you initiate (for example, creating database instances or listing available database instances) runs only in your current default AWS Region. The default AWS Region can be changed in the console, by setting the `AWS_DEFAULT_REGION` environment variable, or it can be overridden by using the `--region` parameter with the AWS Command Line Interface (AWS CLI). For more information, see Configuring the AWS Command Line Interface, specifically the sections about environment variables and command line options.

Amazon RDS supports special AWS Regions called AWS GovCloud (US) that are designed to allow US government agencies and customers to move more sensitive workloads into the cloud. The AWS GovCloud (US) Regions address the US government's specific regulatory and compliance requirements. For more information, see What is AWS GovCloud (US)?

To create or work with an Amazon RDS DB instance in a specific AWS Region, use the corresponding regional service endpoint.

**Note**
Aurora doesn't support Local Zones.

**AWS Regions**

Each AWS Region is designed to be isolated from the other AWS Regions. This design achieves the greatest possible fault tolerance and stability.

When you view your resources, you see only the resources that are tied to the AWS Region that you specified. This is because AWS Regions are isolated from each other, and we don't automatically replicate resources across AWS Regions.
Region availability

**Note**
Aurora MySQL version 5.7 and Aurora PostgreSQL version 10.7 don’t have time zone data that reflect recent changes to Daylight Saving Time (DST) in Brazil. For a workaround until updated versions are available, reset the DB cluster’s time zone parameter if the expected time doesn’t show correctly for the recently changed Brazil time zone. Do the following:

- South America (Sao Paulo) Region – set the time zone to America/Fortaleza.
- South America (Cuiaba) Region – set the time zone to America/Manaus.

To change the time zone, see Modifying parameters in a DB parameter group (p. 303).

When you work with an Aurora DB cluster using the command line interface or API operations, make sure that you specify its regional endpoint.

**Topics**
- Aurora MySQL Region availability (p. 6)
- Aurora PostgreSQL Region availability (p. 8)

### Aurora MySQL Region availability

The following table shows the AWS Regions where Aurora MySQL is currently available and the endpoint for each Region.

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (Ohio)</td>
<td>us-east-2</td>
<td>rds.us-east-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>rds.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>us-west-1</td>
<td>rds.us-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>rds.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
<td>rds.af-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>ap-east-1</td>
<td>rds.ap-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1</td>
<td>rds.ap-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>rds.ap-northeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Region Name</td>
<td>Region</td>
<td>Endpoint</td>
<td>Protocol</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>rds.ap-southeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>rds.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>rds.ap-northeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>rds.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>cn-north-1</td>
<td>rds.cn-north-1.amazonaws.com.cn</td>
<td>HTTPS</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>cn-northwest-1</td>
<td>rds.cn-northwest-1.amazonaws.com.cn</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>rds.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>eu-west-1</td>
<td>rds.eu-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>rds.eu-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>eu-south-1</td>
<td>rds.eu-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>eu-west-3</td>
<td>rds.eu-west-3.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>eu-north-1</td>
<td>rds.eu-north-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td>me-south-1</td>
<td>rds.me-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>sa-east-1</td>
<td>rds.sa-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS GovCloud (US-East)</td>
<td>us-gov-east-1</td>
<td>rds.us-gov-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>us-gov-west-1</td>
<td>rds.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
## Aurora PostgreSQL Region availability

The following table shows the AWS Regions where Aurora PostgreSQL is currently available and the endpoint for each Region.

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (Ohio)</td>
<td>us-east-2</td>
<td>rds.us-east-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>rds.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>us-west-1</td>
<td>rds.us-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>rds.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
<td>rds.af-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>ap-east-1</td>
<td>rds.ap-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1</td>
<td>rds.ap-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>rds.ap-northeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>rds.ap-southeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>rds.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>rds.ap-northeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>rds.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>cn-north-1</td>
<td>rds.cn-north-1.amazonaws.com.cn</td>
<td>HTTPS</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>cn-northwest-1</td>
<td>rds.cn-northwest-1.amazonaws.com.cn</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
### Availability Zones

When you create a DB instance, you can choose an Availability Zone or have AWS choose one for you. An Availability Zone is represented by an AWS Region code followed by a letter identifier (for example, us-east-1a).

### Local time zone for Amazon Aurora DB clusters

By default, the time zone for an Amazon Aurora DB cluster is Universal Time Coordinated (UTC). You can set the time zone for instances in your DB cluster to the local time zone for your application instead.

To set the local time zone for a DB cluster, set the `time_zone` parameter in the cluster parameter group for your DB cluster to one of the supported values listed later in this section. When you set the `time_zone` parameter for a DB cluster, all instances in the DB cluster change to use the new local time zone. If other Aurora DB clusters are using the same cluster parameter group, then all instances in those DB clusters change to use the new local time zone also. For information on cluster-level parameters, see Amazon Aurora DB cluster and DB instance parameters (p. 300).

---

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>rds.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>eu-west-1</td>
<td>rds.eu-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>rds.eu-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>eu-south-1</td>
<td>rds.eu-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>eu-west-3</td>
<td>rds.eu-west-3.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>eu-north-1</td>
<td>rds.eu-north-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td>me-south-1</td>
<td>rds.me-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>sa-east-1</td>
<td>rds.sa-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS GovCloud (US-East)</td>
<td>us-gov-east-1</td>
<td>rds.us-gov-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>us-gov-west-1</td>
<td>rds.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
After you set the local time zone, all new connections to the database reflect the change. If you have any open connections to your database when you change the local time zone, you won't see the local time zone update until after you close the connection and open a new connection.

If you are replicating across AWS Regions, then the replication master DB cluster and the replica use different parameter groups (parameter groups are unique to an AWS Region). To use the same local time zone for each instance, you must set the `time_zone` parameter in the parameter groups for both the replication master and the replica.

When you restore a DB cluster from a DB cluster snapshot, the local time zone is set to UTC. You can update the time zone to your local time zone after the restore is complete. If you restore a DB cluster to a point in time, then the local time zone for the restored DB cluster is the time zone setting from the parameter group of the restored DB cluster.

You can set your local time zone to one of the values listed in the following table. For some time zones, time values for certain date ranges can be reported incorrectly as noted in the table. For Australia time zones, the time zone abbreviation returned is an outdated value as noted in the table.

<table>
<thead>
<tr>
<th>Time zone</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa/Harare</td>
<td>This time zone setting can return incorrect values from 28 Feb 1903 21:49:40 GMT to 28 Feb 1903 21:55:48 GMT.</td>
</tr>
<tr>
<td>Africa/Monrovia</td>
<td></td>
</tr>
<tr>
<td>Africa/Nairobi</td>
<td>This time zone setting can return incorrect values from 31 Dec 1939 21:30:00 GMT to 31 Dec 1959 21:15:15 GMT.</td>
</tr>
<tr>
<td>Africa/Windhoek</td>
<td></td>
</tr>
<tr>
<td>America/Bogota</td>
<td>This time zone setting can return incorrect values from 23 Nov 1914 04:56:16 GMT to 23 Nov 1914 04:56:20 GMT.</td>
</tr>
<tr>
<td>America/Caracas</td>
<td></td>
</tr>
<tr>
<td>America/Chihuahua</td>
<td></td>
</tr>
<tr>
<td>America/Cuiaba</td>
<td></td>
</tr>
<tr>
<td>America/Denver</td>
<td></td>
</tr>
<tr>
<td>America/Fortaleza</td>
<td>If your DB cluster is in the South America (Sao Paulo) Region and the expected time doesn't show correctly for the recently changed Brazil time zone, reset the DB cluster's time zone parameter to America/Fortaleza.</td>
</tr>
<tr>
<td>America/Guatemala</td>
<td></td>
</tr>
<tr>
<td>America/Halifax</td>
<td>This time zone setting can return incorrect values from 27 Oct 1918 05:00:00 GMT to 31 Oct 1918 05:00:00 GMT.</td>
</tr>
<tr>
<td>America/Manaus</td>
<td>If your DB cluster is in the South America (Cuiaba) Region and the expected time doesn't show correctly for the recently changed Brazil time zone, reset the DB cluster's time zone parameter to America/Manaus.</td>
</tr>
<tr>
<td>America/Matamoros</td>
<td></td>
</tr>
<tr>
<td>America/Monterrey</td>
<td></td>
</tr>
<tr>
<td>America/Montevideo</td>
<td></td>
</tr>
<tr>
<td>America/Phoenix</td>
<td></td>
</tr>
<tr>
<td>Time zone</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>America/Tijuana</td>
<td></td>
</tr>
<tr>
<td>Asia/Ashgabat</td>
<td></td>
</tr>
<tr>
<td>Asia/Baghdad</td>
<td></td>
</tr>
<tr>
<td>Asia/Baku</td>
<td></td>
</tr>
<tr>
<td>Asia/Bangkok</td>
<td></td>
</tr>
<tr>
<td>Asia/Beirut</td>
<td></td>
</tr>
<tr>
<td>Asia/Calcutta</td>
<td></td>
</tr>
<tr>
<td>Asia/Kabul</td>
<td></td>
</tr>
<tr>
<td>Asia/Karachi</td>
<td></td>
</tr>
<tr>
<td>Asia/Kathmandu</td>
<td></td>
</tr>
<tr>
<td>Asia/Muscat</td>
<td>This time zone setting can return incorrect values from 31 Dec 1919 20:05:36 GMT to 31 Dec 1919 20:05:40 GMT.</td>
</tr>
<tr>
<td>Asia/Riyadh</td>
<td>This time zone setting can return incorrect values from 13 Mar 1947 20:53:08 GMT to 31 Dec 1949 20:53:08 GMT.</td>
</tr>
<tr>
<td>Asia/Seoul</td>
<td>This time zone setting can return incorrect values from 30 Nov 1904 15:30:00 GMT to 07 Sep 1945 15:00:00 GMT.</td>
</tr>
<tr>
<td>Asia/Shanghai</td>
<td>This time zone setting can return incorrect values from 31 Dec 1927 15:54:08 GMT to 02 Jun 1940 16:00:00 GMT.</td>
</tr>
<tr>
<td>Asia/Singapore</td>
<td></td>
</tr>
<tr>
<td>Asia/Taipei</td>
<td>This time zone setting can return incorrect values from 30 Sep 1937 16:00:00 GMT to 29 Sep 1979 15:00:00 GMT.</td>
</tr>
<tr>
<td>Asia/Tehran</td>
<td></td>
</tr>
<tr>
<td>Asia/Tokyo</td>
<td>This time zone setting can return incorrect values from 30 Sep 1937 15:00:00 GMT to 31 Dec 1937 15:00:00 GMT.</td>
</tr>
<tr>
<td>Asia/Ulaanbaatar</td>
<td></td>
</tr>
<tr>
<td>Atlantic/Azores</td>
<td>This time zone setting can return incorrect values from 24 May 1911 01:54:32 GMT to 01 Jan 1912 01:54:32 GMT.</td>
</tr>
<tr>
<td>Australia/Adelaide</td>
<td>The abbreviation for this time zone is returned as CST instead of ACDT/ACST.</td>
</tr>
<tr>
<td>Australia/Brisbane</td>
<td>The abbreviation for this time zone is returned as EST instead of AEDT/AEST.</td>
</tr>
<tr>
<td>Australia/Darwin</td>
<td>The abbreviation for this time zone is returned as CST instead of ACDT/ACST.</td>
</tr>
<tr>
<td>Australia/Hobart</td>
<td>The abbreviation for this time zone is returned as EST instead of AEDT/AEST.</td>
</tr>
<tr>
<td>Australia/Perth</td>
<td>The abbreviation for this time zone is returned as WST instead of AWDT/AWST.</td>
</tr>
<tr>
<td>Australia/Sydney</td>
<td>The abbreviation for this time zone is returned as EST instead of AEDT/AEST.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Brazil/East</td>
<td></td>
</tr>
<tr>
<td>Canada/Saskatchewan</td>
<td>This time zone setting can return incorrect values from 27 Oct 1918 08:00:00 GMT to 31 Oct 1918 08:00:00 GMT.</td>
</tr>
<tr>
<td>Europe/Amsterdam</td>
<td></td>
</tr>
<tr>
<td>Europe/Athens</td>
<td></td>
</tr>
<tr>
<td>Europe/Dublin</td>
<td></td>
</tr>
<tr>
<td>Europe/Helsinki</td>
<td>This time zone setting can return incorrect values from 30 Apr 1921 22:20:08 GMT to 30 Apr 1921 22:20:11 GMT.</td>
</tr>
<tr>
<td>Europe/Paris</td>
<td></td>
</tr>
<tr>
<td>Europe/Prague</td>
<td></td>
</tr>
<tr>
<td>Europe/Sarajevo</td>
<td></td>
</tr>
<tr>
<td>Pacific/Auckland</td>
<td></td>
</tr>
<tr>
<td>Pacific/Guam</td>
<td></td>
</tr>
<tr>
<td>Pacific/Honolulu</td>
<td>This time zone setting can return incorrect values from 21 May 1933 11:30:00 GMT to 30 Sep 1945 11:30:00 GMT.</td>
</tr>
<tr>
<td>Pacific/Samoa</td>
<td>This time zone setting can return incorrect values from 01 Jan 1911 11:22:48 GMT to 01 Jan 1950 11:30:00 GMT.</td>
</tr>
<tr>
<td>US/Alaska</td>
<td></td>
</tr>
<tr>
<td>US/Central</td>
<td></td>
</tr>
<tr>
<td>US/East</td>
<td></td>
</tr>
<tr>
<td>US/East-Indiana</td>
<td></td>
</tr>
<tr>
<td>US/Pacific</td>
<td></td>
</tr>
<tr>
<td>UTC</td>
<td></td>
</tr>
</tbody>
</table>
Supported features in Amazon Aurora by AWS Region and Aurora DB engine

Aurora MySQL- and PostgreSQL-compatible database engines support several Amazon Aurora and Amazon RDS features and options. The support varies across specific versions of each database engine, and across AWS Regions. You can use the tables in this section to identify Aurora database engine version support and availability in a given AWS Region for the following features:

- Backtracking in Aurora (p. 13)
- Aurora global databases (p. 14)
- Aurora machine learning (p. 16)
- Aurora parallel queries (p. 18)
- Amazon RDS Proxy (p. 19)
- Aurora Serverless v1 (p. 21)
- Data API for Aurora Serverless (p. 23)

Some of these features are Aurora-only capabilities. For example, Aurora Serverless, Aurora global databases, and support for integration with AWS machine learning services aren't supported by Amazon RDS. Other features, such as Amazon RDS Proxy, are supported by both Amazon Aurora and Amazon RDS.

The tables use the following patterns to specify version numbers and level of support:

- **Version x.y** – The specific version alone is supported.
- **Version x.y and later** – The version and all minor versions are also supported. For example, "version 10.11 and later" means that versions 10.11, 10.11.1, and 10.12 are also supported.
- **-** – The feature is not currently available for that particular Aurora feature for the given Aurora database engine, or in that specific AWS Region.

### Backtracking in Aurora

By using backtracking in Aurora, you return the state of an Aurora cluster to a specific point in time, without restoring data from a backup. Backtrack enables you to move your database to a prior point in time without the need to restore from a backup. It completes within seconds, even for large databases. For more information, see Backtracking an Aurora DB cluster (p. 677).

Aurora backtracking is available for Aurora MySQL only. It's not available for Aurora PostgreSQL.

<table>
<thead>
<tr>
<th>Region</th>
<th>Aurora MySQL 5.6</th>
<th>Aurora MySQL 5.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (Ohio)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Aurora global databases

An **Aurora global database** is a single database that spans multiple AWS Regions, enabling low-latency global reads and disaster recovery from any Region-wide outage. It provides built-in fault tolerance for your deployment because the DB instance relies not on a single AWS Region, but upon multiple Regions and different Availability Zones.

Support for this feature varies by Aurora database engine and version. The following table shows the Regions and Aurora database versions that support this feature. For more information, see Using Amazon Aurora global databases (p. 206).

<table>
<thead>
<tr>
<th>Region</th>
<th>Aurora MySQL 5.6</th>
<th>Aurora MySQL 5.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>Version 5.6.10a</td>
<td>Version 2.06 and later</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>AWS GovCloud (US-East)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Region</td>
<td>Aurora MySQL 5.6</td>
<td>Aurora MySQL 5.7</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>US East (Ohio)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>Version 5.6.10a; Version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Version 5.6.10a; Version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Version 5.6.10a; Version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Version 5.6.10a; Version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>Version 5.6.10a; Version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>Version 5.6.10a; Version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>Version 5.6.10a; Version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>Version 5.6.10a; Version 1.22 and later</td>
<td>Version 2.07 and later</td>
</tr>
</tbody>
</table>
## Aurora machine learning

Aurora machine learning provides simple, optimized, and secure integration between Aurora and AWS machine learning services without having to build custom integrations or move data around. Aurora exposes ML models as SQL functions, so you don't need to learn new programming languages or tools. Instead, you use standard SQL to build applications that call ML models, pass data to them, and return predictions as query results. For more information, see Using machine learning (ML) capabilities with Amazon Aurora (p. 387).

<table>
<thead>
<tr>
<th>Region</th>
<th>Aurora MySQL 5.6</th>
<th>Aurora MySQL 5.7</th>
<th>Aurora PostgreSQL 10</th>
<th>Aurora PostgreSQL 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS GovCloud (US-East)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Aurora machine learning

Aurora machine learning provides simple, optimized, and secure integration between Aurora and AWS machine learning services without having to build custom integrations or move data around. Aurora exposes ML models as SQL functions, so you don't need to learn new programming languages or tools. Instead, you use standard SQL to build applications that call ML models, pass data to them, and return predictions as query results. For more information, see Using machine learning (ML) capabilities with Amazon Aurora (p. 387).
<table>
<thead>
<tr>
<th>Region</th>
<th>Aurora MySQL 5.6</th>
<th>Aurora MySQL 5.7</th>
<th>Aurora PostgreSQL 10</th>
<th>Aurora PostgreSQL 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa (Cape Town)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later (SageMaker only)</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later (SageMaker only)</td>
<td>Version 11.6 and later (SageMaker only)</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later (SageMaker only)</td>
<td>Version 11.6 and later (SageMaker only)</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later (SageMaker only)</td>
<td>Version 11.6 and later (SageMaker only)</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>-</td>
<td>-</td>
<td>Version 2.07 and later (SageMaker only)</td>
<td>Version 11.6 and later (SageMaker only)</td>
</tr>
</tbody>
</table>
Aurora parallel queries

Aurora parallel queries can speed up your queries by up to two orders of magnitude, while maintaining high throughput for your core transactional workload. Using the unique Aurora architecture, parallel queries can push down and parallelize query processing across thousands of CPUs in the Aurora storage layer. By offloading analytical query processing to the Aurora storage layer, parallel queries reduce network, CPU, and buffer pool contention for transactional workloads. For more information, see Working with parallel query for Amazon Aurora MySQL (p. 697). To learn more about Aurora MySQL versions available for parallel queries and any steps you might need to take based on that version to support parallel queries, see Planning for a parallel query cluster (p. 700).

Aurora parallel queries are available for Aurora MySQL only. However, PostgreSQL has its own parallel query feature that is available on Amazon RDS. The capability is enabled by default when a new PostgreSQL instance is created (versions 10.1 and later). For more information, see PostgreSQL on Amazon RDS.
Amazon RDS Proxy

Amazon RDS Proxy is a fully managed, highly available database proxy that makes applications more scalable by pooling and sharing established database connections. With RDS Proxy, failover times for Aurora are reduced by up to 66 percent. For more information, see Managing connections with Amazon RDS Proxy (p. 260).

<table>
<thead>
<tr>
<th>Region</th>
<th>Aurora MySQL 5.6</th>
<th>Aurora MySQL 5.7</th>
<th>Aurora PostgreSQL 10</th>
<th>Aurora PostgreSQL 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (Ohio)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Region</td>
<td>Aurora MySQL 5.6</td>
<td>Aurora MySQL 5.7</td>
<td>Aurora PostgreSQL 10</td>
<td>Aurora PostgreSQL 11</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>----------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Version 5.6.10a; version 1.22 and later</td>
<td>Version 2.07 and later</td>
<td>Version 10.11 and later</td>
<td>Version 11.6 and later</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Aurora Serverless v1

Aurora Serverless v1 is an on-demand, auto-scaling feature designed to be a cost-effective approach to running intermittent or unpredictable workloads on Amazon Aurora. It automatically starts up, shuts down, and scales capacity up or down, as needed by your applications. For more information, see Using Amazon Aurora Serverless v1 (p. 134).
<table>
<thead>
<tr>
<th>Region</th>
<th>Aurora MySQL 5.6</th>
<th>Aurora MySQL 5.7</th>
<th>Aurora PostgreSQL 10</th>
<th>Aurora PostgreSQL 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Canada Central</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Data API for Aurora Serverless

The Data API for Aurora Serverless provides a web-services interface to an Aurora Serverless cluster. Rather than managing database connections from client applications, you can run SQL commands against an HTTPS endpoint. For more information, see Using the Data API for Aurora Serverless (p. 162).

<table>
<thead>
<tr>
<th>Region</th>
<th>Aurora MySQL 5.6</th>
<th>Aurora MySQL 5.7</th>
<th>Aurora PostgreSQL 10</th>
<th>Aurora PostgreSQL 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS GovCloud (US-East)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region</th>
<th>Aurora MySQL 5.6</th>
<th>Aurora MySQL 5.7</th>
<th>Aurora PostgreSQL 10</th>
<th>Aurora PostgreSQL 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (Ohio)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Version 5.6.10a</td>
<td>Version 2.07.1</td>
<td>Version 10.12</td>
<td>-</td>
</tr>
</tbody>
</table>
Amazon Aurora connection management

Amazon Aurora typically involves a cluster of DB instances instead of a single instance. Each connection is handled by a specific DB instance. When you connect to an Aurora cluster, the host name and port that you specify point to an intermediate handler called an *endpoint*. Aurora uses the endpoint mechanism to abstract these connections. Thus, you don't have to hardcode all the hostnames or write your own logic for load-balancing and rerouting connections when some DB instances aren't available.
For certain Aurora tasks, different instances or groups of instances perform different roles. For example, the primary instance handles all data definition language (DDL) and data manipulation language (DML) statements. Up to 15 Aurora Replicas handle read-only query traffic.

Using endpoints, you can map each connection to the appropriate instance or group of instances based on your use case. For example, to perform DDL statements you can connect to whichever instance is the primary instance. To perform queries, you can connect to the reader endpoint, with Aurora automatically performing load-balancing among all the Aurora Replicas. For clusters with DB instances of different capacities or configurations, you can connect to custom endpoints associated with different subsets of DB instances. For diagnosis or tuning, you can connect to a specific instance endpoint to examine details about a specific DB instance.

**Topics**
- Types of Aurora endpoints (p. 25)
- Viewing the endpoints for an Aurora cluster (p. 27)
- Using the cluster endpoint (p. 27)
- Using the reader endpoint (p. 27)
- Using custom endpoints (p. 28)
- Creating a custom endpoint (p. 30)
- Viewing custom endpoints (p. 32)
- Editing a custom endpoint (p. 37)
- Deleting a custom endpoint (p. 39)
- End-to-end AWS CLI example for custom endpoints (p. 40)
- Using the instance endpoints (p. 44)
- How Aurora endpoints work with high availability (p. 44)

**Types of Aurora endpoints**

An endpoint is represented as an Aurora-specific URL that contains a host address and a port. The following types of endpoints are available from an Aurora DB cluster.

**Cluster endpoint**

A *cluster endpoint* (or *writer endpoint*) for an Aurora DB cluster connects to the current primary DB instance for that DB cluster. This endpoint is the only one that can perform write operations such as DDL statements. Because of this, the cluster endpoint is the one that you connect to when you first set up a cluster or when your cluster only contains a single DB instance.

Each Aurora DB cluster has one cluster endpoint and one primary DB instance.

You use the cluster endpoint for all write operations on the DB cluster, including inserts, updates, deletes, and DDL changes. You can also use the cluster endpoint for read operations, such as queries.

The cluster endpoint provides failover support for read/write connections to the DB cluster. If the current primary DB instance of a DB cluster fails, Aurora automatically fails over to a new primary DB instance. During a failover, the DB cluster continues to serve connection requests to the cluster endpoint from the new primary DB instance, with minimal interruption of service.

The following example illustrates a cluster endpoint for an Aurora MySQL DB cluster.

```
mydbcluster.cluster-123456789012.us-east-1.rds.amazonaws.com:3306
```

**Reader endpoint**

A *reader endpoint* for an Aurora DB cluster provides load-balancing support for read-only connections to the DB cluster. Use the reader endpoint for read operations, such as queries. By
processing those statements on the read-only Aurora Replicas, this endpoint reduces the overhead on the primary instance. It also helps the cluster to scale the capacity to handle simultaneous `SELECT` queries, proportional to the number of Aurora Replicas in the cluster. Each Aurora DB cluster has one reader endpoint.

If the cluster contains one or more Aurora Replicas, the reader endpoint load-balances each connection request among the Aurora Replicas. In that case, you can only perform read-only statements such as `SELECT` in that session. If the cluster only contains a primary instance and no Aurora Replicas, the reader endpoint connects to the primary instance. In that case, you can perform write operations through the endpoint.

The following example illustrates a reader endpoint for an Aurora MySQL DB cluster.

mydbcluster.cluster-ro-123456789012.us-east-1.rds.amazonaws.com:3306

**Custom endpoint**

A custom endpoint for an Aurora cluster represents a set of DB instances that you choose. When you connect to the endpoint, Aurora performs load balancing and chooses one of the instances in the group to handle the connection. You define which instances this endpoint refers to, and you decide what purpose the endpoint serves.

An Aurora DB cluster has no custom endpoints until you create one. You can create up to five custom endpoints for each provisioned Aurora cluster. You can't use custom endpoints for Aurora Serverless clusters.

The custom endpoint provides load-balanced database connections based on criteria other than the read-only or read/write capability of the DB instances. For example, you might define a custom endpoint to connect to instances that use a particular AWS instance class or a particular DB parameter group. Then you might tell particular groups of users about this custom endpoint. For example, you might direct internal users to low-capacity instances for report generation or ad hoc (one-time) querying, and direct production traffic to high-capacity instances.

Because the connection can go to any DB instance that is associated with the custom endpoint, we recommend that you make sure that all the DB instances within that group share some similar characteristic. Doing so ensures that the performance, memory capacity, and so on, are consistent for everyone who connects to that endpoint.

This feature is intended for advanced users with specialized kinds of workloads where it isn't practical to keep all the Aurora Replicas in the cluster identical. With custom endpoints, you can predict the capacity of the DB instance used for each connection. When you use custom endpoints, you typically don't use the reader endpoint for that cluster.

The following example illustrates a custom endpoint for a DB instance in an Aurora MySQL DB cluster.

myendpoint.cluster-custom-123456789012.us-east-1.rds.amazonaws.com:3306

**Instance endpoint**

An instance endpoint connects to a specific DB instance within an Aurora cluster. Each DB instance in a DB cluster has its own unique instance endpoint. So there is one instance endpoint for the current primary DB instance of the DB cluster, and there is one instance endpoint for each of the Aurora Replicas in the DB cluster.

The instance endpoint provides direct control over connections to the DB cluster, for scenarios where using the cluster endpoint or reader endpoint might not be appropriate. For example, your client application might require more fine-grained load balancing based on workload type. In this case, you can configure multiple clients to connect to different Aurora Replicas in a DB cluster to distribute read workloads. For an example that uses instance endpoints to improve connection speed after
a failover for Aurora PostgreSQL, see Fast failover with Amazon Aurora PostgreSQL (p. 1116). For an example that uses instance endpoints to improve connection speed after a failover for Aurora MySQL, see MariaDB Connector/J failover support – case Amazon Aurora.

The following example illustrates an instance endpoint for a DB instance in an Aurora MySQL DB cluster.

mydbinstance.123456789012.us-east-1.rds.amazonaws.com:3306

**Viewing the endpoints for an Aurora cluster**

In the AWS Management Console, you see the cluster endpoint, the reader endpoint, and any custom endpoints in the detail page for each cluster. You see the instance endpoint in the detail page for each instance. When you connect, you must append the associated port number, following a colon, to the endpoint name shown on this detail page.

With the AWS CLI, you see the writer, reader, and any custom endpoints in the output of the `describe-db-clusters` command. For example, the following command shows the endpoint attributes for all clusters in your current AWS Region.

```bash
aws rds describe-db-clusters --query '*[].
(Endpoint:Endpoint,ReaderEndpoint:ReaderEndpoint,CustomEndpoints:CustomEndpoints)'
```

With the Amazon RDS API, you retrieve the endpoints by calling the `DescribeDbClusterEndpoints` function.

**Using the cluster endpoint**

Because each Aurora cluster has a single built-in cluster endpoint, whose name and other attributes are managed by Aurora, you can’t create, delete, or modify this kind of endpoint.

You use the cluster endpoint when you administer your cluster, perform extract, transform, load (ETL) operations, or develop and test applications. The cluster endpoint connects to the primary instance of the cluster. The primary instance is the only DB instance where you can create tables and indexes, run `INSERT` statements, and perform other DDL and DML operations.

The physical IP address pointed to by the cluster endpoint changes when the failover mechanism promotes a new DB instance to be the read/write primary instance for the cluster. If you use any form of connection pooling or other multiplexing, be prepared to flush or reduce the time-to-live for any cached DNS information. Doing so ensures that you don’t try to establish a read/write connection to a DB instance that became unavailable or is now read-only after a failover.

**Using the reader endpoint**

You use the reader endpoint for read-only connections for your Aurora cluster. This endpoint uses a load-balancing mechanism to help your cluster handle a query-intensive workload. The reader endpoint is the endpoint that you supply to applications that do reporting or other read-only operations on the cluster.

The reader endpoint load-balances connections to available Aurora Replicas in an Aurora DB cluster. It doesn’t load-balance individual queries. If you want to load-balance each query to distribute the read workload for a DB cluster, open a new connection to the reader endpoint for each query.

Each Aurora cluster has a single built-in reader endpoint, whose name and other attributes are managed by Aurora. You can’t create, delete, or modify this kind of endpoint.
If your cluster contains only a primary instance and no Aurora Replicas, the reader endpoint connects to the primary instance. In that case, you can perform write operations through this endpoint.

**Using custom endpoints**

You use custom endpoints to simplify connection management when your cluster contains DB instances with different capacities and configuration settings.

Previously, you might have used the CNAMEs mechanism to set up Domain Name Service (DNS) aliases from your own domain to achieve similar results. By using custom endpoints, you can avoid updating CNAME records when your cluster grows or shrinks. Custom endpoints also mean that you can use encrypted Transport Layer Security/Secure Sockets Layer (TLS/SSL) connections.

Instead of using one DB instance for each specialized purpose and connecting to its instance endpoint, you can have multiple groups of specialized DB instances. In this case, each group has its own custom endpoint. This way, Aurora can perform load balancing among all the instances dedicated to tasks such as reporting or handling production or internal queries. The custom endpoints provide load balancing and high availability for each group of DB instances within your cluster. If one of the DB instances within a group becomes unavailable, Aurora directs subsequent custom endpoint connections to one of the other DB instances associated with the same endpoint.

**Topics**

- Specifying properties for custom endpoints (p. 28)
- Membership rules for custom endpoints (p. 29)
- Managing custom endpoints (p. 29)

**Specifying properties for custom endpoints**

The maximum length for a custom endpoint name is 63 characters. You can see the name format following:

```
endpointName.cluster-custom-customerDnsIdentifier.dnsSuffix
```

Because custom endpoint names don't include the name of your cluster, you don't have to change those names if you rename a cluster. You can't reuse the same custom endpoint name for more than one cluster in the same region. Give each custom endpoint a name that is unique across the clusters owned by your user ID within a particular region.

Each custom endpoint has an associated type that determines which DB instances are eligible to be associated with that endpoint. Currently, the type can be `READER`, `WRITER`, or `ANY`. The following considerations apply to the custom endpoint types:

- **Only DB instances that are read-only Aurora Replicas can be part of a `READER` custom endpoint.** The `READER` type applies only to clusters using single-master replication, because those clusters can include multiple read-only DB instances.

- **Both read-only Aurora Replicas and the read/write primary instance can be part of an `ANY` custom endpoint.** Aurora directs connections to cluster endpoints with type `ANY` to any associated DB instance with equal probability. Because you can't determine in advance if you are connecting to the primary instance of a read-only Aurora Replica, use this kind of endpoint for read-only connections only. The `ANY` type applies to clusters using any replication topology.

- **The `WRITER` type applies only to multi-master clusters, because those clusters can include multiple read/write DB instances.**

- **If you try to create a custom endpoint with a type that isn't appropriate based on the replication configuration for a cluster, Aurora returns an error.**
Membership rules for custom endpoints

When you add a DB instance to a custom endpoint or remove it from a custom endpoint, any existing connections to that DB instance remain active.

You can define a list of DB instances to include in, or exclude from, a custom endpoint. We refer to these lists as static and exclusion lists, respectively. You can use the inclusion/exclusion mechanism to further subdivide the groups of DB instances, and to make sure that the set of custom endpoints covers all the DB instances in the cluster. Each custom endpoint can contain only one of these list types.

In the AWS Management Console, the choice is represented by the check box Attach future instances added to this cluster. When you keep check box clear, the custom endpoint uses a static list containing only the DB instances specified in the dialog. When you choose the check box, the custom endpoint uses an exclusion list. In this case, the custom endpoint represents all DB instances in the cluster (including any that you add in the future) except the ones left unselected in the dialog. The AWS CLI and Amazon RDS API have parameters representing each kind of list. When you use the AWS CLI or Amazon RDS API, you can't add or remove individual members to the lists; you always specify the entire new list.

Aurora doesn't change the DB instances specified in the static or exclusion lists when DB instances change roles between primary instance and Aurora Replica due to failover or promotion. For example, a custom endpoint with type READER might include a DB instance that was an Aurora Replica and then was promoted to a primary instance. The type of a custom endpoint (READER, WRITER, or ANY) determines what kinds of operations you can perform through that endpoint.

You can associate a DB instance with more than one custom endpoint. For example, suppose that you add a new DB instance to a cluster, or that Aurora adds a DB instance automatically through the autoscaling mechanism. In these cases, the DB instance is added to all custom endpoints for which it is eligible. Which endpoints the DB instance is added to is based on the custom endpoint type of READER, WRITER, or ANY, plus any static or exclusion lists defined for each endpoint. For example, if the endpoint includes a static list of DB instances, newly added Aurora Replicas aren't added to that endpoint. Conversely, if the endpoint has an exclusion list, newly added Aurora Replicas are added to the endpoint, if they aren't named in the exclusion list and their roles match the type of the custom endpoint.

If an Aurora Replica becomes unavailable, it remains associated with any custom endpoints. For example, it remains part of the custom endpoint when it is unhealthy, stopped, rebooting, and so on. However, you can't connect to it through those endpoints until it becomes available again.

Managing custom endpoints

Because newly created Aurora clusters have no custom endpoints, you must create and manage these objects yourself. You do so using the AWS Management Console, AWS CLI, or Amazon RDS API.

Note
You must also create and manage custom endpoints for Aurora clusters restored from snapshots. Custom endpoints are not included in the snapshot. You create them again after restoring, and choose new endpoint names if the restored cluster is in the same region as the original one.

To work with custom endpoints from the AWS Management Console, you navigate to the details page for your Aurora cluster and use the controls under the Custom Endpoints section.

To work with custom endpoints from the AWS CLI, you can use these operations:

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

To work with custom endpoints through the Amazon RDS API, you can use the following functions:

• `CreateDBClusterEndpoint`
• `DescribeDBClusterEndpoints`
• `ModifyDBClusterEndpoint`
• `DeleteDBClusterEndpoint`

### Creating a custom endpoint

**Console**

To create a custom endpoint with the AWS Management Console, go to the cluster detail page and choose the **Create custom endpoint** action in the **Endpoints** section. Choose a name for the custom endpoint, unique for your user ID and region. To choose a list of DB instances that remains the same even as the cluster expands, keep the check box **Attach future instances added to this cluster** clear. When you choose that check box, the custom endpoint dynamically adds any new instances as you add them to the cluster.
Create custom endpoint

Endpoint name

Endpoint name is case insensitive, First character must be a letter. Can

Endpoint members

Filter database
You can't select the custom endpoint type of **ANY** or **READER** in the AWS Management Console. All the custom endpoints you create through the AWS Management Console have a type of **ANY**.

### AWS CLI

To create a custom endpoint with the AWS CLI, run the `create-db-cluster-endpoint` command.

The following command creates a custom endpoint attached to a specific cluster. Initially, the endpoint is associated with all the Aurora Replica instances in the cluster. A subsequent command associates it with a specific set of DB instances in the cluster.

For Linux, macOS, or Unix:

```bash
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
```

For Windows:

```bash
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

To create a custom endpoint with the RDS API, run the `CreateDBClusterEndpoint` operation.

### Viewing custom endpoints

#### Console

To view custom endpoints with the AWS Management Console, go to the cluster detail page for the cluster and look under the **Endpoints** section. This section contains information only about custom endpoints. The details for the built-in endpoints are listed in the main **Details** section. To see the details for a specific custom endpoint, select its name to bring up the detail page for that endpoint.

The following screenshot shows how the list of custom endpoints for an Aurora cluster is initially empty.
After you create some custom endpoints for that cluster, they are shown under the **Endpoints** section.
Clicking through to the detail page shows which DB instances the endpoint is currently associated with.
Amazon Aurora User Guide for Aurora
Viewing custom endpoints

RDS ➔ Clusters:

Details

Endpoint name

Endpoint members

Filter endpoint members
To see the additional detail of whether new DB instances added to the cluster are automatically added to the endpoint also, bring up the **Edit** dialog for the endpoint.

**AWS CLI**

To view custom endpoints with the AWS CLI, run the `describe-db-cluster-endpoints` command.

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

The following shows some sample output from a `describe-db-cluster-endpoints` command. The `EndpointType` of `WRITER` or `READER` denotes the built-in read/write and read-only endpoints for the cluster. The `EndpointType` of `CUSTOM` denotes endpoints that you create and choose the associated DB instances. One of the endpoints has a non-empty `StaticMembers` field, denoting that it is associated with a precise set of DB instances. The other endpoint has a non-empty `ExcludedMembers` field, denoting that the endpoint is associated with all DB instances other than the ones listed under `ExcludedMembers`. This second kind of custom endpoint grows to accommodate new instances as you add them to the cluster.

```json
{
  "DBClusterEndpoints": [
    {
      "Endpoint": "custom-endpoint-demo.cluster-123456789012.ca-central-1.rds.amazonaws.com",
      "Status": "available",
      "DBClusterIdentifier": "custom-endpoint-demo",
      "EndpointType": "WRITER"
    },
    {
      "Endpoint": "custom-endpoint-demo.cluster-ro-123456789012.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-123456789012.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-W7PE3TLFFSHQF6G6V5FHU",
},
{
"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-W7PE3TLFFSHQF6G6V5FHU",
"DBClusterEndpointArn": "arn:aws:rds:ca-central-1:11112223333:cluster-endpoint:eight-and-higher"
}
]

RDS API

To view custom endpoints with the RDS API, run the DescribeDBClusterEndpoints.html operation.

Editing a custom endpoint

You can edit the properties of a custom endpoint to change which DB instances are associated with the endpoint. You can also change an endpoint between a static list and an exclusion list. If you need more details about these endpoint properties, see Membership rules for custom endpoints (p. 29).

You can't connect to or use a custom endpoint while the changes from an edit action are in progress. It might take some minutes before the endpoint status returns to Available and you can connect again.

Console

To edit a custom endpoint with the AWS Management Console, you can select the endpoint on the cluster detail page, or bring up the detail page for the endpoint, and choose the Edit action.
Amazon Aurora User Guide for Aurora
Editing a custom endpoint

Edit endpoint:

Endpoint members

Filter database

DB instance name

[Image of RDS and Clusters interface]
AWS CLI

To edit a custom endpoint with the AWS CLI, run the `modify-db-cluster-endpoint` command.

The following commands change the set of DB instances that apply to a custom endpoint and optionally switches between the behavior of a static or exclusion list. The `--static-members` and `--excluded-members` parameters take a space-separated list of DB instance identifiers.

For Linux, macOS, or Unix:

```
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
```

For 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

To edit a custom endpoint with the RDS API, run the `ModifyDBClusterEndpoint.html` operation.

Deleting a custom endpoint

Console

To delete a custom endpoint with the AWS Management Console, go to the cluster detail page, select the appropriate custom endpoint, and select the Delete action.

AWS CLI

To delete a custom endpoint with the AWS CLI, run the `delete-db-cluster-endpoint` command.
The following command deletes a custom endpoint. You don't need to specify the associated cluster, but you must specify the region.

For Linux, macOS, or Unix:

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

For Windows:

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

RDS API

To delete a custom endpoint with the RDS API, run the `DeleteDBClusterEndpoint` operation.

**End-to-end AWS CLI example for custom endpoints**

The following tutorial uses AWS CLI examples with Unix shell syntax to show you might define a cluster with several "small" DB instances and a few "big" DB instances, and create custom endpoints to connect to each set of DB instances. To run similar commands on your own system, you should be familiar enough with the basics of working with Aurora clusters and AWS CLI usage to supply your own values for parameters such as region, subnet group, and VPC security group.

This example demonstrates the initial setup steps: creating an Aurora cluster and adding DB instances to it. This is a heterogeneous cluster, meaning not all the DB instances have the same capacity. Most instances use the AWS instance class `db.r4.4xlarge`, but the last two DB instances use `db.r4.16xlarge`. Each of these sample `create-db-instance` commands prints its output to the screen and saves a copy of the JSON in a file for later inspection.

```bash
aws rds create-db-cluster --db-cluster-identifier custom-endpoint-demo --engine aurora \ --engine-version 5.6.10a --master-username $MASTER_USER --master-user-password $MASTER_PW \ --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
```
The larger instances are reserved for specialized kinds of reporting queries. To make it unlikely for them to be promoted to the primary instance, the following example changes their promotion tier to the lowest priority.

```bash
for i in 09 10
do
  aws rds modify-db-instance --db-instance-id custom-endpoint-demo-$i \ 
  --region $REGION --promotion-tier 15
done
```

Suppose that you want to use the two "bigger" instances only for the most resource-intensive queries. To do this, you can first create a custom read-only endpoint. Then you can add a static list of members so that the endpoint connects only to those DB instances. Those instances are already in the lowest promotion tier, making it unlikely either of them will be promoted to the primary instance. If one of them is promoted to the primary instance, it becomes unreachable through this endpoint because we specified the `READER` type instead of the `ANY` type.

The following example demonstrates the create and modify endpoint commands, and sample JSON output showing the initial and modified state of the custom endpoint.

```bash
$ 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-123456789012.ca-central-1.rds.amazonaws.com",
  "DBClusterEndpointIdentifier": "big-instances",
  "DBClusterIdentifier": "custom-endpoint-demo",
  "StaticMembers": [],
  "DBClusterEndpointResourceIdentifier": "cluster-endpoint-W7PE3TLLFN5H5QFU6J6NV5FU",
  "ExcludedMembers": [],
  "CustomEndpointType": "READER",
  "Status": "creating",
}

$ 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-W7PE3TLLFN5H5QFU6J6NV5FU",
  "CustomEndpointType": "READER",
  "StaticMembers": [
    "custom-endpoint-demo-10",
    "custom-endpoint-demo-09"
  ],
  "Status": "modifying",
  "Endpoint": "big-instances.cluster-custom-123456789012.ca-central-1.rds.amazonaws.com",
  "DBClusterIdentifier": "custom-endpoint-demo"
}
```

The default `READER` endpoint for the cluster can connect to either the "small" or "big" DB instances, making it impractical to predict query performance and scalability when the cluster becomes busy. To divide the workload cleanly between the sets of DB instances, you can ignore the default `READER` endpoint and create a second custom endpoint that connects to all other DB instances. The following
example does so by creating a custom endpoint and then adding an exclusion list. Any other DB instances you add to the cluster later will be added to this endpoint automatically. The ANY type means that this endpoint is associated with eight instances in total: the primary instance and another seven Aurora Replicas. If the example used the READER type, the custom endpoint would only be associated with the seven Aurora Replicas.

```
$ 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-123456789012.ca-central-1.rds.amazonaws.com",
"StaticMembers": [],
"ExcludedMembers": [],
"DBClusterIdentifier": "custom-endpoint-demo",
"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",
"DBClusterEndpointResourceIdentifier": "cluster-endpoint-6RDDXQOC3AKKZT2PRD7ST37BMY",
"CustomEndpointType": "ANY",
"Endpoint": "small-instances.cluster-custom-123456789012.ca-central-1.rds.amazonaws.com",
"EndpointType": "CUSTOM",
"ExcludedMembers": [
    "custom-endpoint-demo-09",
    "custom-endpoint-demo-10"
],
"StaticMembers": [],
"DBClusterIdentifier": "custom-endpoint-demo",
"Status": "modifying"
}
```

The following example checks the state of the endpoints for this cluster. The cluster still has its original cluster endpoint, with EndPointType of WRITER, which you would still use for administration, ETL, and other write operations. It still has its original READER endpoint, which you wouldn't use because each connection to it might be directed to a "small" or "big" DB instance. The custom endpoints make this behavior predictable, with connections guaranteed to use one of the "small" or "big" DB instances based on the endpoint you specify.

```
$ aws rds describe-db-cluster-endpoints --region $REGION
{
"DBClusterEndpoints": [
    
    
    "Endpoint": "custom-endpoint-demo.cluster-123456789012.ca-central-1.rds.amazonaws.com",
    "Status": "available",
    "DBClusterIdentifier": "custom-endpoint-demo"
],
```
The final examples demonstrate how successive database connections to the custom endpoints connect to the various DB instances in the Aurora cluster. The small-instances endpoint always connects to the db.r4.4xlarge DB instances, which are the lower-numbered hosts in this cluster.

```bash
$ mysql -h small-instances.cluster-custom-123456789012.ca-central-1.rds.amazonaws.com -u $MYUSER -p
mysql> select @@aurora_server_id;
+-------------------------+
| @@aurora_server_id      |
+-------------------------+
| custom-endpoint-demo-02 |
+-------------------------+
```

```bash
$ mysql -h small-instances.cluster-custom-123456789012.ca-central-1.rds.amazonaws.com -u $MYUSER -p
mysql> select @@aurora_server_id;
+-------------------------+
| @@aurora_server_id      |
+-------------------------+
| custom-endpoint-demo-02 |
+-------------------------+
```

```bash
$ mysql -h big-instances.cluster-custom-123456789012.ca-central-1.rds.amazonaws.com -u $MYUSER -p
mysql> select @@aurora_server_id;
+-------------------------+
| @@aurora_server_id      |
+-------------------------+
| custom-endpoint-demo-09 |
+-------------------------+
```

```bash
$ mysql -h big-instances.cluster-custom-123456789012.ca-central-1.rds.amazonaws.com -u $MYUSER -p
mysql> select @@aurora_server_id;
+-------------------------+
| @@aurora_server_id      |
+-------------------------+
| custom-endpoint-demo-09 |
+-------------------------+
```

Using the instance endpoints

Each DB instance in an Aurora cluster has its own built-in instance endpoint, whose name and other attributes are managed by Aurora. You can’t create, delete, or modify this kind of endpoint. You might be familiar with instance endpoints if you use Amazon RDS. However, with Aurora you typically use the writer and reader endpoints more often than the instance endpoints.

In day-to-day Aurora operations, the main way that you use instance endpoints is to diagnose capacity or performance issues that affect one specific instance in an Aurora cluster. While connected to a specific instance, you can examine its status variables, metrics, and so on. Doing this can help you determine what’s happening for that instance that’s different from what’s happening for other instances in the cluster.

In advanced use cases, you might configure some DB instances differently than others. In this case, use the instance endpoint to connect directly to an instance that is smaller, larger, or otherwise has different characteristics than the others. Also, set up failover priority so that this special DB instance is the last choice to take over as the primary instance. We recommend that you use custom endpoints instead of the instance endpoint in such cases. Doing so simplifies connection management and high availability as you add more DB instances to your cluster.

How Aurora endpoints work with high availability

For clusters where high availability is important, use the writer endpoint for read/write or general-purpose connections and the reader endpoint for read-only connections. The writer and reader
Endpoints manage DB instance failover better than instance endpoints do. Unlike the instance endpoints, the writer and reader endpoints automatically change which DB instance they connect to if a DB instance in your cluster becomes unavailable.

If the primary DB instance of a DB cluster fails, Aurora automatically fails over to a new primary DB instance. It does so by either promoting an existing Aurora Replica to a new primary DB instance or creating a new primary DB instance. If a failover occurs, you can use the writer endpoint to reconnect to the newly promoted or created primary DB instance, or use the reader endpoint to reconnect to one of the Aurora Replicas in the DB cluster. During a failover, the reader endpoint might direct connections to the new primary DB instance of a DB cluster for a short time after an Aurora Replica is promoted to the new primary DB instance.

If you design your own application logic to manage connections to instance endpoints, you can manually or programmatically discover the resulting set of available DB instances in the DB cluster. You can then confirm their instance classes after failover and connect to an appropriate instance endpoint.

For more information about failovers, see Fault tolerance for an Aurora DB cluster (p. 56).
DB instance classes

The DB instance class determines the computation and memory capacity of an Amazon RDS DB instance. The DB instance class you need depends on your processing power and memory requirements.

For more information about instance class pricing, see Amazon RDS pricing.

Topics
- DB instance class types (p. 46)
- Supported DB engines for DB instance classes (p. 47)
- Hardware specifications for DB instance classes for Aurora (p. 49)

DB instance class types

Amazon Aurora supports two types of instance classes: Memory Optimized and Burstable Performance. For more information about Amazon EC2 instance types, see Instance type in the Amazon EC2 documentation.

The following are the Memory Optimized DB instance classes available:

- **Preview db.r6g** – Newest-generation instance classes powered by AWS Graviton2 processors. These are ideal for running memory-intensive workloads in open-source databases such as MySQL and PostgreSQL.
  
  **Note**
  Graviton2 DB instance classes are now available in preview release. Don't use the db.r6g preview DB instance classes with production databases. Your participation in this preview is governed by section 2 of the AWS Service Terms.

- **db.r5** – Latest-generation instance classes optimized for memory-intensive applications. These offer improved networking performance. They are powered by the AWS Nitro System, a combination of dedicated hardware and lightweight hypervisor.

- **db.r4** – Current-generation instance classes optimized for memory-intensive applications. These offer improved networking performance.

- **db.r3** – Previous-generation instance classes that provide memory optimization. The db.r3 instances classes are not available in the Europe (Paris) region.

The following are the Burstable Performance DB instance classes available:

- **db.t3** – Latest-generation instance classes that provide a baseline performance level, with the ability to burst to full CPU usage. These instance classes provide more computing capacity than the previous db.t2 instance classes. They are powered by the AWS Nitro System, a combination of dedicated hardware and lightweight hypervisor.

- **db.t2** – Current-generation instance classes that provide a baseline performance level, with the ability to burst to full CPU usage. We recommend using these instance classes only for development and test servers, or other nonproduction servers.

  **Note**
  The DB instance classes that use the AWS Nitro System (db.r5, db.t3) are throttled on combined read plus write workload.

For DB instance class hardware specifications, see Hardware specifications for DB instance classes for Aurora (p. 49).
Supported DB engines for DB instance classes

The following are DB engine considerations for DB instance classes:

- **Preview Aurora support for db.r6g**
  - Aurora MySQL version 2.09.1 supports the db.r6g instance classes.
  - Aurora PostgreSQL version 3.4 compatible with PostgreSQL 11.9 supports the db.r6g instance classes.

- **Aurora support for db.r5**
  - Aurora MySQL versions support the db.r5 instance classes as specified in the following table. These instance classes are available in all Aurora regions except AWS GovCloud (US-West), AWS GovCloud (US-East), and China (Beijing).
  - For Aurora PostgreSQL, the versions that support db.r5 instance classes depend on the AWS Region that your DB cluster is in. To determine which Aurora PostgreSQL versions support db.r5 instance classes for a specific AWS Region, use the CLI command `describe-orderable-db-instance-options`. Enter the AWS Region of your cluster for the `--region` parameter in the following command.

  For Linux, macOS, or Unix:

  ```bash
  aws rds describe-orderable-db-instance-options --engine aurora-postgresql --db-instance-class db.r5.large \  
  --query 'OrderableDBInstanceOptions[].[DBInstanceClass,StorageType,Engine,EngineVersion]' --output text \  
  --region your-cluster-AWS-Region
  ```

  For Windows:

  ```bash
  aws rds describe-orderable-db-instance-options --engine aurora-postgresql --db-instance-class db.r5.large ^ \  
  --query 'OrderableDBInstanceOptions[].[DBInstanceClass,StorageType,Engine,EngineVersion]' --output text ^ \  
  --region your-cluster-AWS-Region
  ```

- **Aurora support for db.t3**
  - Aurora MySQL supports the db.t3.medium and db.t3.small instance classes for Aurora MySQL 1.15 and higher, and all Aurora MySQL 2.x versions. These instance classes are available for Aurora MySQL in all Aurora regions except China (Beijing).
  - For Aurora MySQL db.r5, db.r4, and db.t3 DB instance classes, no instances in the cluster can have pending instance-level system updates. To see pending system updates, use the following AWS CLI command.

  ```bash
  aws rds describe-pending-maintenance-actions
  ```

  - Aurora PostgreSQL supports the following db.t3 instance classes:
    - The db.t3.medium instance class is supported for versions compatible with PostgreSQL 10.7 or later.
    - The db.t3.large instance class is supported for versions compatible with PostgreSQL versions 10.11 or later and 11.6 or later.

  In the following table, you can find details about supported Amazon Aurora DB instance classes for the Aurora DB engines.
### Supported DB engines

<table>
<thead>
<tr>
<th>Instance class</th>
<th>Aurora MySQL</th>
<th>Aurora PostgreSQL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preview db.r6g – Newest generation memory optimized instance classes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preview db.r6g.16xlarge</td>
<td>2.09.1</td>
<td>3.4 (PostgreSQL 11.9)</td>
</tr>
<tr>
<td>Preview db.r6g.12xlarge</td>
<td>2.09.1</td>
<td>3.4 (PostgreSQL 11.9)</td>
</tr>
<tr>
<td>Preview db.r6g.4xlarge</td>
<td>2.09.1</td>
<td>3.4 (PostgreSQL 11.9)</td>
</tr>
<tr>
<td>Preview db.r6g.2xlarge</td>
<td>2.09.1</td>
<td>3.4 (PostgreSQL 11.9)</td>
</tr>
<tr>
<td>Preview db.r6g.xlarge</td>
<td>2.09.1</td>
<td>3.4 (PostgreSQL 11.9)</td>
</tr>
<tr>
<td>Preview db.r6g.large</td>
<td>2.09.1</td>
<td>3.4 (PostgreSQL 11.9)</td>
</tr>
<tr>
<td><strong>db.r5 – Latest generation memory optimized instance classes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.r5.24xlarge</td>
<td>1.22 and higher, 2.06 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r5.16xlarge</td>
<td>1.22 and higher, 2.06 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r5.12xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r5.8xlarge</td>
<td>1.22 and higher, 2.06 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r5.4xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r5.2xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r5.xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r5.large</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>db.r4 – Current generation memory optimized instance classes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.r4.16xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r4.8xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r4.4xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r4.2xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r4.xlarge</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td>db.r4.large</td>
<td>1.14.4 and higher</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>db.r3 – Previous generation memory optimized instance classes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.r3.8xlarge</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>db.r3.4xlarge</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>db.r3.2xlarge</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>db.r3.xlarge</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>db.r3.large</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### Hardware specifications for DB instance classes for Aurora

The following terminology is used to describe hardware specifications for DB instance classes:

<table>
<thead>
<tr>
<th>Instance class</th>
<th>Aurora MySQL</th>
<th>Aurora PostgreSQL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>db.t3 – Latest generation burstable performance instance classes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.t3.2xlarge</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>db.t3.xlarge</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>db.t3.large</td>
<td>No</td>
<td>10.11 and higher, 11.6 and higher</td>
</tr>
<tr>
<td>db.t3.medium</td>
<td>1.14.4 and higher</td>
<td>10.7 and higher</td>
</tr>
<tr>
<td>db.t3.small</td>
<td>1.14.4 and later</td>
<td>No</td>
</tr>
<tr>
<td>db.t3.micro</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>db.t2 – Current generation burstable performance instance classes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.t2.medium</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>db.t2.small</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**vCPU**

The number of virtual central processing units (CPUs). A virtual CPU is a unit of capacity that you can use to compare DB instance classes. Instead of purchasing or leasing a particular processor to use for several months or years, you are renting capacity by the hour. Our goal is to make a consistent and specific amount of CPU capacity available, within the limits of the actual underlying hardware.

**ECU**

The relative measure of the integer processing power of an Amazon EC2 instance. To make it easy for developers to compare CPU capacity between different instance classes, we have defined an Amazon EC2 Compute Unit. The amount of CPU that is allocated to a particular instance is expressed in terms of these EC2 Compute Units. One ECU currently provides CPU capacity equivalent to a 1.0–1.2 GHz 2007 Opteron or 2007 Xeon processor.

**Memory (GiB)**

The RAM, in gibibytes, allocated to the DB instance. There is often a consistent ratio between memory and vCPU. As an example, take the db.r4 instance class, which has a memory to vCPU ratio similar to the db.r5 instance class. However, for most use cases the db.r5 instance class provides better, more consistent performance than the db.r4 instance class.

**Max. Bandwidth (Mbps)**

The maximum bandwidth in megabits per second. Divide by 8 to get the expected throughput in megabytes per second.

**Note**

This figure refers to I/O bandwidth for local storage within the DB instance. It doesn’t apply to communication with the Aurora cluster volume.

**Network Performance**

The network speed relative to other DB instance classes.
In the following table, you can find hardware details about the Amazon RDS DB instance classes for Aurora.

For information about Aurora DB engine support for each DB instance class, see Supported DB engines for DB instance classes (p. 47).

<table>
<thead>
<tr>
<th>Instance class</th>
<th>vCPU</th>
<th>ECU</th>
<th>Memory (GiB)</th>
<th>Max. bandwidth (mbps) of local storage</th>
<th>Network performance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preview db.r6g – Newest generation memory optimized instance classes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.r6g.16xlarge</td>
<td>64</td>
<td>–</td>
<td>512</td>
<td>19,000</td>
<td>25 Gbps</td>
</tr>
<tr>
<td>db.r6g.12xlarge</td>
<td>48</td>
<td>–</td>
<td>384</td>
<td>13,500</td>
<td>20 Gbps</td>
</tr>
<tr>
<td>db.r6g.4xlarge</td>
<td>16</td>
<td>–</td>
<td>128</td>
<td>4,750</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r6g.2xlarge</td>
<td>8</td>
<td>–</td>
<td>64</td>
<td>Up to 4,750</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r6g.xlarge</td>
<td>4</td>
<td>–</td>
<td>32</td>
<td>Up to 4,750</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r6g.large</td>
<td>2</td>
<td>–</td>
<td>16</td>
<td>Up to 4,750</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td><strong>db.r5 – Latest generation memory optimized instance classes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.r5.24xlarge</td>
<td>96</td>
<td>347</td>
<td>768</td>
<td>19,000</td>
<td>25 Gbps</td>
</tr>
<tr>
<td>db.r5.16xlarge</td>
<td>64</td>
<td>264</td>
<td>512</td>
<td>13,600</td>
<td>20 Gbps</td>
</tr>
<tr>
<td>db.r5.12xlarge</td>
<td>48</td>
<td>173</td>
<td>384</td>
<td>9,500</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>db.r5.8xlarge</td>
<td>32</td>
<td>132</td>
<td>256</td>
<td>6,800</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>db.r5.4xlarge</td>
<td>16</td>
<td>71</td>
<td>128</td>
<td>4,750</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r5.2xlarge</td>
<td>8</td>
<td>38</td>
<td>64</td>
<td>Up to 4,750</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r5.xlarge</td>
<td>4</td>
<td>19</td>
<td>32</td>
<td>Up to 4,750</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r5.large</td>
<td>2</td>
<td>10</td>
<td>16</td>
<td>Up to 4,750</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td><strong>db.r4 – Current generation memory optimized instance classes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.r4.16xlarge</td>
<td>64</td>
<td>195</td>
<td>488</td>
<td>14,000</td>
<td>25 Gbps</td>
</tr>
<tr>
<td>db.r4.8xlarge</td>
<td>32</td>
<td>99</td>
<td>244</td>
<td>7,000</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>db.r4.4xlarge</td>
<td>16</td>
<td>53</td>
<td>122</td>
<td>3,500</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r4.2xlarge</td>
<td>8</td>
<td>27</td>
<td>61</td>
<td>1,700</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r4.xlarge</td>
<td>4</td>
<td>13.5</td>
<td>30.5</td>
<td>850</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td>db.r4.large</td>
<td>2</td>
<td>7</td>
<td>15.25</td>
<td>425</td>
<td>Up to 10 Gbps</td>
</tr>
<tr>
<td><strong>db.r3 – Previous generation memory optimized instance classes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.r3.8xlarge</td>
<td>32</td>
<td>104</td>
<td>244</td>
<td>—</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>db.r3.4xlarge</td>
<td>16</td>
<td>52</td>
<td>122</td>
<td>2,000</td>
<td>High</td>
</tr>
<tr>
<td>db.r3.2xlarge</td>
<td>8</td>
<td>26</td>
<td>61</td>
<td>1,000</td>
<td>High</td>
</tr>
</tbody>
</table>
Amazon Aurora storage and reliability

Following, you can learn about the Aurora storage subsystem. Aurora uses a distributed and shared storage architecture that is an important factor in performance, scalability, and reliability for Aurora clusters.

**Topics**

- Overview of Aurora storage (p. 51)
- What the cluster volume contains (p. 52)
- How Aurora storage automatically resizes (p. 52)
- How Aurora data storage is billed (p. 52)
- Amazon Aurora reliability (p. 53)

**Overview of Aurora storage**

Aurora data is stored in the *cluster volume*, which is a single, virtual volume that uses solid state drives (SSDs). A cluster volume consists of copies of the data across three Availability Zones in a single AWS Region. Because the data is automatically replicated across Availability Zones, your data is highly durable with less possibility of data loss. This replication also ensures that your database is more available during a failover. It does so because the data copies already exist in the other Availability Zones and continue to serve data requests to the DB instances in your DB cluster. The amount of replication is independent of the number of DB instances in your cluster.
What the cluster volume contains

The Aurora cluster volume contains all your user data, schema objects, and internal metadata such as the system tables and the binary log. For example, Aurora stores all the tables, indexes, binary large objects (BLOBs), stored procedures, and so on for an Aurora cluster in the cluster volume.

The Aurora shared storage architecture makes your data independent from the DB instances in the cluster. For example, you can add a DB instance quickly because Aurora doesn't make a new copy of the table data. Instead, the DB instance connects to the shared volume that already contains all your data. You can remove a DB instance from a cluster without removing any of the underlying data from the cluster. Only when you delete the entire cluster does Aurora remove the data.

How Aurora storage automatically resizes

Aurora cluster volumes automatically grow as the amount of data in your database increases. An Aurora cluster volume can grow to a maximum size of 128 tebibytes (TiB) for the following engine versions:

- Aurora MySQL engine versions 1.23 compatible with MySQL 5.6 and 2.09 compatible with MySQL 5.70
- Aurora PostgreSQL engine versions 9.6.17 or higher, 10.12 or higher, and 11.7 or higher.

This automatic storage scaling is combined with a high-performance and highly distributed storage subsystem. These make Aurora a good choice for your important enterprise data when your main objectives are reliability and high availability. For ways to balance storage costs against these other priorities, see the following

When Aurora data is removed, the space allocated for that data is freed. Examples of removing data include dropping or truncating a table. This automatic reduction in storage usage helps you to minimize storage charges.

**Note**
The storage limits and dynamic resizing behavior discussed here applies to persistent tables and other data stored in the cluster volume. Data for temporary tables is stored in the local DB instance and it's maximum size depends on the instance class that you use.

Some storage features, such as the maximum size of a cluster volume and automatic resizing when data is deleted, depend on the Aurora version of your cluster. For more information, see Storage scaling (p. 349). You can also learn how to avoid storage issues and how to monitor the allocated storage and free space in your cluster.

How Aurora data storage is billed

Even though an Aurora cluster volume can grow up to 128 tebibytes (TiB), you are only charged for the space that you use in an Aurora cluster volume. In earlier Aurora versions, the cluster volume could reuse space that was freed up when you deleted data, but the allocated storage space would never decrease. Starting in Aurora MySQL 2.09.0 and 1.23.0, and Aurora PostgreSQL 3.3.0 and 2.6.0, when Aurora data is removed, such as by dropping a table or database, the overall allocated space decreases by a comparable amount. Thus, you can reduce storage charges by deleting tables, indexes, databases, and so on that you no longer need.

**Tip**
For earlier versions without the dynamic resizing feature, resetting the storage usage for a cluster involved doing a logical dump and restoring to a new cluster. That operation can take a long time for a substantial volume of data. If you encounter this situation, consider upgrading your cluster to a version that supports volume shrinking.

For pricing information about Aurora data storage, see Amazon RDS for Aurora Pricing.
For information about how to minimize storage charges by monitoring storage usage for your cluster, see Storage scaling (p. 349). For pricing information about Aurora data storage, see Amazon RDS for Aurora pricing.

Amazon Aurora reliability

Aurora is designed to be reliable, durable, and fault tolerant. You can architect your Aurora DB cluster to improve availability by doing things such as adding Aurora Replicas and placing them in different Availability Zones, and also Aurora includes several automatic features that make it a reliable database solution.

Topics
- Storage auto-repair (p. 53)
- Survivable cache warming (p. 53)
- Crash recovery (p. 53)

Storage auto-repair

Because Aurora maintains multiple copies of your data in three Availability Zones, the chance of losing data as a result of a disk failure is greatly minimized. Aurora automatically detects failures in the disk volumes that make up the cluster volume. When a segment of a disk volume fails, Aurora immediately repairs the segment. When Aurora repairs the disk segment, it uses the data in the other volumes that make up the cluster volume to ensure that the data in the repaired segment is current. As a result, Aurora avoids data loss and reduces the need to perform a point-in-time restore to recover from a disk failure.

Survivable cache warming

Aurora "warms" the buffer pool cache when a database starts up after it has been shut down or restarted after a failure. That is, Aurora preloads the buffer pool with the pages for known common queries that are stored in an in-memory page cache. This provides a performance gain by bypassing the need for the buffer pool to "warm up" from normal database use.

The Aurora page cache is managed in a separate process from the database, which allows the page cache to survive independently of the database. In the unlikely event of a database failure, the page cache remains in memory, which ensures that the buffer pool is warmed with the most current state when the database restarts.

Crash recovery

Aurora is designed to recover from a crash almost instantaneously and continue to serve your application data without the binary log. Aurora performs crash recovery asynchronously on parallel threads, so that your database is open and available immediately after a crash.

For more information about crash recovery, see Fault tolerance for an Aurora DB cluster (p. 56).

The following are considerations for binary logging and crash recovery on Aurora MySQL:
- Enabling binary logging on Aurora directly affects the recovery time after a crash, because it forces the DB instance to perform binary log recovery.
- The type of binary logging used affects the size and efficiency of logging. For the same amount of database activity, some formats log more information than others in the binary logs. The following settings for the `binlog_format` parameter result in different amounts of log data:
  - `ROW` – The most log data
Amazon Aurora security

Security for Amazon Aurora is managed at three levels:

- **To control who can perform Amazon RDS management actions on Aurora DB clusters and DB instances, you use AWS Identity and Access Management (IAM). When you connect to AWS using IAM credentials, your AWS account must have IAM policies that grant the permissions required to perform Amazon RDS management operations. For more information, see Identity and access management in Amazon Aurora (p. 1222).**

  If you are using IAM to access the Amazon RDS console, you must first log on to the AWS Management Console with your IAM user credentials, and then go to the Amazon RDS console at https://console.aws.amazon.com/rds.

- **Aurora DB clusters must be created in a virtual private cloud (VPC) based on the Amazon VPC service. To control which devices and Amazon EC2 instances can open connections to the endpoint and port of the DB instance for Aurora DB clusters in a VPC, you use a VPC security group. You can make these endpoint and port connections using Transport Layer Security (TLS)/Secure Sockets Layer (SSL). In addition, firewall rules at your company can control whether devices running at your company can open connections to a DB instance. For more information on VPCs, see Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281).**

- **To authenticate logins and permissions for an Amazon Aurora DB cluster, you can take either of the following approaches, or a combination of them.**

  - **You can take the same approach as with a stand-alone DB instance of MySQL or PostgreSQL.**

    Techniques for authenticating logins and permissions for stand-alone DB instances of MySQL or PostgreSQL, such as using SQL commands or modifying database schema tables, also work with Aurora. For more information, see Security with Amazon Aurora MySQL (p. 637) or Security with Amazon Aurora PostgreSQL (p. 997).

  - **You can also use IAM database authentication for Aurora MySQL.**

    With IAM database authentication, you authenticate to your Aurora MySQL DB cluster by using an IAM user or IAM role and an authentication token. An **authentication token** is a unique value that is generated using the Signature Version 4 signing process. By using IAM database authentication, you can use the same credentials to control access to your AWS resources and your databases. For more information, see IAM database authentication (p. 1238).
For information about configuring security, see Security in Amazon Aurora (p. 1205).

Using SSL with Aurora DB clusters

Amazon Aurora DB clusters support Secure Sockets Layer (SSL) connections from applications using the same process and public key as Amazon RDS DB instances. For more information, see Security with Amazon Aurora MySQL (p. 637), Security with Amazon Aurora PostgreSQL (p. 997), or Using TLS/SSL with Aurora Serverless v1 (p. 137).

High availability for Amazon Aurora

The Amazon Aurora architecture involves separation of storage and compute. Aurora includes some high availability features that apply to the data in your DB cluster. The data remains safe even if some or all of the DB instances in the cluster become unavailable. Other high availability features apply to the DB instances. These features help to make sure that one or more DB instances are ready to handle database requests from your application.

Topics
- High availability for Aurora data (p. 55)
- High availability for Aurora DB instances (p. 55)
- High availability across AWS Regions with Aurora global databases (p. 56)
- Fault tolerance for an Aurora DB cluster (p. 56)

High availability for Aurora data

Aurora stores copies of the data in a DB cluster across multiple Availability Zones in a single AWS Region. Aurora stores these copies regardless of whether the instances in the DB cluster span multiple Availability Zones. For more information on Aurora, see Managing an Amazon Aurora DB cluster (p. 322).

When data is written to the primary DB instance, Aurora synchronously replicates the data across Availability Zones to six storage nodes associated with your cluster volume. Doing so provides data redundancy, eliminates I/O freezes, and minimizes latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against failure and Availability Zone disruption. For more information on Availability Zones, see Regions and Availability Zones (p. 5).

High availability for Aurora DB instances

For a cluster using single-master replication, after you create the primary instance, you can create up to 15 read-only Aurora Replicas. The Aurora Replicas are also known as reader instances.

During day-to-day operations, you can offload some of the work for read-intensive applications by using the reader instances to process SELECT queries. When a problem affects the primary instance, one of these reader instances takes over as the primary instance. This mechanism is known as failover. Many Aurora features apply to the failover mechanism. For example, Aurora detects database problems and activates the failover mechanism automatically when necessary. Aurora also has features that reduce the time for failover to complete. Doing so minimizes the time that the database is unavailable for writing during a failover.

To use a connection string that stays the same even when a failover promotes a new primary instance, you connect to the cluster endpoint. The cluster endpoint always represents the current primary
instance in the cluster. For more information about the cluster endpoint, see Amazon Aurora connection management (p. 24).

**Tip**

Within each AWS Region, Availability Zones represent locations that are distinct from each other to provide isolation in case of outages. We recommend that you distribute the primary instance and reader instances in your DB cluster over multiple Availability Zones to improve the availability of your DB cluster. That way, an issue that affects an entire Availability Zone doesn't cause an outage for your cluster.

You can set up a Multi-AZ cluster by making a simple choice when you create the cluster. The choice is simple whether you use the AWS Management Console, the AWS CLI, or the Amazon RDS API. You can also make an existing Aurora cluster into a Multi-AZ cluster by adding a new reader instance and specifying a different Availability Zone.

**High availability across AWS Regions with Aurora global databases**

For high availability across multiple AWS Regions, you can set up Aurora global databases. Each Aurora global database spans multiple AWS Regions, enabling low latency global reads and disaster recovery from outages across an AWS Region. Aurora automatically handles replicating all data and updates from the primary AWS Region to each of the secondary Regions. For more information, see Using Amazon Aurora global databases (p. 206).

**Fault tolerance for an Aurora DB cluster**

An Aurora DB cluster is fault tolerant by design. The cluster volume spans multiple Availability Zones in a single AWS Region, and each Availability Zone contains a copy of the cluster volume data. This functionality means that your DB cluster can tolerate a failure of an Availability Zone without any loss of data and only a brief interruption of service.

If the primary instance in a DB cluster using single-master replication fails, Aurora automatically fails over to a new primary instance in one of two ways:

- By promoting an existing Aurora Replica to the new primary instance
- By creating a new primary instance

If the DB cluster has one or more Aurora Replicas, then an Aurora Replica is promoted to the primary instance during a failure event. A failure event results in a brief interruption, during which read and write operations fail with an exception. However, service is typically restored in less than 120 seconds, and often less than 60 seconds. To increase the availability of your DB cluster, we recommend that you create at least one or more Aurora Replicas in two or more different Availability Zones.

You can customize the order in which your Aurora Replicas are promoted to the primary instance after a failure by assigning each replica a priority. Priorities range from 0 for the first priority to 15 for the last priority. If the primary instance fails, Amazon RDS promotes the Aurora Replica with the better priority to the new primary instance. You can modify the priority of an Aurora Replica at any time. Modifying the priority doesn't trigger a failover.

More than one Aurora Replica can share the same priority, resulting in promotion tiers. If two or more Aurora Replicas share the same priority, then Amazon RDS promotes the replica that is largest in size. If two or more Aurora Replicas share the same priority and size, then Amazon RDS promotes an arbitrary replica in the same promotion tier.

If the DB cluster doesn't contain any Aurora Replicas, then the primary instance is recreated during a failure event. A failure event results in an interruption during which read and write operations fail with an exception. Service is restored when the new primary instance is created, which typically takes less
Amazon Aurora User Guide for Aurora

Replication with Aurora

There are several replication options with Aurora. Each Aurora DB cluster has built-in replication between multiple DB instances in the same cluster. You can also set up replication with your Aurora cluster as the source or the target. When you replicate data into or out of an Aurora cluster, you can choose between built-in features such as Aurora global databases or the traditional replication mechanisms for the MySQL or PostgreSQL DB engines. You can choose the appropriate options based on which one provides the right combination of high availability, convenience, and performance for your needs. The following sections explain how and when to choose each technique.

Topics
- Aurora Replicas (p. 57)
- Replication with Aurora MySQL (p. 58)
- Replication with Aurora PostgreSQL (p. 58)

Aurora Replicas

When you create a second, third, and so on DB instance in an Aurora provisioned DB cluster, Aurora automatically sets up replication from the writer DB instance to all the other DB instances. These other DB instances are read-only and are known as Aurora Replicas. We also refer to them as reader instances when discussing the ways that you can combine writer and reader DB instances within a cluster.

Aurora Replicas have two main purposes. You can issue queries to them to scale the read operations for your application. You typically do so by connecting to the reader endpoint of the cluster. That way, Aurora can spread the load for read-only connections across as many Aurora Replicas as you have in the cluster. Aurora Replicas also help to increase availability. If the writer instance in a cluster becomes unavailable, Aurora automatically promotes one of the reader instances to take its place as the new writer.

An Aurora DB cluster can contain up to 15 Aurora Replicas. The Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region.

The data in your DB cluster has its own high availability and reliability features, independent of the DB instances in the cluster. If you aren't familiar with Aurora storage features, see Overview of Aurora storage (p. 51). The DB cluster volume is physically made up of multiple copies of the data for the DB cluster. The primary instance and the Aurora Replicas in the DB cluster all see the data in the cluster volume as a single logical volume.

As a result, all Aurora Replicas return the same data for query results with minimal replica lag. This lag is usually much less than 100 milliseconds after the primary instance has written an update. Replica lag varies depending on the rate of database change. That is, during periods where a large amount of write operations occur for the database, you might see an increase in replica lag.

Aurora Replicas work well for read scaling because they are fully dedicated to read operations on your cluster volume. Write operations are managed by the primary instance. Because the cluster volume is shared among all DB instances in your DB cluster, minimal additional work is required to replicate a copy of the data for each Aurora Replica.
To increase availability, you can use Aurora Replicas as failover targets. That is, if the primary instance fails, an Aurora Replica is promoted to the primary instance. There is a brief interruption during which read and write requests made to the primary instance fail with an exception, and the Aurora Replicas are rebooted. Promoting an Aurora Replica this way is much faster than recreating the primary instance. If your Aurora DB cluster doesn’t include any Aurora Replicas, then your DB cluster will be unavailable for the duration it takes your DB instance to recover from the failure event. For high-availability scenarios, we recommend that you create one or more Aurora Replicas. These should be of the same DB instance class as the primary instance and in different Availability Zones for your Aurora DB cluster. For more information on Aurora Replicas as failover targets, see Fault tolerance for an Aurora DB cluster (p. 56).

**Note**
You can't create an encrypted Aurora Replica for an unencrypted Aurora DB cluster. You can't create an unencrypted Aurora Replica for an encrypted Aurora DB cluster.

**Tip**
You can use Aurora Replicas within an Aurora cluster as your only form of replication to keep your data highly available. You can also combine the built-in Aurora replication with the other types of replication. Doing so can help to provide an extra level of high availability and geographic distribution of your data.

For details on how to create an Aurora Replica, see Adding Aurora replicas to a DB cluster (p. 345).

### Replication with Aurora MySQL

In addition to Aurora Replicas, you have the following options for replication with Aurora MySQL:

- Aurora MySQL DB clusters in different AWS Regions.
  - You can replicate data across multiple Regions by using an Aurora global database. For details, see High availability across AWS Regions with Aurora global databases (p. 56)
  - You can create a single Aurora Read Replica of an Aurora MySQL DB cluster in a different AWS Region, by using MySQL binary log (binlog) replication.
  - Two Aurora MySQL DB clusters in the same region, by using MySQL binary log (binlog) replication.
  - An Amazon RDS MySQL DB instance as the master and an Aurora MySQL DB cluster, by creating an Aurora Read Replica of an Amazon RDS MySQL DB instance. Typically, you use this approach for migration to Aurora MySQL, rather than for ongoing replication.

For more information about replication with Aurora MySQL, see Single-master replication with Amazon Aurora MySQL (p. 730).

### Replication with Aurora PostgreSQL

In addition to Aurora Replicas, you have the following options for replication with Aurora PostgreSQL:

- An Amazon RDS PostgreSQL DB instance as the source of data and an Aurora PostgreSQL DB cluster, by creating an Aurora Replica of an Amazon RDS PostgreSQL DB instance.
- Two Aurora PostgreSQL DB clusters in the same region, by using PostgreSQL's logical replication feature.
- An Aurora primary DB cluster in one Region and up to five read-only secondary DB clusters in different Regions by using an Aurora global database. Aurora PostgreSQL doesn't support cross-region Aurora Replicas. However, you can use Aurora global database to scale your Aurora PostgreSQL DB cluster's Read capabilities to more than one AWS Region and to meet availability goals. For more information, see Using Amazon Aurora global databases (p. 206).

For more information about replication with Aurora PostgreSQL, see Replication with Amazon Aurora PostgreSQL (p. 1034).
DB instance billing for Aurora

Amazon RDS instances in an Aurora cluster are billed based on the following components:

- **DB instance hours (per hour)** – Based on the DB instance class of the DB instance (for example, db.t2.small or db.m4.large). Pricing is listed on a per-hour basis, but bills are calculated down to the second and show times in decimal form. RDS usage is billed in one second increments, with a minimum of 10 minutes. For more information, see DB instance classes (p. 46).

- **I/O requests (per 1 million requests per month)** – Total number of storage I/O requests that you have made in a billing cycle.

- **Backup storage (per GiB per month)** – **Backup storage** is the storage that is associated with automated database backups and any active database snapshots that you have taken. Increasing your backup retention period or taking additional database snapshots increases the backup storage consumed by your database. Per second billing doesn't apply to backup storage (metered in GB-month).

  For more information, see Backing up and restoring an Amazon Aurora DB cluster (p. 414).

- **Data transfer (per GB)** – Data transfer in and out of your DB instance from or to the internet and other AWS Regions.

Amazon RDS provides the following purchasing options to enable you to optimize your costs based on your needs:

- **On-Demand Instances** – Pay by the hour for the DB instance hours that you use. Pricing is listed on a per-hour basis, but bills are calculated down to the second and show times in decimal form. RDS usage is now billed in one second increments, with a minimum of 10 minutes.

- **Reserved Instances** – Reserve a DB instance for a one-year or three-year term and get a significant discount compared to the on-demand DB instance pricing. With Reserved Instance usage, you can launch, delete, start, or stop multiple instances within an hour and get the Reserved Instance benefit for all of the instances.

  For Aurora pricing information, see the Aurora pricing page.

**Topics**

- On-Demand DB instances for Aurora (p. 60)
- Reserved DB instances for Aurora (p. 61)
On-Demand DB instances for Aurora

Amazon RDS on-demand DB instances are billed based on the class of the DB instance (for example, db.t2.small or db.m4.large). For Amazon RDS pricing information, see the Amazon RDS product page.

Billing starts for a DB instance as soon as the DB instance is available. Pricing is listed on a per-hour basis, but bills are calculated down to the second and show times in decimal form. Amazon RDS usage is billed in one-second increments, with a minimum of 10 minutes. In the case of billable configuration change, such as scaling compute or storage capacity, you're charged a 10-minute minimum. Billing continues until the DB instance terminates, which occurs when you delete the DB instance or if the DB instance fails.

If you no longer want to be charged for your DB instance, you must stop or delete it to avoid being billed for additional DB instance hours. For more information about the DB instance states for which you are billed, see DB instance status (p. 481).

Stopped DB instances

While your DB instance is stopped, you're charged for provisioned storage, including Provisioned IOPS. You are also charged for backup storage, including storage for manual snapshots and automated backups within your specified retention window. You aren't charged for DB instance hours.

Multi-AZ DB instances

If you specify that your DB instance should be a Multi-AZ deployment, you're billed according to the Multi-AZ pricing posted on the Amazon RDS pricing page.
Reserved DB instances for Aurora

Using reserved DB instances, you can reserve a DB instance for a one- or three-year term. Reserved DB instances provide you with a significant discount compared to on-demand DB instance pricing. Reserved DB instances are not physical instances, but rather a billing discount applied to the use of certain on-demand DB instances in your account. Discounts for reserved DB instances are tied to instance type and AWS Region.

The general process for working with reserved DB instances is: First get information about available reserved DB instance offerings, then purchase a reserved DB instance offering, and finally get information about your existing reserved DB instances.

Overview of reserved DB instances

When you purchase a reserved DB instance in Amazon RDS, you purchase a commitment to getting a discounted rate, on a specific DB instance type, for the duration of the reserved DB instance. To use an Amazon RDS reserved DB instance, you create a new DB instance just like you do for an on-demand instance. The new DB instance that you create must match the specifications of the reserved DB instance. If the specifications of the new DB instance match an existing reserved DB instance for your account, you are billed at the discounted rate offered for the reserved DB instance. Otherwise, the DB instance is billed at an on-demand rate.

For more information about reserved DB instances, including pricing, see Amazon RDS reserved instances.

Offering types

Reserved DB instances are available in three varieties—No Upfront, Partial Upfront, and All Upfront—that let you optimize your Amazon RDS costs based on your expected usage.

No Upfront

This option provides access to a reserved DB instance without requiring an upfront payment. Your No Upfront reserved DB instance bills a discounted hourly rate for every hour within the term, regardless of usage, and no upfront payment is required. This option is only available as a one-year reservation.

Partial Upfront

This option requires a part of the reserved DB instance to be paid upfront. The remaining hours in the term are billed at a discounted hourly rate, regardless of usage. This option is the replacement for the previous Heavy Utilization option.

All Upfront

Full payment is made at the start of the term, with no other costs incurred for the remainder of the term regardless of the number of hours used.

If you are using consolidated billing, all the accounts in the organization are treated as one account. This means that all accounts in the organization can receive the hourly cost benefit of reserved DB instances that are purchased by any other account. For more information about consolidated billing, see Amazon RDS reserved DB instances in the AWS Billing and Cost Management User Guide.

Size-flexible reserved DB instances

When you purchase a reserved DB instance, one thing that you specify is the instance class, for example db.m4.large. For more information about instance classes, see DB instance classes (p. 46).
If you have a DB instance, and you need to scale it to larger capacity, your reserved DB instance is automatically applied to your scaled DB instance. That is, your reserved DB instances are automatically applied across all DB instance class sizes. Size-flexible reserved DB instances are available for DB instances with the same AWS Region and database engine. Size-flexible reserved DB instances can only scale in their instance class type. For example, a reserved DB instance for a db.m4.large can apply to a db.m4.xlarge, but not to a db.m5.large, because db.m4 and db.m5 are different instance class types.

Reserved DB instance benefits also apply for both Multi-AZ and Single-AZ configurations. Flexibility means that you can move freely between configurations within the same DB instance class type. For example, you can move from a Single-AZ deployment running on one large DB instance (four normalized units) to a Multi-AZ deployment running on two small DB instances (2*2 = 4 normalized units).

Size-flexible reserved DB instances are available for the following Aurora database engines:

- Aurora MySQL
- Aurora PostgreSQL

You can compare usage for different reserved DB instance sizes by using normalized units. For example, one unit of usage on two db.m3.large DB instances is equivalent to eight normalized units of usage on one db.m3.small. The following table shows the number of normalized units for each DB instance size.

<table>
<thead>
<tr>
<th>Instance size</th>
<th>Single-AZ normalized units</th>
<th>Multi-AZ normalized units</th>
</tr>
</thead>
<tbody>
<tr>
<td>micro</td>
<td>0.5</td>
<td>1</td>
</tr>
<tr>
<td>small</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>medium</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>large</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>xlarge</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>2xlarge</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>4xlarge</td>
<td>32</td>
<td>64</td>
</tr>
<tr>
<td>8xlarge</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td>10xlarge</td>
<td>80</td>
<td>160</td>
</tr>
<tr>
<td>12xlarge</td>
<td>96</td>
<td>192</td>
</tr>
<tr>
<td>16xlarge</td>
<td>128</td>
<td>256</td>
</tr>
<tr>
<td>24xlarge</td>
<td>192</td>
<td>384</td>
</tr>
</tbody>
</table>

For example, suppose that you purchase a db.t2.medium reserved DB instance, and you have two running db.t2.small DB instances in your account in the same AWS Region. In this case, the billing benefit is applied in full to both instances.
Alternatively, if you have one `db.t2.large` instance running in your account in the same AWS Region, the billing benefit is applied to 50 percent of the usage of the DB instance.

### Reserved DB instance billing example

The price for a reserved DB instance doesn’t include regular costs associated with storage, backups, and I/O. The following example illustrates the total cost per month for a reserved DB instance:

- An Aurora MySQL reserved Single-AZ `db.r4.large` DB instance class in US East (N. Virginia) at a cost of $0.19 per hour, or $138.70 per month
- Aurora storage at a cost of $0.10 per GiB per month (assume $45.60 per month for this example)
- Aurora I/O at a cost of $0.20 per 1 million requests (assume $20 per month for this example)
- Aurora backup storage at $0.021 per GiB per month (assume $30 per month for this example)

Add all of these options ($138.70 + $45.60 + $20 + $30) with the reserved DB instance, and the total cost per month is $234.30.

If you chose to use an on-demand DB instance instead of a reserved DB instance, an Aurora MySQL Single-AZ `db.r4.large` DB instance class in US East (N. Virginia) costs $0.29 per hour, or $217.50 per month. So, for an on-demand DB instance, add all of these options ($217.50 + $45.60 + $20 + $30), and the total cost per month is $313.10.
Deleting a reserved DB instance

The terms for a reserved DB instance involve a one-year or three-year commitment. You can't cancel a reserved DB instance. However, you can delete a DB instance that is covered by a reserved DB instance discount. The process for deleting a DB instance that is covered by a reserved DB instance discount is the same as for any other DB instance.

Your upfront payment for a reserved DB instance reserves the resources for your use. Because these resources are reserved for you, you are billed for the resources regardless of whether you use them.

If you delete a DB instance that is covered by a reserved DB instance discount, you can launch another DB instance with compatible specifications. In this case, you continue to get the discounted rate during the reservation term (one or three years).

Console

You can use the AWS Management Console to work with reserved DB instances as shown in the following procedures.

To get pricing and information about available reserved DB instance offerings

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Reserved instances.
3. Choose Purchase Reserved DB Instance.
4. For Product description, choose the DB engine and licensing type.
5. For DB instance class, choose the DB instance class.
6. For Multi-AZ deployment, choose whether you want a Multi-AZ deployment.
   
   **Note**
   
   Reserved Amazon Aurora instances always have the Multi-AZ deployment option set to No. When you create an Amazon Aurora DB cluster from your reserved DB instance, the DB cluster is automatically created as Multi-AZ.
7. For Term, choose the length of time you want the DB instance reserved.
8. For Offering type, choose the offering type.

After you select the offering type, you can see the pricing information.

**Important**

Choose Cancel to avoid purchasing the reserved DB instance and incurring any charges.

After you have information about the available reserved DB instance offerings, you can use the information to purchase an offering as shown in the following procedure.

To purchase a reserved DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Reserved instances.
3. Choose **Purchase Reserved DB Instance**.
4. For **Product description**, choose the DB engine and licensing type.
5. For **DB instance class**, choose the DB instance class.
6. For **Multi-AZ deployment**, choose whether you want a Multi-AZ deployment.

   **Note**
   Reserved Amazon Aurora instances always have the **Multi-AZ deployment** option set to **No**. When you create an Amazon Aurora DB cluster from your reserved DB instance, the DB cluster is automatically created as Multi-AZ.

7. For **Term**, choose the length of time you want the DB instance reserved.
8. For **Offering type**, choose the offering type.

   After you choose the offering type, you can see the pricing information, as shown following.
Purchase Reserved DB Instances

Choose from the options below, then enter the number of DB instances you wish to reserve with this order. When you are done, click the Continue button.

Options

Product description
aurora-mysql

DB instance class
db.r4.4xlarge — 16 vCPU, 122 GiB RAM

Multi AZ deployment
Multi-AZ deployment model is not applicable for this database engine and edition

Yes
No

Term
1 year

Offering type
All Upfront

Reserved id (optional)
Optional tag to track your reservation

Number of DB instances
1

Pricing details

One-time payment (per instance)
USD

Total one-time payment*
USD

Usage charges*
USD (hourly)
*Additional taxes may apply

This hourly rate is charged for every hour for each instance in the Reserved Instance term you purchase, regardless of instance usage

Charges for your usage will appear on your monthly bill.

Cancel
Continue
9. (Optional) You can assign your own identifier to the reserved DB instances that you purchase to help you track them. For **Reserved Id**, type an identifier for your reserved DB instance.

10. Choose **Continue**.

The **Purchase Reserved DB Instance** dialog box appears, with a summary of the reserved DB instance attributes that you've selected and the payment due, as shown following.
11. On the confirmation page, review your reserved DB instance. If the information is correct, choose **Purchase** to purchase the reserved DB instance.

   Alternatively, choose **Back** to edit your reserved DB instance.

After you have purchased reserved DB instances, you can get information about your reserved DB instances as shown in the following procedure.

**To get information about reserved DB instances for your AWS account**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the **Navigation** pane, choose **Reserved instances**.

   The reserved DB instances for your account appear. To see detailed information about a particular reserved DB instance, choose that instance in the list. You can then see detailed information about that instance in the detail pane at the bottom of the console.

**AWS CLI**

You can use the AWS CLI to work with reserved DB instances as shown in the following examples.

**Example Get available reserved DB instance offerings**

To get information about available reserved DB instance offerings, call the AWS CLI command `describe-reserved-db-instances-offerings`.

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

This call returns output similar to the following:

<table>
<thead>
<tr>
<th>OFFERING</th>
<th>OfferingId</th>
<th>Class</th>
<th>Multi-AZ</th>
<th>Duration</th>
<th>Fixed Price</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>438012d3-4052-4cc7-b2e3-8d3372e0e706</td>
<td>db.m1.large</td>
<td>y</td>
<td>1y</td>
<td>1820.00 USD</td>
</tr>
<tr>
<td></td>
<td>649fd0c8-cf6d-47a0-bfa6-060f8e75e95f</td>
<td>db.m1.small</td>
<td>n</td>
<td>1y</td>
<td>227.50 USD</td>
</tr>
<tr>
<td></td>
<td>123456cd-ab1c-47a0-bfa6-12345667232f</td>
<td>db.m1.small</td>
<td>n</td>
<td>1y</td>
<td>162.00 USD</td>
</tr>
<tr>
<td></td>
<td>123456cd-ab1c-47a0-bfa6-12345667232d</td>
<td>db.m1.large</td>
<td>y</td>
<td>1y</td>
<td>700.00 USD</td>
</tr>
<tr>
<td></td>
<td>123456cd-ab1c-47a0-bfa6-12345667232e</td>
<td>db.m1.xlarge</td>
<td>n</td>
<td>1y</td>
<td>4242.00 USD</td>
</tr>
</tbody>
</table>

After you have information about the available reserved DB instance offerings, you can use the information to purchase an offering as shown in the following example.

**Example Purchase a reserved DB instance**

To purchase a reserved DB instance, use the AWS CLI command `purchase-reserved-db-instances-offering` with the following parameters:
• `--reserved-db-instances-offering-id` – the id of the offering that you want to purchase. See the preceding example to get the offering ID.
• `--reserved-db-instance-id` – you can assign your own identifier to the reserved DB instances that you purchase to help you track them.

The following example purchases the reserved DB instance offering with ID `649fd0c8-cf6d-47a0-bfa6-060f8e75e95f`, and assigns the identifier of `MyReservation`.

For Linux, macOS, or Unix:
```
aws rds purchase-reserved-db-instances-offering \
  --reserved-db-instances-offering-id 649fd0c8-cf6d-47a0-bfa6-060f8e75e95f \
  --reserved-db-instance-id MyReservation
```

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

The command returns output similar to the following:

<table>
<thead>
<tr>
<th>ReservationId</th>
<th>Class</th>
<th>Multi-AZ</th>
<th>Start Time</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyReservation</td>
<td>db.m1.small</td>
<td>y</td>
<td>2011-12-09T23:37:44.720Z</td>
<td>1y</td>
</tr>
<tr>
<td>455.00 USD</td>
<td>0.092 USD</td>
<td>1</td>
<td>payment-pending</td>
<td>mysql</td>
</tr>
<tr>
<td>Partial</td>
<td>Upfront</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

After you have purchased reserved DB instances, you can get information about your reserved DB instances as shown in the following example.

**Example Get your reserved DB instances**

To get information about reserved DB instances for your AWS account, call the AWS CLI command `describe-reserved-db-instances`.

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

The command returns output similar to the following:

<table>
<thead>
<tr>
<th>ReservationId</th>
<th>Class</th>
<th>Multi-AZ</th>
<th>Start Time</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyReservation</td>
<td>db.m1.small</td>
<td>y</td>
<td>2011-12-09T23:37:44.720Z</td>
<td>1y</td>
</tr>
<tr>
<td>455.00 USD</td>
<td>0.092 USD</td>
<td>1</td>
<td>retired</td>
<td>mysql</td>
</tr>
<tr>
<td>Partial</td>
<td>Upfront</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**RDS API**

You can use the RDS API to work with reserved DB instances as shown in the following examples.

**Example Get available reserved DB instance offerings**

To get information about available reserved DB instance offerings, call the Amazon RDS API function `DescribeReservedDBInstancesOfferings`.

```
https://rds.us-east-1.amazonaws.com/
  ?Action=DescribeReservedDBInstancesOfferings
  &SignatureMethod=HmacSHA256
  &SignatureVersion=4
```

69
After you have information about the available reserved DB instance offerings, you can use the information to purchase an offering as shown in the following example.

**Example Purchase a reserved DB instance**

To purchase a reserved DB instance, call the Amazon RDS API operation `PurchaseReservedDBInstancesOffering` with the following parameters:

- `--reserved-db-instances-offering-id` – the id of the offering that you want to purchase. See the preceding example to get the offering ID.
- `--reserved-db-instance-id` – you can assign your own identifier to the reserved DB instances that you purchase to help you track them.

The following example purchases the reserved DB instance offering with ID `649fd0c8-cf6d-47a0-bfa6-060f8e75e95f`, and assigns the identifier of `MyReservation`.

```
```
This call returns output similar to the following:

```xml
  <PurchaseReservedDBInstancesOfferingResult>
    <ReservedDBInstance>
      <OfferingType>Partial Upfront</OfferingType>
      <CurrencyCode>USD</CurrencyCode>
      <RecurringCharges/>
      <ProductDescription>mysql</ProductDescription>
      <ReservedDBInstancesOfferingId>649fd0c8-cf6d-47a0-bfa6-060f8e75e95f</ReservedDBInstancesOfferingId>
      <MultiAZ>true</MultiAZ>
      <State>payment-pending</State>
      <ReservedDBInstanceId>MyReservation</ReservedDBInstanceId>
      <DBInstanceCount>10</DBInstanceCount>
      <StartTime>2011-12-18T23:24:56.577Z</StartTime>
      <Duration>31536000</Duration>
      <FixedPrice>123.0</FixedPrice>
      <UsagePrice>0.123</UsagePrice>
      <DBInstanceClass>db.m1.small</DBInstanceClass>
    </ReservedDBInstance>
  </PurchaseReservedDBInstancesOfferingResult>
  <ResponseMetadata>
    <RequestId>7f099901-29cf-11e1-bd06-6fe008f046c3</RequestId>
  </ResponseMetadata>
</PurchaseReservedDBInstancesOfferingResponse>
```

After you have purchased reserved DB instances, you can get information about your reserved DB instances as shown in the following example.

### Example Get your reserved DB instances

To get information about reserved DB instances for your AWS account, call the Amazon RDS API operation `DescribeReservedDBInstances`.

```xml
https://rds.us-west-2.amazonaws.com/?Action=DescribeReservedDBInstances
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&Version=2014-09-01
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140420/us-west-2/rds/aws4_request
&X-Amz-Date=20140420T162211Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=60f392e56f75b6b10d210aee6f72ad78d5c14b0a8449a0f77475e6e12b6e9
```

The API returns output similar to the following:
  <DescribeReservedDBInstancesResult>
    <ReservedDBInstances>
      <ReservedDBInstance>
        <OfferingType>Partial Upfront</OfferingType>
        <CurrencyCode>USD</CurrencyCode>
        <RecurringCharges/>
        <ProductDescription>mysql</ProductDescription>
        <ReservedDBInstancesOfferingId>649fd0c8-cf6d-47a0-bfa6-060f8e75e95f</ReservedDBInstancesOfferingId>
        <MultiAZ>false</MultiAZ>
        <State>payment-failed</State>
        <ReservedDBInstanceId>MyReservation</ReservedDBInstanceId>
        <DBInstanceCount>1</DBInstanceCount>
        <StartTime>2010-12-15T00:25:14.131Z</StartTime>
        <Duration>31536000</Duration>
        <FixedPrice>227.5</FixedPrice>
        <UsagePrice>0.046</UsagePrice>
        <DBInstanceClass>db.m1.small</DBInstanceClass>
      </ReservedDBInstance>
      <ReservedDBInstance>
        <OfferingType>Partial Upfront</OfferingType>
        <CurrencyCode>USD</CurrencyCode>
        <RecurringCharges/>
        <ProductDescription>mysql</ProductDescription>
        <ReservedDBInstancesOfferingId>649fd0c8-cf6d-47a0-bfa6-060f8e75e95f</ReservedDBInstancesOfferingId>
        <MultiAZ>false</MultiAZ>
        <State>payment-failed</State>
        <ReservedDBInstanceId>MyReservation</ReservedDBInstanceId>
        <DBInstanceCount>1</DBInstanceCount>
        <StartTime>2010-12-15T01:07:22.275Z</StartTime>
        <Duration>31536000</Duration>
        <FixedPrice>227.5</FixedPrice>
        <UsagePrice>0.046</UsagePrice>
        <DBInstanceClass>db.m1.small</DBInstanceClass>
      </ReservedDBInstance></ReservedDBInstances>
</DescribeReservedDBInstancesResult>
<ResponseMetadata>
  <RequestId>23400d50-2978-11e1-9e6d-771388d6ed6b</RequestId>
</ResponseMetadata>
</DescribeReservedDBInstancesResponse>
Setting up your environment for Amazon Aurora

Before you use Amazon Aurora for the first time, complete the following tasks:

1. Sign up for AWS (p. 73)
2. Create an IAM user (p. 73)
3. Determine requirements (p. 75)
4. Provide access to the DB cluster in the VPC by creating a security group (p. 76)

Sign up for AWS

When you sign up for Amazon RDS (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon RDS. You are charged only for the services that you use.

With Amazon RDS, you pay only for the resources you use. The Amazon RDS DB cluster that you create is live (not running in a sandbox). You incur the standard Amazon RDS usage fees for the cluster until you terminate it. For more information about Amazon RDS usage rates, see the Amazon RDS product page. If you are a new AWS customer, you can get started with Amazon RDS for free; for more information, see AWS free usage tier.

If you have an AWS account already, skip to the next task. If you don't have an AWS account, use the following procedure to create one.

To create an AWS account

2. Follow the online instructions.
   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Note your AWS account number, because you'll need it for the next task.

Create an IAM user

Services in AWS, such as Amazon RDS, require that you provide credentials when you access them, so that the service can determine whether you have permission to access its resources. The console requires your password. You can create access keys for your AWS account to access the command line interface or API. However, we don't recommend that you access AWS using the credentials for your AWS account; we recommend that you use AWS Identity and Access Management (IAM) instead. Create an IAM user, and then add the user to an IAM group with administrative permissions or grant this user administrative permissions. You can then access AWS using a special URL and the credentials for the IAM user.

If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console.
To create an administrator user for yourself and add the user to an administrators group (console)

1. Sign in to the IAM console as the account owner by choosing Root user and entering your AWS account email address. On the next page, enter your password.

   **Note**
   We strongly recommend that you adhere to the best practice of using the Administrator IAM user below and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.

2. In the navigation pane, choose Users and then choose Add user.

3. For User name, enter Administrator.

4. Select the check box next to AWS Management Console access. Then select Custom password, and then enter your new password in the text box.

5. (Optional) By default, AWS requires the new user to create a new password when first signing in. You can clear the check box next to User must create a new password at next sign-in to allow the new user to reset their password after they sign in.

6. Choose Next: Permissions.

7. Under Set permissions, choose Add user to group.

8. Choose Create group.

9. In the Create group dialog box, for Group name enter Administrators.

10. Choose Filter policies, and then select AWS managed -job function to filter the table contents.

11. In the policy list, select the check box for AdministratorAccess. Then choose Create group.

   **Note**
   You must activate IAM user and role access to Billing before you can use the AdministratorAccess permissions to access the AWS Billing and Cost Management console. To do this, follow the instructions in step 1 of the tutorial about delegating access to the billing console.

12. Back in the list of groups, select the check box for your new group. Choose Refresh if necessary to see the group in the list.

13. Choose Next: Tags.

14. (Optional) Add metadata to the user by attaching tags as key-value pairs. For more information about using tags in IAM, see Tagging IAM entities in the IAM User Guide.

15. Choose Next: Review to see the list of group memberships to be added to the new user. When you are ready to proceed, choose Create user.

You can use this same process to create more groups and users and to give your users access to your AWS account resources. To learn about using policies that restrict user permissions to specific AWS resources, see Access management and Example policies.

To sign in as this new IAM user, sign out of the AWS console, then use the following URL, where your_aws_account_id is your AWS account number without the hyphens (for example, if your AWS account number is 1234-5678-9012, your AWS account ID is 123456789012):

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Enter the IAM user name and password that you just created. When you’re signed in, the navigation bar displays “your_user_name @ your_aws_account_id”.

If you don’t want the URL for your sign-in page to contain your AWS account ID, you can create an account alias. From the IAM dashboard, choose Customize and enter an alias, such as your company name. To sign in after you create an account alias, use the following URL:
Determine requirements

The basic building block of Aurora is the DB cluster. One or more DB instances can belong to a DB cluster. A DB cluster provides a network address called the Cluster Endpoint. Your applications connect to the cluster endpoint exposed by the DB cluster whenever they need to access the databases created in that DB cluster. The information you specify when you create the DB cluster controls configuration elements such as memory, database engine and version, network configuration, security, and maintenance periods.

You must know your DB cluster and network needs before you create a security group and before you create a DB cluster. For example, you must know the following:

- What are the memory and processor requirements for your application or service? You will use these settings when you determine what DB instance class you will use when you create your DB cluster. For specifications about DB instance classes, see DB instance classes (p. 46).

- Your DB cluster is in a virtual private cloud (VPC). Security group rules must be configured to connect to a DB cluster. The follow list describes the rules for each VPC option:
  - **Default VPC** — If your AWS account has a default VPC in the region, that VPC is configured to support DB clusters. If you specify the default VPC when you create the DB cluster:
    - You must create a VPC security group that authorizes connections from the application or service to the Aurora DB cluster with the database. Note that you must use the Amazon EC2 API or the Security Group option on the VPC Console to create VPC security groups. For information, see Step 4: Create a VPC security group (p. 1297).
    - You must specify the default DB subnet group. If this is the first DB cluster you have created in the region, Amazon RDS will create the default DB subnet group when it creates the DB cluster.
  - **User-defined VPC** — If you want to specify a user-defined VPC when you create a DB cluster:
    - You must create a VPC security group that authorizes connections from the application or service to the Aurora DB cluster with the database. Note that you must use the Amazon EC2 API or the Security Group option on the VPC Console to create VPC security groups. For information, see Step 4: Create a VPC security group (p. 1297).
    - The VPC must meet certain requirements in order to host DB clusters, such as having at least two subnets, each in a separate availability zone. For information, see Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281).
    - You must specify a DB subnet group that defines which subnets in that VPC can be used by the DB cluster. For information, see the DB Subnet Group section in Working with a DB instance in a VPC (p. 1292).

- Do you need failover support? On Aurora, a Multi-AZ deployment creates a primary instance and Aurora Replicas. You can configure the primary instance and Aurora Replicas to be in different Availability Zones for failover support. We recommend Multi-AZ deployments for production workloads to maintain high availability. For development and test purposes, you can use a non-Multi-AZ deployment. For more information, see High availability for Amazon Aurora (p. 55).

- Does your AWS account have policies that grant the permissions needed to perform Amazon RDS operations? If you are connecting to AWS using IAM credentials, your IAM account must have IAM policies that grant the permissions required to perform Amazon RDS operations. For more information, see Identity and access management in Amazon Aurora (p. 1222).

- What TCP/IP port will your database be listening on? The firewall at some companies may block connections to the default port for your database engine. If your company firewall blocks the default
Port, choose another port for the new DB cluster. Note that once you create a DB cluster that listens on a port you specify, you can change the port by modifying the DB cluster.

- What region do you want your database in? Having the database close in proximity to the application or web service could reduce network latency.

Once you have the information you need to create the security group and the DB cluster, continue to the next step.

**Provide access to the DB cluster in the VPC by creating a security group**

Your DB cluster will most likely be created in a VPC. Security groups provide access to the DB cluster in the VPC. They act as a firewall for the associated DB cluster, controlling both inbound and outbound traffic at the cluster level. DB clusters are created by default with a firewall and a default security group that prevents access to the DB cluster. You must therefore add rules to a security group that enable you to connect to your DB cluster. Use the network and configuration information you determined in the previous step to create rules to allow access to your DB cluster.

The security group you need to create is a **VPC security group**, unless you have a legacy DB cluster not in a VPC that requires a **DB security group**. If you created your AWS account after March 2013, chances are very good that you have a default VPC, and your DB cluster will be created in that VPC. DB clusters in a VPC require that you add rules to a VPC security group to allow access to the cluster.

For example, if you have an application that will access a database on your DB cluster in a VPC, you must add a Custom TCP rule that specifies the port range and IP addresses that application will use to access the database. If you have an application on an Amazon EC2 cluster, you can use the VPC security group you set up for the Amazon EC2 cluster.

**To create a VPC security group**

2. In the top right corner of the AWS Management Console, select the region in which you want to create the VPC security group and the DB cluster. In the list of Amazon VPC resources for that region, it should show that you have at least one VPC and several Subnets. If it does not, you do not have a default VPC in that region.
3. In the navigation pane, choose **Security Groups**.
4. Choose **Create security group**.
5. On the **Create Security Group** page, type the **Security group name** and **Description**. Select the **VPC** that you want to create your DB cluster in. Choose **Create**.
6. Select the VPC security group that you created. The details pane at the bottom of the console window displays the details for the security group, and tabs for working with inbound and outbound rules. Choose the **Inbound Rules** tab.
7. On the **Inbound Rules** tab, choose **Edit rules**, and then choose **Add rule**. From the **Type** list, select **Custom TCP Rule**. Type the port value you will use for your DB cluster in **Port Range**, and then type the IP address range (CIDR value) from where you will access the cluster, or select a security group name in **Source**.
8. If you need to add more IP addresses or different port ranges, choose **Add Rule**.
9. Choose **Save rules**.
10. If necessary, you can use the **Outbound Rules** tab to add rules for outbound traffic.
You will use the VPC security group you just created as the security group for your DB cluster when you create it.

Finally, a quick note about VPC subnets: If you use a default VPC, a default subnet group spanning all of the VPC’s subnets has already been created for you. When you create a DB cluster, you can select the default VPC and use default for the DB Subnet Group.

Once you have completed the setup requirements, you can use your requirements and the security group you created to launch a DB cluster. For information on creating a DB cluster, see the relevant documentation in the following table:

After setting up, you can create a test Amazon Aurora DB cluster. For instructions, see Getting started with Amazon Aurora (p. 78).
Getting started with Amazon Aurora

This section shows you how to create and connect to an Aurora DB cluster using Amazon RDS.

These procedures are tutorials that demonstrate the basics of getting started with Aurora. Subsequent sections introduce more advanced Aurora concepts and procedures, such as the different kinds of endpoints and how to scale Aurora clusters up and down.

**Important**
You must complete the tasks in the Setting up your environment for Amazon Aurora (p. 73) section before you can create a DB cluster.

**Topics**
- Creating a DB cluster and connecting to a database on an Aurora MySQL DB cluster (p. 78)
- Creating a DB cluster and connecting to a database on an Aurora PostgreSQL DB cluster (p. 87)
- Tutorial: Create a web server and an Amazon Aurora DB cluster (p. 99)

Creating a DB cluster and connecting to a database on an Aurora MySQL DB cluster

The easiest way to create an Aurora MySQL DB cluster is to use the Amazon RDS console. After you create the DB cluster, you can use standard MySQL utilities, such as MySQL Workbench, to connect to a database on the DB cluster.

**Topics**
- Create an Aurora MySQL DB cluster (p. 78)
- Connect to an instance in a DB cluster (p. 85)
- Delete the sample DB cluster, DB subnet group, and VPC (p. 87)

Create an Aurora MySQL DB cluster

Before you create a DB cluster, you must first have a virtual private cloud (VPC) based on the Amazon VPC service and an Amazon RDS DB subnet group. Your VPC must have at least one subnet in each of at least two Availability Zones. You can use the default VPC for your AWS account, or you can create your own VPC. The Amazon RDS console makes it easy for you to create your own VPC for use with Amazon Aurora or use an existing VPC with your Aurora DB cluster.

If you want to create a VPC and DB subnet group for use with your Aurora DB cluster yourself, rather than having Amazon RDS create the VPC and DB subnet group for you, then follow the instructions in How to create a VPC for use with Amazon Aurora (p. 1281). Otherwise, follow the instructions in this topic to create your DB cluster and have Amazon RDS create a VPC and DB subnet group for you.

**Note**
A new console interface is available for database creation. Choose either the New Console or the Original Console instructions based on the console that you are using. The New Console instructions are open by default.
New console

You can create an Aurora with MySQL compatibility DB cluster with the AWS Management Console with Easy Create enabled or disabled. With Easy Create enabled, you specify only the DB engine type, DB instance size, and DB instance identifier. Easy Create uses the default setting for other configuration options. With Easy Create disabled, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

Note
For this example, Easy Create is enabled. For information about creating an Aurora MySQL DB cluster with Easy Create not enabled, see Creating an Amazon Aurora DB cluster (p. 118).

To create an Aurora MySQL DB cluster with Easy Create enabled

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region in which you want to create the DB instance.
   
   Aurora is not available in all AWS Regions. For a list of AWS Regions where Aurora is available, see Region availability (p. 6).
3. In the navigation pane, choose Databases.
4. Choose Create database and make sure that Easy Create is chosen.

5. For Engine type, choose Amazon Aurora.
6. For Edition, choose Amazon Aurora with MySQL 5.6 compatibility.
7. For DB instance size, choose Dev/Test.
8. For DB cluster identifier, enter a name for the DB cluster, or leave the default name.
9. For Master username, enter a name for the user, or leave the default name.

The Create database page should look similar to the following image:
Create database

Choose a database creation method

- Standard Create
  You set all of the configuration options, including ones for availability, security, backups, and maintenance.

- Easy Create
  Use recommended best-practice configuration options. Some configuration options can be changed after the database is created.

Configuration

Engine type

- Amazon Aurora
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft SQL Server

Edition

- Amazon Aurora with MySQL 5.6 compatibility
- Amazon Aurora with PostgreSQL compatibility

DB instance size

- Production
  - db.r5.2xlarge
  - 8 vCPUs
  - 64 GiB RAM

- Dev/Test
  - db.r5.large
  - 2 vCPUs
  - 16 GiB RAM

- Serverless
  - 4-64 GiB RAM
10. To use an automatically generated password for the DB cluster, make sure that the **Auto generate a password** is chosen.

   To enter your password, clear the **Auto generate a password** check box, and then enter the same password in **Master password** and **Confirm password**.

11. (Optional) Open **View default settings for Easy create**.

![View default settings for Easy create]

   You can examine the default settings used when **Easy Create** is enabled. If you want to change one or more settings during database creation, choose **Standard Create** to set them. The **Editable after database creation** column shows which options you can change after database creation. To change a setting with **No** in that column, use **Standard Create**. For settings with **Yes** in that column, you can either use **Standard Create** or modify the DB instance after it’s created to change the setting.

12. Choose **Create database**.

   If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

   To view the user name and password for the DB instance, choose **View credential details**.

![Creating database database-1]

   To connect to the DB instance as the master user, use the user name and password that appear.

   **Important**
   
   You can't view the master user password again. If you don't record it, you might have to change it. If you need to change the master user password after the DB instance is available, you can modify the DB instance to do so. For more information about modifying a DB instance, see **Modifying an Amazon Aurora DB cluster** (p. 327).

13. For **Databases**, choose the name of the new Aurora MySQL DB cluster.

   On the RDS console, the details for new DB cluster appear. The DB cluster and its DB instance have a status of **creating** until the DB cluster is ready to use. When the state changes to **available** for both, you can connect to the DB cluster. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new DB cluster is available.
Amazon Aurora User Guide for Aurora
Create an Aurora MySQL DB cluster

Original console

To launch an Aurora MySQL DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.

2. In the top-right corner of the AWS Management Console, choose the AWS Region that you want to create your DB cluster in. For a list of AWS Regions where Aurora is available, see Region availability (p. 6).

3. In the navigation pane, choose Databases.

   If the navigation pane is closed, choose the menu icon at the top left to open it.

4. Choose Create database to open the Select engine page.

5. On the Select engine page, choose Amazon Aurora and choose the MySQL-compatible edition.
6. Choose Next.

7. Set the following values on the Specify DB details page:
   - **DB instance class**: `db.r4.large`
   - **DB instance identifier**: `gs-db-instance1`
   - **Master username**: Using alphanumeric characters, type a user name, used to log on to your DB instances in the DB cluster.
   - **Master password** and **Confirm password**: Type a password in the Master Password box that contains from 8 to 41 printable ASCII characters (excluding /,", and @) for your user password, used to log on to your database. Then type the password again in the Confirm Password box.
8. Choose Next and set the following values on the Configure Advanced Settings page:

- **Virtual Private Cloud (VPC):** If you have an existing VPC, then you can use that VPC with your Amazon Aurora DB cluster by choosing your VPC identifier, for example `vpc-a464d1c1`. For information on using an existing VPC, see How to create a VPC for use with Amazon Aurora (p. 1281).

Otherwise, you can choose to have Amazon RDS create a VPC for you by choosing Create a new VPC. This example uses the Create a new VPC option.
• **Subnet group:** If you have an existing subnet group, then you can use that subnet group with your Amazon Aurora DB cluster by choosing your subnet group identifier, for example, `gs-subnet-group1`.

Otherwise, you can choose to have Amazon RDS create a subnet group for you by choosing **Create a new subnet group**. This example uses the **Create a new subnet group** option.

• **Public accessibility:** Yes

  **Note**
  Your production DB cluster might not need to be in a public subnet, because only your application servers require access to your DB cluster. If your DB cluster doesn't need to be in a public subnet, set **Publicly Accessible** to No.

• **Availability zone:** No Preference

• **VPC security groups:** If you have one or more existing VPC security groups, then you can use one or more of those VPC security groups with your Amazon Aurora DB cluster by choosing your VPC security group identifiers, for example, `gs-security-group1`.

Otherwise, you can choose to have Amazon RDS create a VPC security group for you by choosing **Create new VPC security group**. This example uses the **Create new VPC security group** option.

• **DB cluster identifier:** `gs-db-cluster1`

• **Database name:** `sampledb`

  **Note**
  This creates the default database. To create additional databases, connect to the DB cluster and use the SQL command `CREATE DATABASE`.

• **Database port:** 3306

  **Note**
  You might be behind a corporate firewall that does not allow access to default ports such as the Aurora MySQL default port, 3306. In this case, provide a port value that your corporate firewall allows. Remember that port value later when you connect to the Aurora DB cluster.

9. Leave the rest of the values as their defaults, and choose **Create database** to create the DB cluster and primary instance.

**Connect to an instance in a DB cluster**

Once Amazon RDS provisions your DB cluster and creates the primary instance, you can use any standard SQL client application to connect to a database on the DB cluster. In this example, you connect to a database on the Aurora MySQL DB cluster using MySQL monitor commands. One GUI-based application that you can use to connect is MySQL Workbench. For more information, go to the [Download MySQL Workbench page](https://console.aws.amazon.com/rds/).

**To connect to a database on an Aurora MySQL DB cluster using the MySQL monitor**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).

2. Choose **Databases** and then choose the DB cluster name to show its details. On the **Connectivity & security** tab, copy the value for the **Endpoint name** of the **Writer** endpoint. Also, note the port number for the endpoint.
3. Type the following command at a command prompt on a client computer to connect to a database on an Aurora MySQL DB cluster using the MySQL monitor. Use the cluster endpoint to connect to the primary instance, and the master user name that you created previously. (You are prompted for a password.) If you supplied a port value other than 3306, use that for the -P parameter instead.

```
PROMPT> mysql -h <cluster endpoint> -P 3306 -u <myusername> -p
```

You should see output similar to the following.

```
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 350
Server version: 5.6.10-log MySQL Community Server (GPL)
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql>
```

For more information about connecting to the DB cluster, see Connecting to an Amazon Aurora MySQL DB cluster (p. 253).
Delete the sample DB cluster, DB subnet group, and VPC

Once you have connected to the sample DB cluster that you created, you can delete the DB cluster, DB subnet group, and VPC (if you created a VPC).

To delete a DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Databases and then choose the DB instance associated with the DB cluster.
3. For Actions, choose Delete.
4. Choose Delete.

After all of the DB instances associated with a DB cluster are deleted, the DB cluster is deleted automatically.

To delete a DB subnet group

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Subnet groups and then choose the DB subnet group.
3. Choose Delete.
4. Choose Delete.

To delete a VPC

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose Your VPCs and then choose the VPC that was created for this procedure.
3. For Actions, choose Delete VPC.
4. Choose Delete.

Creating a DB cluster and connecting to a database on an Aurora PostgreSQL DB cluster

The easiest way to create an Aurora PostgreSQL DB cluster is to use the Amazon RDS console. After you create the DB cluster, you can use standard PostgreSQL utilities, such as pgAdmin, to connect to a database on the DB cluster.

Topics

- Create an Aurora PostgreSQL DB cluster (p. 88)
- Connect to an instance in an Aurora PostgreSQL DB cluster (p. 96)
- Delete the sample DB cluster, DB subnet group, and VPC (p. 97)
Create an Aurora PostgreSQL DB cluster

Before you create a DB cluster, you must first have a virtual private cloud (VPC) based on the Amazon VPC service and an Amazon RDS DB subnet group. Your VPC must have at least one subnet in each of at least two Availability Zones. You can use the default VPC for your AWS account, or you can create your own VPC. The Amazon RDS console makes it easy for you to create your own VPC for use with Amazon Aurora or use an existing VPC with your Aurora DB cluster.

If you want to create a VPC and DB subnet group for use with your Amazon Aurora DB cluster yourself, rather than having Amazon RDS create the VPC and DB subnet group for you, follow the instructions in How to create a VPC for use with Amazon Aurora (p. 1281). Otherwise, follow the instructions in this topic to create your DB cluster and have Amazon RDS create a VPC and DB subnet group for you.

Note
A new console interface is available for database creation. Choose either the New Console or the Original Console instructions based on the console that you are using. The New Console instructions are open by default.

New console

You can create an Aurora PostgreSQL DB cluster with the AWS Management Console with Easy Create enabled or disabled. With Easy Create enabled, you specify only the DB engine type, DB instance size, and DB instance identifier. Easy Create uses the default setting for other configuration options. With Easy Create disabled, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

Note
For this example, Easy Create is enabled. For information about creating an Aurora PostgreSQL DB cluster with Easy Create not enabled, see Creating an Amazon Aurora DB cluster (p. 118).

To create an Aurora PostgreSQL DB cluster with Easy Create enabled

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region in which you want to create the DB instance.

   Aurora is not available in all AWS Regions. For a list of AWS Regions where Aurora is available, see Region availability (p. 6).
3. In the navigation pane, choose Databases.
4. Choose Create database and make sure that Easy Create is chosen.
5. For **Engine type**, choose **Amazon Aurora**.
6. For **Edition**, choose **Amazon Aurora with PostgreSQL compatibility**.
7. For **DB instance size**, choose **Dev/Test**.
8. For **DB cluster identifier**, enter a name for the DB cluster, or leave the default name.
9. For **Master username**, enter a name for the master user, or leave the default name.

The **Create database** page should look similar to the following image.
Create database

Choose a database creation method

- **Standard Create**
  You set all of the configuration options, including ones for availability, security, backups, and maintenance.

- **Easy Create**
  Use recommended best-practice configuration options. Some configuration options can be changed after the database is created.

Configuration

**Engine type**

- **Amazon Aurora**
- **MySQL**
- **MariaDB**
- **PostgreSQL**
- **Oracle**
- **Microsoft SQL Server**

**Edition**

- **Amazon Aurora with MySQL 5.6 compatibility**
- **Amazon Aurora with PostgreSQL compatibility**

**DB instance size**

- **Production**
  - db.r4.2xlarge
  - 8 vCPUs
  - 61 GiB RAM
- **Dev/Test**
  - db.r4.large
  - 2 vCPUs
  - 15.25 GiB RAM

**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 region.
10. To use an automatically generated master password for the DB cluster, make sure that the **Auto generate a password** check box is chosen.

To enter your master password, clear the **Auto generate a password** check box, and then enter the same password in **Master password** and **Confirm password**.

11. (Optional) Open **View default settings for Easy create**.

You can examine the default settings used when **Easy Create** is enabled. If you want to change one or more settings during database creation, choose **Standard Create** to set them. The **Editable after database creation** column shows which options can be changed after database creation. To change a setting with **No** in that column, use **Standard Create**. For settings with **Yes** in that column, you can either use **Standard Create**, or you can modify the DB instance after it is created to change the setting.

12. Choose **Create database**.

If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

To view the master user name and password for the DB instance, choose **View credential details**.

To connect to the DB instance as the master user, use the user name and password that appear.

**Important**
You can't view the master user password again. If you don't record it, you might have to change it. If you need to change the master user password after the DB instance is available, you can modify the DB instance to do so. For more information about modifying a DB instance, see **Modifying an Amazon Aurora DB cluster** (p. 327).

13. For **Databases**, choose the name of the new Aurora PostgreSQL DB cluster.

On the RDS console, the details for new DB cluster appear. The DB cluster and its DB instance have a status of **creating** until the DB cluster is ready to use. When the state changes to **available** for both, you can connect to the DB cluster. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new DB cluster is available.
To launch an Aurora PostgreSQL DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the top-right corner of the AWS Management Console, choose the AWS Region that you want to create your DB cluster in. For a list of AWS Regions where Aurora is available, see Region availability (p. 6).
3. In the navigation pane, choose Databases.

   If the navigation pane is closed, choose the menu icon at the top left to open it.
4. Choose Create database to open the Select engine page.
5. On the Select engine page, choose Amazon Aurora and choose the PostgreSQL-compatible edition.
6. Choose **Next**.
7. Set the following values on the **Specify DB details** page:
• **DB instance class**: db.r4.large

• **DB instance identifier**: aurora-postgres-db-instance1

• **Master username**: Using alphanumeric characters, type a master user name, used to log on to your DB instances in the DB cluster.

• **Master password** and **Confirm password**: Type a password in the Master Password box that contains from 8 to 41 printable ASCII characters (excluding /,", and @) for your master user password, used to log on to your database. Then type the password again in the Confirm Password box.
Specify DB details

Instance specifications
Estimate your monthly costs for the DB Instance using the AWS Simple Monthly Calculator.

DB engine
Aurora PostgreSQL

Capacity type
- Provisioned
  You provision and manage the server instance sizes.
- Provisioned with Aurora parallel query enabled
  You provision and manage the server instance sizes, and Aurora improves the performance of analytic queries by pushing processing down to the Aurora storage layer (currently available for Aurora MySQL 5.6)
- Serverless
  You specify the minimum and maximum of resources for a DB cluster. Aurora scales the capacity based on database load.

DB engine version
- Aurora PostgreSQL (compatible with PostgreSQL 9.6.9)

DB instance class
- db.r4.large — 2 vCPU, 15.25 GiB RAM

Multi-AZ deployment
- Create Replica in Different Zone
- No

Settings

DB instance identifier
Specify a name that is unique for all DB instances owned by your AWS account in the current region.
- aurora-postgres-db-instance1

DB instance identifier is case insensitive, but stored as all lower-case, as in "mydbinstance". Must contain from 1 to 63 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Cannot end with a hyphen or contain two consecutive hyphens.

Master username
Specify an alphanumeric string that defines the login ID for the master user.
- myawsuser

Master Username must start with a letter. Must contain 1 to 15 alphanumeric characters.

Master password
Master Password must be at least eight characters long, as in "mypass": Can be any printable ASCII character except ",", ";", or "@".
8. Choose Next and set the following values on the Configure Advanced Settings page:

- **Virtual Private Cloud (VPC):** If you have an existing VPC, then you can use that VPC with your Amazon Aurora DB cluster by choosing your VPC identifier, for example vpc-a464d1c1. For information on using an existing VPC, see How to create a VPC for use with Amazon Aurora (p. 1281).

  Otherwise, you can choose to have Amazon RDS create a VPC for you by choosing Create a new VPC. This example uses the Create a new VPC option.

- **Subnet group:** If you have an existing subnet group, then you can use that subnet group with your Amazon Aurora DB cluster by choosing your subnet group identifier, for example, gs-subnet-group1.

  Otherwise, you can choose to have Amazon RDS create a subnet group for you by choosing Create a new subnet group. This example uses the Create a new subnet group option.

- **Public accessibility:** Yes

  Note
  Your production DB cluster might not need to be in a public subnet, because only your application servers require access to your DB cluster. If your DB cluster doesn't need to be in a public subnet, set Publicly Accessible to No.

- **Availability zone:** No Preference

- **VPC security groups:** If you have one or more existing VPC security groups, then you can use one or more of those VPC security groups with your Amazon Aurora DB cluster by choosing your VPC security group identifiers, for example, gs-security-group1.

  Otherwise, you can choose to have Amazon RDS create a VPC security group for you by choosing Create new VPC security group. This example uses the Create new VPC security group option.

- **DB cluster identifier:** aurora-postgres-db-cluster1

- **Database name:** sampledb

  Note
  This creates the default database. To create additional databases, connect to the DB cluster and use the SQL command `CREATE DATABASE`.

- **Database port:** 5432

  Note
  You might be behind a corporate firewall that does not allow access to default ports such as the Aurora PostgreSQL default port, 5432. In this case, provide a port value that your corporate firewall allows. Remember that port value later when you connect to the Aurora DB cluster.

9. Leave the rest of the values as their defaults, and choose Create database to create the DB cluster and primary instance.

Connect to an instance in an Aurora PostgreSQL DB cluster

Once Amazon RDS provisions your DB cluster and creates the primary instance, you can use any standard SQL client application to connect to a database on the DB cluster.

To connect to a database on an Aurora PostgreSQL DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
Delete the sample DB cluster, DB subnet group, and VPC

Once you have connected to the sample DB cluster that you created, you can delete the DB cluster, DB subnet group, and VPC (if you created a VPC).

**To delete a DB cluster**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. Choose **Databases** and then choose the DB instance associated with the DB cluster.
3. For **Actions**, choose **Delete**.
4. Choose **Delete**.

   After all of the DB instances associated with a DB cluster are deleted, the DB cluster is deleted automatically.
To delete a DB subnet group
1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Subnet groups and then choose the DB subnet group.
3. Choose Delete.
4. Choose Delete.

To delete a VPC
1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose Your VPCs and then choose the VPC that was created for this procedure.
3. For Actions, choose Delete VPC.
4. Choose Delete.
Tutorial: Create a web server and an Amazon Aurora DB cluster

This tutorial helps you install an Apache web server with PHP and create a MySQL database. The web server runs on an Amazon EC2 instance using Amazon Linux, and the MySQL database is an Aurora MySQL DB cluster. Both the Amazon EC2 instance and the DB cluster run in a virtual private cloud (VPC) based on the Amazon VPC service.

**Important**
There's no charge for creating an AWS account. However, by completing this tutorial, you might incur costs for the AWS resources you use. You can delete these resources after you complete the tutorial if they are no longer needed.

**Note**
This tutorial works with Amazon Linux and might not work for other versions of Linux such as Ubuntu.

In the tutorial that follows, you specify the VPC, subnets, and security groups when you create the DB cluster. You also specify them when you create the EC2 instance to host your web server. The VPC, subnets, and security groups are required for the DB cluster and the web server to communicate. After the VPC is set up, this tutorial shows you how to create the DB cluster and install the web server. You connect your web server to your DB cluster in the VPC using the DB cluster writer endpoint.

1. **Complete the tasks in Tutorial: Create an Amazon VPC for use with a DB instance (p. 1298).**

   Before you begin this tutorial, make sure that you have a VPC with both public and private subnets, and corresponding security groups. If you don't have these, complete the following tasks in the tutorial:

   a. [Create a VPC with private and public subnets (p. 1298)]
   b. [Create additional subnets (p. 1299)]
   c. [Create a VPC security group for a public web server (p. 1300)]
   d. [Create a VPC security group for a private DB instance (p. 1301)]
   e. [Create a DB subnet group (p. 1301)]

2. **Create an Amazon Aurora DB cluster (p. 100)**

3. **Create an EC2 instance and install a web server (p. 105)**

The following diagram shows the configuration when the tutorial is complete.
Create an Amazon Aurora DB cluster

In this step, you create an Amazon Aurora MySQL DB cluster that maintains the data used by a web application.

Important
Before you begin this step, you must have a VPC with both public and private subnets, and corresponding security groups. If you don't have these, see Tutorial: Create an Amazon VPC for use with a DB instance (p. 1298). Complete the steps in Create a VPC with private and public subnets (p. 1298), Create additional subnets (p. 1299), Create a VPC security group for a public web server (p. 1300), and Create a VPC security group for a private DB instance (p. 1301).

To create an Aurora MySQL DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region where you want to create the DB cluster. This example uses the US West (Oregon) Region.
3. In the navigation pane, choose Databases.
4. Choose Create database.
5. On the Create database page, shown following, make sure that the Standard Create option is chosen, and then choose Amazon Aurora. Keep the default values for Version and Database Location.
6. In the Database features section, choose One writer and multiple readers.

7. In the Templates section, choose Dev/Test.

8. In the Settings section, set these values:
   - DB cluster identifier – tutorial-db-cluster
   - Master username – tutorial_user
   - Auto generate a password – Disable the option
   - Master password – Choose a password.
   - Confirm password – Retype the password.
9. In the **DB instance size** section, set these values:

- **Burstable classes (includes t classes)**
- **db.t2.small**

10. In the **Availability & durability** section, use the default values.

11. In the **Connectivity** section, open **Additional connectivity configuration** and set these values:
• **Virtual private cloud (VPC)** – Choose an existing VPC with both public and private subnets, such as the `tutorial-vpc` (vpc-identifier) created in Create a VPC with private and public subnets (p. 1298)

  **Note**
  The VPC must have subnets in different Availability Zones.

• **Subnet group** – The DB subnet group for the VPC, such as the `tutorial-db-subnet-group` created in Create a DB subnet group (p. 1301)

• **Public access** – No

• **Existing VPC security groups** – Choose an existing VPC security group that is configured for private access, such as the `tutorial-db-securitygroup` created in Create a VPC security group for a private DB instance (p. 1301).

  Remove other security groups, such as the default security group, by choosing the X associated with each.

• **Database port** – 3306
12. Open the **Additional configuration** section, and enter `sample` for **Initial database name**. Keep the default settings for the other options.

13. To create your Aurora MySQL DB cluster, choose **Create database**.

Your new DB cluster appears in the **Databases** list with the status **Creating**.

14. Wait for the **Status** of your new DB cluster to show as **Available**. Then choose the DB cluster name to show its details.

15. In the **Connectivity & security** section, view the **Endpoint** and **Port** of the writer DB instance.
Note the endpoint and port for your writer DB instance. You use this information to connect your web server to your DB cluster.

To make sure that your Aurora MySQL DB cluster is as secure as possible, verify that sources outside of the VPC can't connect to your Aurora MySQL DB cluster.


Create an EC2 instance and install a web server

In this step, you create a web server to connect to the Amazon Aurora DB cluster that you created in Create an Amazon Aurora DB cluster (p. 100).

Launch an EC2 instance

First, you create an Amazon EC2 instance in the public subnet of your VPC.

To launch an EC2 instance

1. Sign in to the AWS Management Console and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Choose EC2 Dashboard, and then choose Launch instance, as shown following.
3. Choose the **Amazon Linux 2 AMI**.

4. Choose the **t2.micro** instance type, as shown following, and then choose **Next: Configure Instance Details**.
5. On the **Configure Instance Details** page, shown following, set these values and keep the other values as their defaults:

- **Network**: Choose the VPC with both public and private subnets that you chose for the DB cluster, such as the `vpc-identifier | tutorial-vpc` created in Create a VPC with private and public subnets (p. 1298).
- **Subnet**: Choose an existing public subnet, such as `subnet-identifier | Tutorial public | us-west-2a` created in Create a VPC security group for a public web server (p. 1300).
- **Auto-assign Public IP**: Choose **Enable**.
6. Choose **Next: Add Storage**.

7. On the **Add Storage** page, keep the default values and choose **Next: Add Tags**.

8. On the **Add Tags** page, shown following, choose **Add Tag**, then enter **Name** for **Key** and enter **tutorial-web-server** for **Value**.

9. Choose **Next: Configure Security Group**.

10. On the **Configure Security Group** page, shown following, choose **Select an existing security group**. Then choose an existing security group, such as the **tutorial-securitygroup** created in [Create a VPC security group for a public web server](p. 1300). Make sure that the security group that you choose includes inbound rules for Secure Shell (SSH) and HTTP access.

12. On the Review Instance Launch page, shown following, verify your settings and then choose Launch.

13. On the Select an existing key pair or create a new key pair page, shown following, choose Create a new key pair and set Key pair name to tutorial-key-pair. Choose Download Key Pair, and then save the key pair file on your local machine. You use this key pair file to connect to your EC2 instance.
14. To launch your EC2 instance, choose Launch Instances. On the Launch Status page, shown following, note the identifier for your new EC2 instance, for example: i-0288d65fd4470b6a9.
15. Choose View Instances to find your instance.
16. Wait until Instance Status for your instance reads as Running before continuing.

Install an Apache web server with PHP

Next, you connect to your EC2 instance and install the web server.

To connect to your EC2 instance and install the Apache web server with PHP

1. Connect to the EC2 instance that you created earlier by following the steps in Connect to your Linux instance.
2. Get the latest bug fixes and security updates by updating the software on your EC2 instance. To do this, use the following command.
   
   **Note**
   The `–y` option installs the updates without asking for confirmation. To examine updates before installing, omit this option.

   ```
   sudo yum update -y
   ```

3. After the updates complete, install the PHP software using the `yum install` command. This command installs multiple software packages and related dependencies at the same time.
Create a web server

```bash
sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
```

If you receive an error stating `sudo: amazon-linux-extras: command not found`, then your instance was not launched with an Amazon Linux 2 AMI (perhaps you are using the Amazon Linux AMI instead). You can view your version of Amazon Linux using the following command.

```bash
cat /etc/system-release
```

For more information, see Updating instance software.

4. Install the Apache web server.

```bash
sudo yum install -y httpd
```

5. Start the web server with the command shown following.

```bash
sudo systemctl start httpd
```

You can test that your web server is properly installed and started. To do this, enter the public Domain Name System (DNS) name of your EC2 instance in the address bar of a web browser, for example: `http://ec2-42-8-168-21.us-west-1.compute.amazonaws.com`. If your web server is running, then you see the Apache test page.

If you don't see the Apache test page, check your inbound rules for the VPC security group that you created in Tutorial: Create an Amazon VPC for use with a DB instance (p. 1298). Make sure that your inbound rules include a rule allowing HTTP (port 80) access for the IP address you use to connect to the web server.

**Note**
The Apache test page appears only when there is no content in the document root directory, `/var/www/html`. After you add content to the document root directory, your content appears at the public DNS address of your EC2 instance instead of the Apache test page.

6. Configure the web server to start with each system boot using the `chkconfig` command.

```bash
sudo systemctl enable httpd
```

To allow `ec2-user` to manage files in the default root directory for your Apache web server, modify the ownership and permissions of the `/var/www` directory. In this tutorial, you add a group named `www` to your EC2 instance. Then you give that group ownership of the `/var/www` directory and add write permissions for the group. Any members of that group can then add, delete, and modify files for the web server.

**To set file permissions for the Apache web server**

1. Add the `www` group to your EC2 instance with the following command.

```bash
sudo groupadd www
```

2. Add the `ec2-user` user to the `www` group.

```bash
sudo usermod -a -G www ec2-user
```

3. Log out to refresh your permissions and include the new `www` group.
4. Log back in again and verify that the www group exists with the `groups` command.

```
exit
```

```
groups
```

Your output looks similar to the following:

```
ec2-user adm wheel systemd-journal www
```

5. Change the group ownership of the `/var/www` directory and its contents to the `www` group.

```
sudo chgrp -R www /var/www
```

6. Change the directory permissions of `/var/www` and its subdirectories to add group write permissions and set the group ID on subdirectories created in the future.

```
sudo chmod 2775 /var/www
find /var/www -type d -exec sudo chmod 2775 {} +
```

7. Recursively change the permissions for files in the `/var/www` directory and its subdirectories to add group write permissions.

```
find /var/www -type f -exec sudo chmod 0664 {} +
```

### Connect your Apache web server to your DB instance

Next, you add content to your Apache web server that connects to your Amazon Aurora DB cluster.

**To add content to the Apache web server that connects to your DB cluster**

1. While still connected to your EC2 instance, change the directory to `/var/www` and create a new subdirectory named `inc`.

```
cd /var/www
mkdir inc
cd inc
```

2. Create a new file in the `inc` directory named `dbinfo.inc`, and then edit the file by calling nano (or the editor of your choice).

```
>dbinfo.inc
nano dbinfo.inc
```

3. Add the following contents to the `dbinfo.inc` file. Here, `db_instance_endpoint` is DB cluster writer endpoint, without the port, and `master_password` is the master password for your DB cluster.

```
<?php

<db_instance_endpoint>
<master_password>

```

**Note**

We recommend placing the user name and password information in a folder that isn't part of the document root for your web server. Doing this reduces the possibility of your security information being exposed.
4. Save and close the `dbinfo.inc` file.
5. Change the directory to `/var/www/html`.

```bash
cd /var/www/html
```
6. Create a new file in the `html` directory named `SamplePage.php`, and then edit the file by calling `nano` (or the editor of your choice).

```bash
SamplePage.php
nano SamplePage.php
```
7. Add the following contents to the `SamplePage.php` file:

```php
<?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"></td>
<td><input type="text" name="ADDRESS"></td>
</tr>
</table>
```

**Note**

We recommend placing the user name and password information in a folder that isn't part of the document root for your web server. Doing this reduces the possibility of your security information being exposed.
Create a web server

```php
<?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;
}
?>

8. Save and close the SamplePage.php file.


You can use SamplePage.php to add data to your DB cluster. The data that you add is then displayed on the page. To verify that the data was inserted into the table, you can install MySQL on the Amazon EC2 instance, connect to the DB instance, and query the table.

To make sure that your DB cluster is as secure as possible, verify that sources outside of the VPC can't connect to your DB cluster.

After you have finished testing your web server and your database, you should delete your DB cluster and your Amazon EC2 instance.

• To delete a DB cluster, follow the instructions in Deleting an Aurora DB cluster or a DB instance (p. 398). You don't need to create a final snapshot.

• To terminate an Amazon EC2 instance, follow the instruction in Terminate your instance in the Amazon EC2 User Guide.
Configuring your Amazon Aurora DB cluster

This section shows how to set up your Aurora DB cluster. Before creating an Aurora DB cluster, decide on the DB instance class that will run the DB cluster. Also, decide where the DB cluster will run by choosing an AWS Region. Next, create the DB cluster. If you have data outside of Aurora, you can migrate the data into an Aurora DB cluster.

Topics
- Creating an Amazon Aurora DB cluster (p. 118)
- Using Amazon Aurora Serverless v1 (p. 134)
- Using Amazon Aurora Serverless v2 (preview) (p. 193)
- Using Amazon Aurora global databases (p. 206)
- Connecting to an Amazon Aurora DB cluster (p. 253)
- Working with DB parameter groups and DB cluster parameter groups (p. 298)
- Migrating data to an Amazon Aurora DB cluster (p. 321)
Creating an Amazon Aurora DB cluster

An Amazon Aurora DB cluster consists of a DB instance, compatible with either MySQL or PostgreSQL, and a cluster volume that represents the data for the DB cluster, copied across three Availability Zones as a single, virtual volume. By default, the DB cluster contains a primary writer DB instance and, optionally, up to 15 Aurora Replicas (reader DB instances). For more information about Aurora DB clusters, see Amazon Aurora DB clusters (p. 3).

In the following topic, you can find out how to create an Aurora DB cluster. To get started, first see DB cluster prerequisites (p. 118).

For simple instructions on connecting to your Aurora DB cluster, see Connecting to an Amazon Aurora DB cluster (p. 253).

DB cluster prerequisites

Important
Before you can create an Aurora DB cluster, you must complete the tasks in Setting up your environment for Amazon Aurora (p. 73).

The following are prerequisites to create a DB cluster.

VPC

You can only create an Amazon Aurora DB cluster in a virtual private cloud (VPC) based on the Amazon VPC service, in an AWS Region that has at least two Availability Zones. The DB subnet group that you choose for the DB cluster must cover at least two Availability Zones. This configuration ensures that your DB cluster always has at least one DB instance available for failover, in the unlikely event of an Availability Zone failure.

If you are using the AWS Management Console to create your Aurora DB cluster, you can have Amazon RDS automatically create a VPC for you. Or you can use an existing VPC or create a new VPC for your Aurora DB cluster. Your VPC must have at least one subnet in each of at least two Availability Zones for you to use it with an Amazon Aurora DB cluster. For more information, see How to create a VPC for use with Amazon Aurora (p. 1281). For information on VPCs, see Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281).

Note
You can communicate with an EC2 instance that is not in a VPC and an Amazon Aurora DB cluster using ClassicLink. For more information, see A DB instance in a VPC accessed by an EC2 instance not in a VPC (p. 1290).

If you don't have a default VPC or you haven't created a VPC, you can have Amazon RDS automatically create a VPC for you when you create an Aurora DB cluster using the console. Otherwise, you must do the following:

- Create a VPC with at least one subnet in each of at least two of the Availability Zones in the AWS Region where you want to deploy your DB cluster. For more information, see How to create a VPC for use with Amazon Aurora (p. 1281).
- Specify a VPC security group that authorizes connections to your Aurora DB cluster. For more information, see Working with a DB instance in a VPC (p. 1292).
- Specify an RDS DB subnet group that defines at least two subnets in the VPC that can be used by the Aurora DB cluster. For more information, see Working with DB subnet groups (p. 1292).
Additional prerequisites

If you are connecting to AWS using AWS Identity and Access Management (IAM) credentials, your AWS account must have IAM policies that grant the permissions required to perform Amazon RDS operations. For more information, see Identity and access management in Amazon Aurora (p. 1222).

If you are using IAM to access the Amazon RDS console, you must first sign on to the AWS Management Console with your IAM user credentials. Then go to the Amazon RDS console at https://console.aws.amazon.com/rds/.

If you want to tailor the configuration parameters for your DB cluster, you must specify a DB cluster parameter group and DB parameter group with the required parameter settings. For information about creating or modifying a DB cluster parameter group or DB parameter group, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

You must determine the TCP/IP port number to specify for your DB cluster. The firewalls at some companies block connections to the default ports (3306 for MySQL, 5432 for PostgreSQL) for Aurora. If your company firewall blocks the default port, choose another port for your DB cluster. All instances in a DB cluster use the same port.

Creating a DB cluster

You can create an Aurora DB cluster using the AWS Management Console, the AWS CLI, or the RDS API.

**Note**
If you are using the console, a new console interface is available for database creation. Choose either the New Console or the Original Console instructions based on the console that you are using. The New Console instructions are open by default.

New console

You can create a DB instance running MySQL with the AWS Management Console with Easy create enabled or not enabled. With Easy create enabled, you specify only the DB engine type, DB instance size, and DB instance identifier. Easy Create uses the default setting for other configuration options. With Easy create not enabled, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

**Note**
For this example, Standard Create is enabled, and Easy Create isn't enabled. For information about creating an Aurora MySQL DB cluster with Easy create enabled, see Getting started with Amazon Aurora (p. 78).

To create an Aurora DB cluster using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region in which you want to create the DB cluster.

   Aurora is not available in all AWS Regions. For a list of AWS Regions where Aurora is available, see Region availability (p. 6).
3. In the navigation pane, choose Databases.
4. Choose Create database.
5. In Choose a database creation method, choose Standard Create.
6. In Engine options, choose Amazon Aurora.
7. In **Edition**, choose one of the following:
   - **Amazon Aurora with MySQL compatibility**
• **Amazon Aurora with PostgreSQL compatibility**

8. If you chose **Amazon Aurora with MySQL compatibility**, choose one of the following in **Database features**:

- **One writer and multiple readers**
  
  For more information, see Amazon Aurora DB clusters (p. 3).

- **Serverless**
  
  For more information, see Using Amazon Aurora Serverless v1 (p. 134).

9. In **Templates**, choose the template that matches your use case.

10. To enter your master password, do the following:

   a. In the **Settings** section, open **Credential Settings**.
   
   b. Clear the **Auto generate a password** check box.
   
   c. (Optional) Change the **Master username** value and enter the same password in **Master password** and **Confirm password**.

   By default, the new DB instance uses an automatically generated password for the master user.

11. For the remaining sections, specify your DB cluster settings. For information about each setting, see **Settings for Aurora DB clusters** (p. 128).

12. Choose **Create database**.

   If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

   To view the master user name and password for the DB cluster, choose **View credential details**.

   ![](Creating database database-1.png)

   To connect to the DB instance as the master user, use the user name and password that appear.

   **Important**

   You can't view the master user password again. If you don't record it, you might have to change it. If you need to change the master user password after the DB instance is available, you can modify the DB instance to do so. For more information about modifying a DB instance, see **Modifying an Amazon Aurora DB cluster** (p. 327).

13. For **Databases**, choose the name of the new Aurora DB cluster.

   On the RDS console, the details for new DB cluster appear. The DB cluster and its DB instance have a status of **creating** until the DB cluster is ready to use. When the state changes to **available** for both, you can connect to the DB cluster. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new DB cluster is available.
When the state changes to available, you can connect to the primary instance for your DB cluster. Depending on the DB instance class and store allocated, it can take several minutes for the new instance to be available.

To view the newly created cluster, choose **Databases** from the navigation pane in the Amazon RDS console. Then choose the DB cluster to show the DB cluster details. For more information, see **Viewing an Amazon Aurora DB cluster (p. 473)**.

On the **Connectivity & security** tab, note the port and the endpoint of the writer DB instance. Use the endpoint and port of the cluster in your JDBC and ODBC connection strings for any application that performs write or read operations.
Original console

To create an Aurora DB cluster using the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the top-right corner of the AWS Management Console, choose the AWS Region in which you want to create the Aurora DB cluster.
3. In the navigation pane, choose Databases.
   If the navigation pane is closed, choose the menu icon at the top left to open it.
4. Choose Create database to open the Select engine page.
5. On the Select engine page, choose an edition of Aurora. Choose either MySQL 5.6-compatible, MySQL 5.7-compatible, or PostgreSQL-compatible.

6. Choose Next.
7. On the Specify DB details page, specify your DB instance information. For information about each setting, see Settings for Aurora DB clusters (p. 128).
A typical **Specify DB details** page looks like the following.

8. Confirm your master password and choose **Next**.

9. On the **Configure advanced settings** page, you can customize additional settings for your Aurora DB cluster. For information about each setting, see **Settings for Aurora DB clusters** (p. 128).

10. Choose **Create database** to create your Aurora DB cluster, and then choose **Close**.

    On the Amazon RDS console, the new DB cluster appears in the list of DB clusters. The DB cluster will have a status of **creating** until the DB cluster is created and ready for use. When the state
changes to available, you can connect to the writer instance for your DB cluster. Depending on the DB cluster class and store allocated, it can take several minutes for the new cluster to be available.

To view the newly created cluster, choose Databases from the navigation pane in the Amazon RDS console and choose the DB cluster to show the DB cluster details. For more information, see Viewing an Amazon Aurora DB cluster (p. 473).

Note the ports and the endpoints of the cluster. Use the endpoint and port of the writer DB cluster in your JDBC and ODBC connection strings for any application that performs write or read operations.
AWS CLI

Note
Before you can create an Aurora DB cluster using the AWS CLI, you must fulfill the required prerequisites, such as creating a VPC and an RDS DB subnet group. For more information, see DB cluster prerequisites (p. 118).

You can use the AWS CLI to create an Aurora MySQL DB cluster or an Aurora PostgreSQL DB cluster.

To create an Aurora MySQL DB cluster using the AWS CLI

When you create an Aurora MySQL DB cluster or DB instance, ensure that you specify the correct value for the --engine option value based on the MySQL compatibility of the DB cluster or DB instance.

- When you create an Aurora MySQL 5.7 DB cluster or DB instance, you must specify aurora-mysql for the --engine option.
- When you create an Aurora MySQL 5.6 DB cluster or DB instance, you must specify aurora for the --engine option.

Complete the following steps:

1. Identify the DB subnet group and VPC security group ID for your new DB cluster, and then call the create-db-cluster AWS CLI command to create the Aurora MySQL DB cluster.

For example, the following command creates a new MySQL 5.7–compatible DB cluster named sample-cluster.

For Linux, macOS, or Unix:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora-mysql
  --engine-version 5.7.12 --master-username user-name --master-user-password password
  --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
```

For Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora-mysql
  --engine-version 5.7.12 --master-username user-name --master-user-password password
  --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
```

The following command creates a new MySQL 5.6–compatible DB cluster named sample-cluster.

For Linux, macOS, or Unix:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora
  --engine-version 5.6.10a --master-username user-name --master-user-password password
  --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
```

For Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora
  --engine-version 5.6.10a --master-username user-name --master-user-password password
```
2. If you use the console to create a DB cluster, then Amazon RDS automatically creates the primary instance (writer) for your DB cluster. If you use the AWS CLI to create a DB cluster, you must explicitly create the primary instance for your DB cluster. The primary instance is the first instance that is created in a DB cluster.

Call the `create-db-instance` AWS CLI command to create the primary instance for your DB cluster. Include the name of the DB cluster as the `--db-cluster-identifier` option value.

For example, the following command creates a new MySQL 5.7–compatible DB instance named `sample-instance`.

For Linux, macOS, or Unix:

```
aws rds create-db-instance --db-instance-identifier sample-instance
    --db-cluster-identifier sample-cluster --engine aurora-mysql
    --db-instance-class db.r4.large
```

For Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance
    --db-cluster-identifier sample-cluster --engine aurora-mysql
    --db-instance-class db.r4.large
```

The following command creates a new MySQL 5.6–compatible DB instance named `sample-instance`.

For Linux, macOS, or Unix:

```
aws rds create-db-instance --db-instance-identifier sample-instance
    --db-cluster-identifier sample-cluster --engine aurora
    --db-instance-class db.r4.large
```

For Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance
    --db-cluster-identifier sample-cluster --engine aurora
    --db-instance-class db.r4.large
```

**To create an Aurora PostgreSQL DB cluster using the AWS CLI**

1. Identify the DB subnet group and VPC security group ID for your new DB cluster, and then call the `create-db-cluster` AWS CLI command to create the Aurora PostgreSQL DB cluster.

For example, the following command creates a new DB cluster named `sample-cluster`.

For Linux, macOS, or Unix:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster
    --engine aurora-postgresql
    --master-username user-name
    --master-user-password password
    --db-subnet-group-name mysubnetgroup
    --vpc-security-group-ids sg-c7e5b0d2
```

For Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster
    --engine aurora-postgresql
    --master-username user-name
    --master-user-password password
    --db-subnet-group-name mysubnetgroup
    --vpc-security-group-ids sg-c7e5b0d2
```
2. If you use the console to create a DB cluster, then Amazon RDS automatically creates the primary instance (writer) for your DB cluster. If you use the AWS CLI to create a DB cluster, you must explicitly create the primary instance for your DB cluster. The primary instance is the first instance that is created in a DB cluster.

Call the `create-db-instance` AWS CLI command to create the primary instance for your DB cluster. Include the name of the DB cluster as the `--db-cluster-identifier` option value.

For Linux, macOS, or Unix:
```
aws rds create-db-instance --db-instance-identifier sample-instance
  --db-cluster-identifier sample-cluster --engine aurora-postgresql
  --db-instance-class db.r4.large
```

For Windows:
```
aws rds create-db-instance --db-instance-identifier sample-instance
  --db-cluster-identifier sample-cluster --engine aurora-postgresql
  --db-instance-class db.r4.large
```

### RDS API

**Note**

Before you can create an Aurora DB cluster using the AWS CLI, you must fulfill the required prerequisites, such as creating a VPC and an RDS DB subnet group. For more information, see DB cluster prerequisites (p. 118).

Identify the DB subnet group and VPC security group ID for your new DB cluster, and then call the `CreateDBInstance` operation to create the DB cluster.

When you create an Aurora MySQL DB cluster or DB instance, ensure that you specify the correct value for the `Engine` parameter value based on the MySQL compatibility of the DB cluster or DB instance.

- When you create an Aurora MySQL 5.7 DB cluster or DB instance, you must specify `aurora-mysql` for the `Engine` parameter.
- When you create an Aurora MySQL 5.6 DB cluster or DB instance, you must specify `aurora` for the `Engine` parameter.

When you create an Aurora PostgreSQL DB cluster or DB instance, specify `aurora-postgresql` for the `Engine` parameter.

### Settings for Aurora DB clusters

The following table contains details about settings that you choose when you create an Aurora DB cluster.
<table>
<thead>
<tr>
<th>Available settings</th>
<th>For this option</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability zone</strong></td>
<td>Determine if you want to specify a particular Availability Zone. For more information about Availability Zones, see Regions and Availability Zones (p. 5).</td>
<td></td>
</tr>
<tr>
<td><strong>Auto minor version upgrade</strong></td>
<td>Choose Enable auto minor version upgrade if you want to enable your Aurora DB cluster to receive preferred minor version upgrades to the DB engine automatically when they become available. The Auto minor version upgrade setting applies to both Aurora PostgreSQL and Aurora MySQL DB clusters. For Aurora MySQL 1.x and 2.x clusters, this setting upgrades the clusters to a maximum version of 1.22.2 and 2.07.2. For more information about engine updates for Aurora PostgreSQL, see Database engine updates for Amazon Aurora PostgreSQL (p. 1147). For more information about engine updates for Aurora MySQL, see Database engine updates for Amazon Aurora MySQL (p. 874).</td>
<td></td>
</tr>
<tr>
<td><strong>Backtrack</strong></td>
<td>Applies only to Aurora MySQL. Choose Enable Backtrack to enable backtracking or Disable Backtrack to disable backtracking. Using backtracking, you can rewind a DB cluster to a specific time, without creating a new DB cluster. It is disabled by default. If you enable backtracking, also specify the amount of time that you want to be able to backtrack your DB cluster (the target backtrack window). For more information, see Backtracking an Aurora DB cluster (p. 677).</td>
<td></td>
</tr>
<tr>
<td><strong>Copy tags to snapshots</strong></td>
<td>Choose this option to copy any DB instance tags to a DB snapshot when you create a snapshot. For more information, see Tagging Amazon RDS resources (p. 401).</td>
<td></td>
</tr>
<tr>
<td><strong>Database authentication</strong></td>
<td>The database authentication option you want to use. Choose Password authentication to authenticate database users with database passwords only. Choose Password and IAM DB authentication to authenticate database users with database passwords and user credentials through IAM users and roles. For more information, see IAM database authentication (p. 1238).</td>
<td></td>
</tr>
<tr>
<td><strong>Database port</strong></td>
<td>Specify the port for applications and utilities to use to access the database. Aurora MySQL DB clusters default to the default MySQL port, 3306, and Aurora PostgreSQL DB clusters default to the default PostgreSQL port, 5432. The firewalls at some companies block connections to these default ports. If your company firewall blocks the default port, choose another port for the new DB cluster.</td>
<td></td>
</tr>
<tr>
<td>For this option</td>
<td>Do this</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| DB cluster identifier             | Enter a name for your DB cluster that is unique for your account in the AWS Region that you chose. This identifier is used in the cluster endpoint address for your DB cluster. For information on the cluster endpoint, see Amazon Aurora connection management (p. 24). The DB cluster identifier has the following constraints:  
  • It must contain from 1 to 63 alphanumeric characters or hyphens.  
  • Its first character must be a letter.  
  • It cannot end with a hyphen or contain two consecutive hyphens.  
  • It must be unique for all DB clusters per AWS account, per AWS Region. |
| DB cluster parameter group        | Choose a DB cluster parameter group. Aurora has a default DB cluster parameter group you can use, or you can create your own DB cluster parameter group. For more information about DB cluster parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298). |
| DB engine version                 | Applies only to the provisioned capacity type. Choose the version number of your DB engine.                                                                                                           |
| DB instance class                 | Applies only to the provisioned capacity type. Choose a DB instance class that defines the processing and memory requirements for each instance in the DB cluster. For more information about DB instance classes, see DB instance classes (p. 46). |
| DB instance identifier            | Enter a name for the primary instance in your DB cluster. This identifier is used in the endpoint address for the primary instance of your DB cluster. The DB instance identifier has the following constraints:  
  • It must contain from 1 to 63 alphanumeric characters or hyphens.  
  • Its first character must be a letter.  
  • It can't end with a hyphen or contain two consecutive hyphens.  
  • It must be unique for all DB instances per AWS account, per AWS Region. |
<p>| DB parameter group                | Choose a parameter group. Aurora has a default parameter group you can use, or you can create your own parameter group. For more information about parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298). |</p>
<table>
<thead>
<tr>
<th>For this option</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable deletion protection</td>
<td>Choose <strong>Enable deletion protection</strong> to prevent your DB cluster from being deleted. If you create a production DB cluster with the console, deletion protection is enabled by default.</td>
</tr>
<tr>
<td>Enable encryption</td>
<td>Choose <strong>Enable encryption</strong> to enable encryption at rest for this DB cluster. For more information, see Encrypting Amazon Aurora resources (p. 1208).</td>
</tr>
<tr>
<td>Enable Enhanced Monitoring</td>
<td>Choose <strong>Enable enhanced monitoring</strong> to enable gathering metrics in real time for the operating system that your DB cluster runs on. For more information, see Enhanced Monitoring (p. 504).</td>
</tr>
<tr>
<td>Enable Performance Insights</td>
<td>Choose <strong>Enable Performance Insights</strong> to enable Amazon RDS Performance Insights. For more information, see Using Amazon RDS Performance Insights (p. 514).</td>
</tr>
<tr>
<td>Failover priority</td>
<td>Choose a failover priority for the instance. If you don't choose a value, the default is <strong>tier-1</strong>. This priority determines the order in which Aurora Replicas are promoted when recovering from a primary instance failure. For more information, see Fault tolerance for an Aurora DB cluster (p. 56).</td>
</tr>
<tr>
<td>Granularity</td>
<td>Only available if <strong>Enhanced Monitoring</strong> is set to <strong>Enable enhanced monitoring</strong>. Set the interval, in seconds, between when metrics are collected for your DB cluster.</td>
</tr>
<tr>
<td>Initial database name</td>
<td>Enter a name for your default database. If you don't provide a name, Amazon RDS doesn't create a database on the DB cluster you are creating.</td>
</tr>
</tbody>
</table>

For Aurora MySQL, the default database name has these constraints:

- It must contain 1–64 alphanumeric characters.
- It can't be a word reserved by the database engine.

For Aurora PostgreSQL, the default database name has these constraints:

- It must contain 1–63 alphanumeric characters.
- It must begin with a letter or an underscore. Subsequent characters can be letters, underscores, or digits (0–9).
- It can't be a word reserved by the database engine.

To create additional databases, connect to the DB cluster and use the SQL command `CREATE DATABASE`. For more information about connecting to the DB cluster, see Connecting to an Amazon Aurora DB cluster (p. 253).
### Available settings

<table>
<thead>
<tr>
<th>For this option</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log exports</strong></td>
<td>Choose the types of MySQL or PostgreSQL database log files to generate. For more information, see [MySQL database log files](p. 622) and [PostgreSQL database log files](p. 627).</td>
</tr>
<tr>
<td><strong>Maintenance window</strong></td>
<td>Choose <strong>Select window</strong> and specify the weekly time range during which system maintenance can occur. Or choose <strong>No preference</strong> for Amazon RDS to assign a period randomly.</td>
</tr>
<tr>
<td><strong>Master key</strong></td>
<td>Only available if <strong>Encryption</strong> is set to <strong>Enable encryption</strong>. Choose the master key to use for encrypting this DB cluster. For more information, see [Encrypting Amazon Aurora resources](p. 1208).</td>
</tr>
<tr>
<td><strong>Option group</strong></td>
<td>Aurora has a default option group.</td>
</tr>
</tbody>
</table>
| **Master password** | Enter a password to log on to your DB cluster:  
  - For Aurora MySQL, the password must contain 8–41 printable ASCII characters.  
  - For Aurora PostgreSQL, it must contain 8–128 printable ASCII characters.  
  - It can't contain /, \, @, or a space. |
| **Master username** | Enter a name to use as the master user name to log on to your DB cluster:  
  - For Aurora MySQL, the name must contain 1–16 alphanumeric characters.  
  - For Aurora PostgreSQL, it must contain 1–63 alphanumeric characters.  
  - The first character must be a letter.  
  - The name can't be a word reserved by the database engine. |
<p>| <strong>Monitoring Role</strong> | Only available if <strong>Enhanced Monitoring</strong> is set to <strong>Enable enhanced monitoring</strong>. Choose the IAM role that you created to permit Amazon RDS to communicate with Amazon CloudWatch Logs for you, or choose <strong>Default</strong> to have RDS create a role for you named rds-monitoring-role. For more information, see [Enhanced Monitoring](p. 504). |
| <strong>Multi-AZ deployment</strong> | Applies only to the provisioned capacity type. Determine if you want to create Aurora Replicas in other Availability Zones for failover support. If you choose <strong>Create Replica in Different Zone</strong>, then Amazon RDS creates an Aurora Replica for you in your DB cluster in a different Availability Zone than the primary instance for your DB cluster. For more information about multiple Availability Zones, see [Regions and Availability Zones](p. 5). |
| <strong>Option group</strong> | Aurora has a default option group. |</p>
<table>
<thead>
<tr>
<th>Available settings</th>
<th>For this option</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance Insights</strong></td>
<td>Doesn't apply to MySQL 5.6. Choose <strong>Enable Performance Insights</strong> if you want to use Amazon RDS Performance Insights to monitor your Amazon Aurora DB cluster load. For more information about Performance Insights, see Using Amazon RDS Performance Insights (p. 514).</td>
<td></td>
</tr>
<tr>
<td><strong>Public access</strong></td>
<td>Choose <strong>Publicly accessible</strong> to give the DB cluster a public IP address, or choose <strong>Not publicly accessible</strong>. The instances in your DB cluster can be a mix of both public and private DB instances. For more information about hiding instances from public access, see Hiding a DB instance in a VPC from the internet (p. 1293). To connect to a DB instance from outside of its Amazon VPC, the DB instance must be publicly accessible, access must be granted using the inbound rules of the DB instance’s security group, and other requirements must be met. For more information, see Can't connect to Amazon RDS DB instance (p. 1306). If your DB instance is isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 1221).</td>
<td></td>
</tr>
<tr>
<td><strong>Retention period</strong></td>
<td>Choose the length of time, from 1 to 35 days, that Aurora retains backup copies of the database. Backup copies can be used for point-in-time restores (PITR) of your database down to the second.</td>
<td></td>
</tr>
<tr>
<td><strong>Subnet group</strong></td>
<td>Choose the DB subnet group to use for the DB cluster. For more information, see DB cluster prerequisites (p. 118).</td>
<td></td>
</tr>
<tr>
<td><strong>Select the log types to publish to Amazon CloudWatch Logs</strong></td>
<td>Applies only to Aurora MySQL. In the Log exports section, choose the logs that you want to start publishing to Amazon CloudWatch Logs. For more about publishing to CloudWatch Logs, see Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs (p. 824).</td>
<td></td>
</tr>
<tr>
<td><strong>Virtual Private Cloud (VPC)</strong></td>
<td>Choose the VPC to host the DB cluster. Choose <strong>Create a new VPC</strong> to have Amazon RDS create a VPC for you. For more information, see DB cluster prerequisites (p. 118).</td>
<td></td>
</tr>
<tr>
<td><strong>VPC security group</strong></td>
<td>Choose <strong>Create new</strong> to have Amazon RDS create a VPC security group for you. Or choose <strong>Choose existing</strong> and specify one or more VPC security groups to secure network access to the DB cluster. When you choose <strong>Create new</strong> in the RDS console, a new security group is created with an inbound rule that allows access to the DB instance from the IP address detected in your browser. For more information, see DB cluster prerequisites (p. 118).</td>
<td></td>
</tr>
</tbody>
</table>
Using Amazon Aurora Serverless v1

Amazon Aurora Serverless v1 (Amazon Aurora Serverless version 1) is an on-demand autoscaling configuration for Amazon Aurora. An Aurora Serverless DB cluster is a DB cluster that scales compute capacity up and down based on your application’s needs. This contrasts with Aurora provisioned DB clusters, for which you manually manage capacity. Aurora Serverless v1 provides a relatively simple, cost-effective option for infrequent, intermittent, or unpredictable workloads. It is cost-effective because it automatically starts up, scales compute capacity to match your application’s usage, and shuts down when it’s not in use.

To learn more about pricing, see Serverless Pricing under MySQL-Compatible Edition or PostgreSQL-Compatible Edition on the Amazon Aurora pricing page.

Aurora Serverless v1 clusters have the same kind of high-capacity, distributed, and highly available storage volume that is used by provisioned DB clusters. The cluster volume for an Aurora Serverless v1 cluster is always encrypted. You can choose the encryption key, but you can’t disable encryption. That means that you can perform the same operations on an Aurora Serverless v1 that you can on encrypted snapshots. For more information, see Aurora Serverless v1 and snapshots (p. 144).

Topics

- Advantages of Aurora Serverless v1 (p. 134)
- Use cases for Aurora Serverless v1 (p. 135)
- Limitations of Aurora Serverless v1 (p. 135)
- Configuration requirements for Aurora Serverless v1 (p. 136)
- Using TLS/SSL with Aurora Serverless v1 (p. 137)
- How Aurora Serverless v1 works (p. 138)
- Creating an Aurora Serverless v1 DB cluster (p. 145)
- Restoring an Aurora Serverless v1 DB cluster (p. 150)
- Modifying an Aurora Serverless v1 DB cluster (p. 154)
- Scaling Aurora Serverless v1 DB cluster capacity manually (p. 156)
- Viewing Aurora Serverless v1 DB cluster capacity (p. 158)
- Deleting an Aurora Serverless v1 DB cluster (p. 159)
- Aurora Serverless v1 and Aurora database engine versions (p. 161)
- Using the Data API for Aurora Serverless (p. 162)
- Logging Data API calls with AWS CloudTrail (p. 186)
- Using the query editor for Aurora Serverless (p. 188)

Advantages of Aurora Serverless v1

Aurora Serverless v1 provides the following advantages:

- **Simpler than provisioned** – Aurora Serverless v1 removes much of the complexity of managing DB instances and capacity.
- **Scalable** – Aurora Serverless v1 seamlessly scales compute and memory capacity as needed, with no disruption to client connections.
- **Cost-effective** – When you use Aurora Serverless v1, you pay only for the database resources that you consume, on a per-second basis.
- **Highly available storage** – Aurora Serverless v1 uses the same fault-tolerant, distributed storage system with six-way replication as Aurora to protect against data loss.
Use cases for Aurora Serverless v1

Aurora Serverless v1 is designed for the following use cases:

- **Infrequently used applications** – You have an application that is only used for a few minutes several times per day or week, such as a low-volume blog site. With Aurora Serverless v1, you pay for only the database resources that you consume on a per-second basis.
- **New applications** – You're deploying a new application and you're unsure about the instance size you need. By using Aurora Serverless v1, you can create a database endpoint and have the database autoscale to the capacity requirements of your application.
- **Variable workloads** – You're running a lightly used application, with peaks of 30 minutes to several hours a few times each day, or several times per year. Examples are applications for human resources, budgeting, and operational reporting applications. With Aurora Serverless v1, you no longer need to provision for peak or average capacity.
- **Unpredictable workloads** – You're running daily workloads that have sudden and unpredictable increases in activity. An example is a traffic site that sees a surge of activity when it starts raining. With Aurora Serverless v1, your database autoscales capacity to meet the needs of the application's peak load and scales back down when the surge of activity is over.
- **Development and test databases** – Your developers use databases during work hours but don't need them on nights or weekends. With Aurora Serverless v1, your database automatically shuts down when it's not in use.
- **Multi-tenant applications** – With Aurora Serverless v1, you don't have to individually manage database capacity for each application in your fleet. Aurora Serverless v1 manages individual database capacity for you.

Limitations of Aurora Serverless v1

The following limitations apply to Aurora Serverless v1:

- Aurora Serverless v1 is available in certain AWS Regions and for specific Aurora MySQL and Aurora PostgreSQL versions only. For more information, see Aurora Serverless v1 (p. 21).
- Aurora Serverless v1 doesn't support the following features:
  - Aurora cloning
  - Aurora global databases
  - Aurora multi-master clusters
  - Aurora Replicas
  - AWS Identity and Access Management (IAM) database authentication
  - Backtracking in Aurora
  - Database activity streams
  - Performance Insights
- Connections to an Aurora Serverless v1 DB cluster are closed automatically if held open for longer than one day.
- All Aurora Serverless v1 DB clusters have the following limitations:
  - You can't export Aurora Serverless v1 snapshots to Amazon S3 buckets.
  - You can't save data to text files in Amazon S3.
  - You can't load text file data to Aurora MySQL Serverless from Amazon S3. However, you can load data to Aurora PostgreSQL Serverless from Amazon S3 by using the `aws_s3` extension with the `aws_s3.table_import_from_s3` function and the `credentials` parameter. For more information, see Importing Amazon S3 data into an Aurora PostgreSQL DB cluster (p. 1017).
- Aurora MySQL–based DB clusters running Aurora Serverless v1 don't support the following:
• Invoking AWS Lambda functions from within your Aurora MySQL DB cluster. However, AWS Lambda functions can make calls to your Aurora MySQL Serverless DB cluster.

• Restoring a snapshot from a DB instance that isn’t Aurora MySQL or RDS MySQL.

• Replicating data using replication based on binary logs (binlogs). This limitation is true regardless of whether your Aurora MySQL-based DB cluster Aurora Serverless v1 is the source or the target of the replication. To replicate data into an Aurora Serverless v1 DB cluster from a MySQL DB instance outside Aurora, such as one running on Amazon EC2, consider using AWS Database Migration Service. For more information, see the AWS Database Migration Service User Guide.

• Aurora PostgreSQL–based DB clusters running Aurora Serverless v1 have the following limitations:
  • The logical replication feature available in Amazon RDS PostgreSQL and Aurora PostgreSQL is not supported.
  • Outbound communications such as those enabled by Amazon RDS for PostgreSQL extensions aren’t supported. For example, you can’t access external data with the postgres_fdw/dblink extension. For more information about RDS PostgreSQL extensions, see PostgreSQL on Amazon RDS in the RDS User Guide.
  • Currently, certain SQL queries and commands aren’t recommended. These include session-level advisory locks, temporary relations, asynchronous notifications (LISTEN), and cursors with hold (DECLARE name ... CURSOR WITH HOLD FOR query). Also, NOTIFY commands prevent scaling and aren’t recommended.

  For more information, see Autoscaling for Aurora Serverless (p. 140).

Configuration requirements for Aurora Serverless v1

When you create an Aurora Serverless v1 DB cluster, pay attention to the following requirements:

• Use these specific port numbers for each DB engine:
  • Aurora MySQL – 3306
  • Aurora PostgreSQL – 5432

• Create your Aurora Serverless v1 DB cluster in a virtual private cloud (VPC) based on the Amazon VPC service. Aurora Serverless v1 DB clusters are accessible only from a VPC and can’t use a public IP address.

• You can’t give an Aurora Serverless v1 DB cluster a public IP address. You can access an Aurora Serverless v1 DB cluster only from within a VPC.

• Create two AWS PrivateLink endpoints for each Aurora Serverless v1 DB cluster. If you reach the limit for AWS PrivateLink endpoints within your VPC, you can’t create any more Aurora Serverless v1 clusters in that VPC. For information about checking and changing the limits on endpoints within a VPC, see Amazon VPC limits.

• Create subnets in different Availability Zones for the DB subnet group that you use for your Aurora Serverless v1 DB cluster. In other words, you can’t have more than one subnet in the same Availability Zone.

• Changes to a subnet group used by an Aurora Serverless v1 DB cluster aren’t applied to the cluster.

• You can access an Aurora Serverless v1 DB cluster from AWS Lambda. To do so, you must configure your Lambda function to run in the same VPC as your Aurora Serverless v1 DB cluster. For more information about working with AWS Lambda, see Configuring a Lambda function to access resources in an Amazon VPC in the AWS Lambda Developer Guide.
Using TLS/SSL with Aurora Serverless v1

By default, Aurora Serverless v1 uses the Transport Layer Security/Secure Sockets Layer (TLS/SSL) protocol to encrypt communications between clients and your Aurora Serverless v1 DB cluster. It supports TLS/SSL versions 1.0, 1.1, and 1.2.

You don't need to configure your Aurora Serverless v1 DB cluster to use TLS/SSL. Depending on the client that you use to connect to Aurora Serverless v1 DB cluster, you might not need to specify TLS/SSL to get an encrypted connection.

For example, to use the PostgreSQL Client to connect to an Aurora Serverless v1 DB cluster running Aurora with PostgreSQL compatibility, connect as you normally do.

```
psql -h endpoint -U user
```

After you enter your password, the PostgreSQL Client shows you see the connection details, including the TLS/SSL version and cipher.

```
psql (12.5 (Ubuntu 12.5-0ubuntu0.20.04.1), server 10.12)
Type "help" for help.
```

To use the MySQL Client to connect to an Aurora Serverless v1 DB cluster running Aurora with MySQL compatibility, you specify TLS/SSL in your request. The following example includes the Amazon root CA 1 trust store downloaded from Amazon Trust Services, which is necessary for this connection to succeed.

```
mysql -h endpoint -P 3306 -u user -p --ssl-ca=amazon-root-CA-1.pem --ssl-mode=REQUIRED
```

When prompted, enter your password. Soon, the MySQL monitor opens. You can confirm that the session is encrypted by using the `status` command.

```
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...
```

To learn more about connecting to Aurora MySQL database with the MySQL Client, see Connecting to a DB instance running the MySQL database engine.

**Note**
TLS/SSL support for Aurora Serverless v1 DB clusters currently isn't available in the China (Beijing) AWS Region.

Session variables that you might use with the MySQL Client or the PostgreSQL Client in other environments have no effect when using TLS/SSL between client and Aurora Serverless v1.

Aurora Serverless v1 supports all TLS/SSL modes available to the MySQL Client (`mysql`) and PostgreSQL Client (`psql`), including those listed in the following table.

<table>
<thead>
<tr>
<th>Description of TLS/SSL mode</th>
<th>mysql</th>
<th>psql</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect without using TLS/SSL</td>
<td>DISABLED</td>
<td>disable</td>
</tr>
</tbody>
</table>
How Aurora Serverless v1 works

Amazon Aurora offers two different DB engine modes aimed at two broadly different usage models.

The provisioned DB engine mode is designed for predictable workloads. When you work with Aurora provisioned DB clusters, you choose your DB instance class size and several other configuration options. For example, you can create one or more Aurora Replicas to increase read throughput. If your workload changes, you can modify the DB instance class size and change the number of Aurora Replicas. The provisioned model works well when you can adjust capacity in advance of expected consumption patterns.

The serverless DB engine mode is designed for a different usage pattern entirely. For example, your database usage might be heavy for a short period of time, followed by long periods of light activity or no activity at all. Some examples are retail websites with intermittent sales events, databases that produce reports when needed, development and testing environments, and new applications with uncertain requirements. For cases such as these and many others, configuring capacity correctly in advance isn’t always possible with the provisioned model. It can also result in higher costs if you overprovision and have capacity that you don’t use.

By using Aurora Serverless v1, you can create a database endpoint without specifying the DB instance class size. You specify only the minimum and maximum range for the Aurora Serverless v1 DB cluster’s capacity. The Aurora Serverless v1 database endpoint makes up a router fleet that supports continuous connections and distributes the workload among resources. Aurora Serverless v1 scales the resources automatically based on your minimum and maximum capacity specifications.

### Description of TLS/SSL mode

<table>
<thead>
<tr>
<th>mysql</th>
<th>psql</th>
</tr>
</thead>
<tbody>
<tr>
<td>Try the connection using TLS/SSL first, but fall back to non-SSL if necessary.</td>
<td>PREFERRED</td>
</tr>
<tr>
<td>Enforce using TLS/SSL.</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>Enforce TLS/SSL and verify the CA.</td>
<td>VERIFY_CA</td>
</tr>
<tr>
<td>Enforce TLS/SSL, verify the CA, and verify the CA hostname.</td>
<td>VERIFY_IDENTITY</td>
</tr>
</tbody>
</table>

Aurora Serverless v1 uses wildcard certificates. If you specify the "verify CA" or the "verify CA and CA hostname" option when using TLS/SSL, first download the Amazon root CA 1 trust store from Amazon Trust Services. After doing so, you can identify this PEM-formatted file in your client command. To do so using the PostgreSQL Client:

For Linux, macOS, or Unix:

```
psql 'host=endpoint user=user sslmode=require sslrootcert=amazon-root-CA-1.pem dbname=db-name'
```

To learn more about working with the Aurora PostgreSQL database using the Postgres Client, see Connecting to a DB instance running the PostgreSQL database engine.

If you use the MySQL Client to connect with TLS/SSL's VERIFY_IDENTITY mode, currently you need to use the MySQL 8.0-compatible mysql command. For more information, see Connecting to a DB instance running the MySQL database engine.

For more information about connecting to Aurora DB clusters in general, see Connecting to an Amazon Aurora DB cluster (p. 253).
You don't need to change your database client application code to use the router fleet. Aurora Serverless v1 manages the connections automatically. Scaling is fast thanks to a "warm" resources pool that's always ready to service requests. Storage and processing are separate, so your Aurora Serverless v1 DB cluster can scale down to zero when it's finished processing workloads. When your Aurora Serverless v1 DB cluster scales to zero, you're charged only for storage.

Topics
- Aurora Serverless v1 architecture (p. 139)
- Autoscaling for Aurora Serverless (p. 140)
- Automatic pause and resume for Aurora Serverless v1 (p. 140)
- Timeout action for capacity changes (p. 141)
- Aurora Serverless v1 and parameter groups (p. 142)
- Aurora Serverless v1 and maintenance (p. 144)
- Aurora Serverless v1 and failover (p. 144)
- Aurora Serverless v1 and snapshots (p. 144)

### Aurora Serverless v1 architecture

The following image shows an overview the Aurora Serverless v1 architecture.

![Aurora Serverless v1 Architecture Diagram]

Instead of provisioning and managing database servers, you specify Aurora capacity units (ACUs). Each ACU is a combination of approximately 2 gigabytes (GB) of memory, corresponding CPU, and networking. Database storage automatically scales from 10 gibibytes (GiB) to 128 tebibytes (TiB), the same as storage in a standard Aurora DB cluster.

You can specify the minimum and maximum ACU. The minimum Aurora capacity unit is the lowest ACU to which the DB cluster can scale down. The maximum Aurora capacity unit is the highest ACU to which the DB cluster can scale up. Based on your settings, Aurora Serverless v1 automatically creates scaling rules for thresholds for CPU utilization, connections, and available memory.
Aurora Serverless v1 manages the warm pool of resources in an AWS Region to minimize scaling time. When Aurora Serverless v1 adds new resources to the Aurora DB cluster, it uses the router fleet to switch active client connections to the new resources. At any specific time, you are only charged for the ACUs that are being actively used in your Aurora DB cluster.

**Autoscaling for Aurora Serverless**

The capacity allocated to your Aurora Serverless v1 DB cluster seamlessly scales up and down based on the load generated by your client application. Here, load is CPU utilization and number of connections. Aurora Serverless v1 can also scale to zero capacity when there are no connections if you enable the pause-and-resume option for your DB cluster's capacity settings. For more information, see Automatic pause and resume for Aurora Serverless v1 (p. 140).

Aurora Serverless v1 scales up when capacity constraints are seen in CPU or connections. It also scales up when it detects performance issues that can be resolved by scaling up.

After scaling up, the cooldown period for scaling down is 15 minutes. After scaling down, the cooldown period for scaling down again is 310 seconds.

**Note**
There is no cooldown period for scaling up. Aurora Serverless v1 can scale up whenever necessary, including immediately after scaling up or scaling down.

A *scaling point* is a point in time at which the database can safely initiate the scaling operation. Under the following conditions, Aurora Serverless v1 might not be able to find a scaling point:

- Long-running queries or transactions are in progress
- Temporary tables or table locks are in use

If Aurora Serverless v1 can't find a scaling point, its behavior depends on the DB cluster's timeout action setting. Aurora Serverless v1 can force the change, or it can keep its original capacity if Aurora Serverless v1 can't find a scaling point before timing out. For more information, see Timeout action for capacity changes (p. 141).

You can see scaling events in the details for a DB cluster in the AWS Management Console. You can also monitor the current capacity allocated to the DB cluster by using the `ServerlessDatabaseCapacity` metric for Amazon CloudWatch.

During autoscaling, Aurora Serverless v1 resets the `EngineUptime` metric. The reset metric value doesn't indicate any issues with seamless scaling and doesn't mean that any connections were dropped. For more information about metrics, see Monitoring Amazon Aurora DB cluster metrics (p. 489).

**Automatic pause and resume for Aurora Serverless v1**

You can choose to pause your Aurora Serverless v1 DB cluster after a given amount of time with no activity. You specify the amount of time with no activity before the DB cluster is paused. When you select this option, the default inactivity time is five minutes, but you can change this value. This is an optional setting.

When the DB cluster is paused, no compute or memory activity occurs, and you are charged only for storage. If database connections are requested when an Aurora Serverless DB cluster is paused, the DB cluster automatically resumes and services the connection requests.

When the DB cluster resumes activity, it has the same capacity as it had when Aurora paused the cluster. The number of ACUs depends on how much Aurora scaled the cluster up or down before pausing it.

**Note**
If a DB cluster is paused for more than seven days, the DB cluster might be backed up with a snapshot. In this case, Aurora restores the DB cluster from the snapshot when there is a request to connect to it.
Timeout action for capacity changes

When your Aurora Serverless v1 DB cluster needs to scale its capacity for the current workload, it first tries to find a scaling point for making the change. The scaling point is the point at which your Aurora Serverless v1 DB cluster can safely start scaling to the resized capacity, without disrupting processing. To learn more about how Aurora Serverless v1 finds a scaling point, see Autoscaling for Aurora Serverless (p. 140).

If your Aurora Serverless v1 DB cluster can't find a scaling point within 5 minutes, it times out. Aurora Serverless v1 then takes the appropriate action based on your Aurora Serverless v1 DB cluster's `TimeoutAction` setting, as follows:

- **Force the capacity change** – If your Aurora Serverless v1 DB cluster can't find a scaling point before timing out, the `TimeoutAction` value of `ForceApplyCapacityChange` causes Aurora Serverless v1 to force the change. If Aurora Serverless v1 is processing a transaction, the transaction is interrupted and displays the following message:

  ERROR 1105 (HY000): The last transaction was aborted due to Seamless Scaling. Please retry.

  You can resubmit the transaction as soon as your Aurora Serverless v1 DB cluster is available.

- **Roll back the capacity change** – If your Aurora Serverless v1 DB cluster can't find the scaling point before timing out, the `TimeoutAction` value of `RollbackCapacityChange` causes Aurora Serverless v1 to stop looking for a scaling point. Instead, your Aurora Serverless v1 DB cluster remains at its original capacity.

You choose the timeout action when you create your Aurora Serverless v1 DB using the AWS Management Console or the AWS CLI. For more information, see Creating an Aurora Serverless v1 DB cluster (p. 145).

**Important**

For clusters with many concurrent connections, the `ForceApplyCapacityChange` setting can result in dropped connections for long-running queries and temporary tables. We recommend you choose `ForceApplyCapacityChange` only if appropriate for your use case.

You can also modify the timeout action and other capacity settings at any time. For more information, see Modifying an Aurora Serverless v1 DB cluster (p. 154).

For an Aurora Serverless v1 DB cluster that's already been configured, you can quickly get the settings by using the `describe-db-clusters` AWS CLI command. For example, if you have an Aurora Serverless v1 DB cluster running in the US-East (Northern Virginia) Region, you can run the following command.

```
$ aws rds describe-db-clusters --region us-east-1
```

You can see all details for the DB clusters associated with your AWS account displayed, including the `ScalingConfigurationInfo` as shown in the following output extract.

```
...
"ScalingConfigurationInfo": {
  "MinCapacity": 2,
  "MaxCapacity": 32,
  "AutoPause": true,
  "SecondsUntilAutoPause": 1200,
  "TimeoutAction": "RollbackCapacityChange"
},
...
```
As shown in the example, the Aurora Serverless v1 DB cluster as configured won't force the cluster to a new scaling point.

**Aurora Serverless v1 and parameter groups**

When you create your Aurora Serverless v1 DB cluster, you can create a single database instance using your chosen DB engine. Unlike Aurora provisioned DB clusters which can have multiple DB instances, Aurora Serverless v1 has a single read/write DB instance. In provisioned Aurora DB clusters, each DB instance has an associated *DB parameter group* that you can configure differently from instance to instance. An Aurora DB cluster has its own set of parameters in its associated *DB cluster parameter group*. These two general types of parameter groups control different operational aspects, some cluster-wide, some per instance, for a provisioned Aurora DB clusters.

Because Aurora Serverless v1 handles the DB instance capacity for you, parameter groups work differently for Aurora Serverless v1 DB clusters. As it's processing your workloads and scaling database capacity, Aurora Serverless v1 changes various parameters in its DB cluster parameter group as needed to work best for the increased or decreased capacity. That's why some of the default parameter values and other configuration details that you might use with other Aurora clusters don't apply for Aurora Serverless v1 clusters.

Your Aurora Serverless v1 DB cluster has an associated DB cluster parameter group only. Its DB cluster parameter group contains default values for any parameters that would typically be held in the DB parameter group of an Aurora provisioned DB cluster. You can't change the values of the default parameter groups of either type, nor can you change the values of the parameter group. However, you can create your own custom version of an Aurora DB cluster parameter group based on one of the provided DB cluster parameter groups and configure parameters as needed.

To get a list of available default parameters by engine type, see *Getting a list of parameters for Aurora Serverless v1* (p. 143)

**To create a custom DB cluster parameter group for Aurora Serverless v1**

1. Sign in to the AWS Management Console and then open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. Choose **Parameter groups**.
3. Choose **Create parameter group** to open the Parameter group details pane.
4. Choose the appropriate default DB cluster group for the DB engine you want to use for your Aurora Serverless v1 DB cluster. Be sure you choose the following options:
   a. For **Parameter group family**, choose the appropriate family for your chosen DB engine. Be sure your selection has the prefix `aurora-` in its name.
   b. For **Type**, choose **DB Cluster Parameter Group**.
   c. For **Group name** and **Description**, enter meaningful names for you or others who might need to work with your Aurora Serverless v1 DB cluster and its parameters.
   d. Choose **Create**.

Your custom DB cluster parameter group is added to the list of Parameter groups available to your account in your AWS Region. You can now use your custom DB cluster parameter group when you create new Aurora Serverless v1 DB clusters in the same Region.

You can also modify your existing Aurora Serverless v1 DB clusters to use your custom DB cluster parameter group. When you make changes such as this to an active DB cluster, Aurora Serverless v1 needs to start a seamless scale so that it can apply the parameter changes. If the Aurora Serverless v1 DB cluster is paused, it resumes and starts scaling. The scaling operation for a parameter group change uses the `ForceApplyCapacityChange` timeout action. That means that if your Aurora Serverless v1 DB
Getting a list of parameters for Aurora Serverless v1

By using the AWS CLI, you can get a list of default parameters available for Aurora Serverless v1 for specific DB engine. You run the describe-engine-default-cluster-parameters command and query the AWS Region that you plan to use for your Aurora Serverless v1 DB cluster. Or you can invoke the DescribeEngineDefaultClusterParameters API operation.

Before using the CLI commands, configure your AWS CLI with your AWS Access Key ID and AWS Secret Access Key. Also configure the AWS Region for your AWS CLI, to avoid needing to use the --region parameter in the command. To learn how, see Configuration basics in the AWS Command Line Interface User Guide.

You can get a list of the parameters available for an Aurora MySQL Serverless DB cluster. For Aurora MySQL 5.7, the default DB cluster parameter group is aurora5.6, as shown in the following.

For Linux, macOS, or Unix:

```bash
aws rds describe-engine-default-cluster-parameters
    --db-parameter-group-family aurora5.6 --query
    'EngineDefaults.Parameters[*].
      {ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} | [?
        contains(SupportedEngineModes, 'serverless') == 'true'] | [*].{param:ParameterName}'
    --output text
```

For Windows:

```bash
aws rds describe-engine-default-cluster-parameters
    --db-parameter-group-family aurora5.6 --query
    "EngineDefaults.Parameters[*].
      {ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} | [?
        contains(SupportedEngineModes, 'serverless') == 'true'] | [*].{param:ParameterName}"
    --output text
```

You can get a list of default parameters from Aurora PostgreSQL Serverless DB cluster parameter group with the following AWS CLI command. In this example, the default DB cluster parameter group being queried is aurora-postgresql10.

For Linux, macOS, or Unix:

```bash
aws rds describe-engine-default-cluster-parameters
    --db-parameter-group-family aurora-postgresql10 --query
    'EngineDefaults.Parameters[*].
      {ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} | [?
        contains(SupportedEngineModes, 'serverless') == 'true'] | [*].{param:ParameterName}'
    --output text
```

For Windows:

```bash
aws rds describe-engine-default-cluster-parameters
    --db-parameter-group-family aurora-postgresql10 --query
    "EngineDefaults.Parameters[*].
      {ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} | [?
        contains(SupportedEngineModes, 'serverless') == 'true'] | [*].{param:ParameterName}"
    --output text
```
For more information, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

**Aurora Serverless v1 and maintenance**

Maintenance for Aurora Serverless v1 DB cluster, such as applying the latest features, fixes, and security updates, is performed automatically for you. Unlike provisioned Aurora DB clusters, Aurora Serverless v1 doesn't have user-settable maintenance windows. However, it does have a maintenance window that you can view in the AWS Management Console in **Maintenance & backups** for your Aurora Serverless v1 DB cluster. You can find the date and time that maintenance might be performed and if any maintenance is pending for your Aurora Serverless v1 DB cluster, as shown following.

Whenever possible, Aurora Serverless v1 performs maintenance in a non-disruptive manner. When maintenance is required, your Aurora Serverless v1 DB cluster scales its capacity to handle the necessary operations. Before scaling, Aurora Serverless v1 looks for a scaling point and it does so for up to seven days if necessary.

At the end of each day that Aurora Serverless v1 can't find a scaling point, it creates a cluster event. This event notifies you of the pending maintenance and the need to scale to perform maintenance. The notification includes the date when the Aurora Serverless v1 can force the DB cluster to scale.

Until that time, your Aurora Serverless v1 DB cluster continues looking for a scaling point and behaves according to its **TimeoutAction** setting. That is, if it can't find a scaling point before timing out, it abandons the capacity change if it's configured to **RollbackCapacityChange**. Or it forces the change if it's set to **ForceApplyCapacityChange**. As with any change that's forced without an appropriate scaling point, this might interrupt your workload.

For more information, see Timeout action for capacity changes (p. 141).

**Aurora Serverless v1 and failover**

If the DB instance for an Aurora Serverless v1 DB cluster becomes unavailable or the Availability Zone (AZ) it is in fails, Aurora recreates the DB instance in a different AZ. We refer to this capability as automatic multi-AZ failover.

This failover mechanism takes longer than for an Aurora provisioned cluster. The Aurora Serverless v1 failover time is currently undefined because it depends on demand and capacity availability in other AZs within the given AWS Region.

Because Aurora separates computation capacity and storage, the storage volume for the cluster is spread across multiple AZs. Your data remains available even if outages affect the DB instance or the associated AZ.

**Aurora Serverless v1 and snapshots**

The cluster volume for an Aurora Serverless v1 cluster is always encrypted. You can choose the encryption key, but you can’t disable encryption. To copy or share a snapshot of an Aurora Serverless v1 cluster, you encrypt the snapshot using your own AWS Key Management Service customer master key (CMK). For more information, see Copying a DB cluster snapshot. To learn more about encryption and Amazon Aurora, see Encrypting Amazon Aurora resources.
Creating an Aurora Serverless v1 DB cluster

When you create an Aurora Serverless v1 DB cluster, you can set the minimum and maximum capacity for the cluster. A capacity unit is equivalent to a specific compute and memory configuration. Aurora Serverless creates scaling rules for thresholds for CPU utilization, connections, and available memory and seamlessly scales to a range of capacity units as needed for your applications. For more information see Aurora Serverless v1 architecture (p. 139).

You can set the following specific values for your Aurora Serverless v1 DB cluster:

- **Minimum Aurora capacity unit** – Aurora Serverless v1 can reduce capacity down to this capacity unit.
- **Maximum Aurora capacity unit** – Aurora Serverless v1 can increase capacity up to this capacity unit.

You can also choose the following optional scaling configuration options:

- **Force scaling the capacity to the specified values when the timeout is reached** – You can choose this setting if you want Aurora Serverless v1 to force Aurora Serverless v1 to scale even if it can't find a scaling point before it times out. If you want Aurora Serverless v1 to cancel capacity changes if it can't find a scaling point, don't choose this setting. For more information, see Timeout action for capacity changes (p. 141).
- **Pause compute capacity after consecutive minutes of inactivity** – You can choose this setting if you want Aurora Serverless v1 to scale to zero when there's no activity on your DB cluster for an amount of time you specify. With this setting enabled, your Aurora Serverless v1 DB cluster automatically resumes processing and scales to the necessary capacity to handle the workload when database traffic resumes.

Before you can create an Aurora Serverless v1 DB cluster, you need an AWS account. You also need to have completed the setup tasks for working with Amazon Aurora. For more information, see Setting up your environment for Amazon Aurora (p. 73). You also need to complete other preliminary steps for creating any Aurora DB cluster. To learn more, see Creating an Amazon Aurora DB cluster (p. 118).

Aurora Serverless v1 is available in certain AWS Regions and for specific Aurora MySQL and Aurora PostgreSQL versions only. For more information, see Aurora Serverless v1 (p. 21).

**Note**

The cluster volume for an Aurora Serverless v1 cluster is always encrypted. When you create your Aurora Serverless v1 DB cluster, you can't turn off encryption, but you can choose to use your own encryption key.

You can create an Aurora Serverless v1 DB cluster with the AWS Management Console, the AWS CLI, or the RDS API by following the steps below.

**Console**

To create a new Aurora Serverless v1 DB cluster, you sign in to the AWS Management Console and choose an AWS Region that supports Aurora Serverless v1. Choose Amazon RDS from the AWS Services list, and then choose Create database.

On the Create database page:

- Choose **Standard Create** for the database creation method.
- Choose **Amazon Aurora** for the Engine type in the Engine options section.

You then choose **Amazon Aurora with MySQL compatibility** or **Amazon Aurora with PostgreSQL compatibility** and continue creating the Aurora Serverless v1 DB cluster by using the steps from the
following examples. If you choose a version of the DB engine that doesn't support Aurora Serverless v1, the Serverless option doesn't display.

Example for Aurora MySQL

Choose Amazon Aurora with MySQL Compatibility for the Edition. Choose the Aurora MySQL engine you want for your cluster from the Version selector. The following image shows an example.

Choose Serverless for the Capacity type.

You can configure the scaling configuration of the Aurora Serverless v1 DB cluster by adjusting values in the Capacity settings section of the page. To learn more about capacity settings, see Autoscaling for Aurora Serverless (p. 140). The following image shows the Capacity settings you can adjust for an Aurora MySQL Serverless DB cluster.
You can also enable the Data API for your Aurora MySQL Serverless DB cluster. Select the Data API checkbox in the Connectivity section of the Create database page. To learn more about the Data API, see Using the Data API for Aurora Serverless (p. 162).

Example for Aurora PostgreSQL

Choose Amazon Aurora with Postgres; Compatibility for the Edition and select the Version of Aurora PostgreSQL available for Aurora Serverless v1. For more information, see Aurora Serverless v1 (p. 21).
You can configure the scaling configuration of the Aurora Serverless v1 DB cluster by adjusting values in the **Capacity settings** section of the page. The following image shows the **Capacity settings** you can adjust for an Aurora PostgreSQL Serverless DB cluster. To learn more about capacity settings, see [Autoscaling for Aurora Serverless](p. 140).

### Capacity settings

This billing estimate is based on published prices. [Learn more](#)

<table>
<thead>
<tr>
<th>Minimum Aurora capacity unit</th>
<th>Info</th>
<th>Maximum Aurora capacity unit</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 4GB RAM</td>
<td></td>
<td>384 768GB RAM</td>
<td></td>
</tr>
</tbody>
</table>

**Additional scaling configuration**

- [ ] Force scaling the capacity to the specified values when the timeout is reached [Info]
  
  Enable to force capacity scaling as soon as possible. Disable to cancel the capacity changes when a timeout is reached.

- [x] Pause compute capacity after consecutive minutes of inactivity [Info]
  
  You are only charged for database storage while the compute capacity is paused.

  - [ ] hours
  - [ ] minutes
  - [ ] seconds

  Max: 24 hours
You can also enable the Data API for your Aurora MySQL Serverless DB cluster. Select the Data API checkbox in the Connectivity section of the Create database page. See Using the Data API for Aurora Serverless (p. 162) for more information about the Data API.

For more information on creating an Aurora DB cluster using the AWS Management Console, see Creating an Amazon Aurora DB cluster (p. 118).

**Note**
If you receive the following error message when trying to create your cluster, your account needs additional permissions.

Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.
See Using service-linked roles for Amazon Aurora (p. 1277) for more information.

You can't directly connect to the DB instance on your Aurora Serverless v1 DB cluster. To connect to your Aurora Serverless v1 DB cluster, you use the database endpoint. You can find the endpoint for your Aurora Serverless v1 DB cluster on the Connectivity & security tab for your cluster in the AWS Management Console. For more information, see Connecting to an Amazon Aurora DB cluster (p. 253).

**AWS CLI**

To create a new Aurora Serverless v1 DB cluster with the AWS CLI, run the create-db-cluster command and specify serverless for the --engine-mode option.

You can optionally specify the --scaling-configuration option to configure the minimum capacity, maximum capacity, and automatic pause when there are no connections.

The following command examples create a new Serverless DB cluster by setting the --engine-mode option to serverless. The examples also specify values for the --scaling-configuration option.

**Example for Aurora MySQL**

The following commands create new MySQL–compatible Serverless DB clusters. Valid capacity values for Aurora MySQL are 1, 2, 4, 8, 16, 32, 64, 128, and 256.

For Linux, macOS, or Unix:

```bash
aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora --engine-version 5.6.10a \
--engine-mode serverless --scaling-configuration MinCapacity=4,MaxCapacity=32,SecondsUntilAutoPause=1000,AutoPause=true \
--master-username username --master-user-password password

aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.07.1 \
--engine-mode serverless --scaling-configuration MinCapacity=4,MaxCapacity=32,SecondsUntilAutoPause=1000,AutoPause=true \
--master-username username --master-user-password password
```

For Windows:

```bash
aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora --engine-version 5.6.10a ^ \
--engine-mode serverless --scaling-configuration MinCapacity=4,MaxCapacity=32,SecondsUntilAutoPause=1000,AutoPause=true ^ \
--master-username username --master-user-password password
```

149
Restoring an Aurora Serverless v1 DB cluster

You can configure an Aurora Serverless v1 DB cluster when you restore a provisioned DB cluster snapshot with the AWS Management Console, the AWS CLI, or the RDS API.

When you restore a snapshot to an Aurora Serverless v1 DB cluster, you can set the following specific values:

- **Minimum Aurora capacity unit** – Aurora Serverless v1 can reduce capacity down to this capacity unit.
- **Maximum Aurora capacity unit** – Aurora Serverless v1 can increase capacity up to this capacity unit.
- **Timeout action** – The action to take when a capacity modification times out because it can’t find a scaling point. Aurora Serverless v1 DB cluster can force your DB cluster to the new capacity settings if
set the **Force scaling the capacity to the specified values**... option. Or, it can roll back the capacity change to cancel it if you don't choose the option. For more information, see Timeout action for capacity changes (p. 141).

- **Pause after inactivity** – The amount of time with no database traffic to scale to zero processing capacity. When database traffic resumes, Aurora automatically resumes processing capacity and scales to handle the traffic.

For general information about restoring a DB cluster from a snapshot, see Restoring from a DB cluster snapshot (p. 420).

**Console**

You can restore a DB cluster snapshot to an Aurora DB cluster with the AWS Management Console.

**To restore a DB cluster snapshot to an Aurora DB cluster**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region that hosts your source DB cluster.
3. In the navigation pane, choose **Snapshots**, and choose the DB cluster snapshot that you want to restore.
4. For **Actions**, choose **Restore Snapshot**.
5. On the **Restore DB Cluster** page, choose **Serverless** for **Capacity type**.

6. In the **DB cluster identifier** field, type the name for your restored DB cluster, and complete the other fields.
7. In the **Capacity settings** section, modify the scaling configuration.
8. Choose **Restore DB Cluster**.

To connect to an Aurora Serverless v1 DB cluster, use the database endpoint. For details, see the instructions in **Connecting to an Amazon Aurora DB cluster** (p. 253).

**Note**
If you encounter the following error message, your account requires additional permissions: Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.
For more information, see **Using service-linked roles for Amazon Aurora** (p. 1277).

**AWS CLI**
You can configure an Aurora Serverless v1 DB cluster when you restore from a snapshot of another DB cluster. You can do so with the AWS CLI by using the `restore-db-cluster-from-snapshot` CLI command. With your command, you include the following required parameters:

- `--db-cluster-identifier mynewdbcluster`
- `--snapshot-identifier mydbclustersnapshot`
- `--engine-mode serverless`

To restore a snapshot to an Aurora Serverless v1 cluster with MySQL 5.7 compatibility, include the following additional parameters:

- `--engine aurora-mysql`
• --engine-version 5.7

The --engine and --engine-version parameters let you create a MySQL 5.7-compatible Aurora Serverless v1 cluster from a MySQL 5.6-compatible Aurora or Aurora Serverless v1 snapshot. The following example restores a snapshot from a MySQL 5.6-compatible cluster named mydbclustersnapshot to a MySQL 5.7-compatible Aurora Serverless v1 cluster named mynewdbcluster.

For Linux, macOS, or Unix:

```bash
aws rds restore-db-cluster-from-snapshot --db-cluster-identifier mynewdbcluster --snapshot-identifier mydbclustersnapshot --engine-mode serverless --engine aurora-mysql --engine-version 5.7
```

For Windows:

```bash
aws rds restore-db-cluster-from-snapshot --db-instance-identifier mynewdbcluster --db-snapshot-identifier mydbclustersnapshot --engine-mode serverless --engine aurora-mysql --engine-version 5.7
```

You can optionally specify the --scaling-configuration option to configure the minimum capacity, maximum capacity, and automatic pause when there are no connections. Valid capacity values include the following:

• Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128, and 256.
• Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192, and 384.

In the following example, you restore from a previously created DB cluster snapshot named mydbclustersnapshot to a new DB cluster named mynewdbcluster. You set the --scaling-configuration so that the new Aurora Serverless DB cluster can scale from 8 ACUs to 64 ACUs (Aurora capacity units) as needed to process the workload. After processing completes and after 1000 seconds with no connections to support, the cluster shuts down until connection requests prompt it to restart.

For Linux, macOS, or Unix:

```bash
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=1000,AutoPause=true
```

For Windows:

```bash
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=1000,AutoPause=true
```
RDS API

To configure an Aurora Serverless v1 DB cluster when you restore from a DB cluster using the RDS API, run the RestoreDBClusterFromSnapshot operation and specify serverless for the EngineMode parameter.

You can optionally specify the ScalingConfiguration parameter to configure the minimum capacity, maximum capacity, and automatic pause when there are no connections. Valid capacity values include the following:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128, and 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192, and 384.

Modifying an Aurora Serverless v1 DB cluster

After you configure an Aurora Serverless v1 DB cluster, you can modify its scaling configuration with the AWS Management Console, the AWS CLI, or the RDS API.

You can set the minimum and maximum capacity for the DB cluster. Each capacity unit is equivalent to a specific compute and memory configuration. Aurora Serverless v1 automatically creates scaling rules for thresholds for CPU utilization, connections, and available memory. You can also set whether Aurora Serverless v1 pauses the database when there's no activity and then resumes when activity begins again.

You can set the following specific values:

- **Minimum Aurora capacity unit** – Aurora Serverless v1 can reduce capacity down to this capacity unit.
- **Maximum Aurora capacity unit** – Aurora Serverless v1 can increase capacity up to this capacity unit.
- **Timeout action** – The action to take when a capacity modification times out because it can't find a scaling point. Aurora can force the capacity change to set the capacity to the specified value as soon as possible. Or, it can roll back the capacity change to cancel it. For more information, see Timeout action for capacity changes (p. 141).
- **Pause after inactivity** – The amount of time with no database traffic to scale to zero processing capacity. When database traffic resumes, Aurora automatically resumes processing capacity and scales to handle the traffic.

Console

You can modify the scaling configuration of an Aurora DB cluster with the AWS Management Console.

To modify an Aurora Serverless v1 DB cluster

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the Aurora Serverless v1 DB cluster that you want to modify.
4. For Actions, choose Modify cluster.
5. In the Capacity settings section, modify the scaling configuration.
6. Choose **Continue**.
7. Choose **Modify cluster**.

The change is applied immediately.

**AWS CLI**

To modify the scaling configuration of an Aurora Serverless v1 DB cluster using the AWS CLI, run the `modify-db-cluster` AWS CLI command. Specify the `--scaling-configuration` option to configure the minimum capacity, maximum capacity, and automatic pause when there are no connections. Valid capacity values include the following:

- **Aurora MySQL**: 1, 2, 4, 8, 16, 32, 64, 128, and 256.
- **Aurora PostgreSQL**: 2, 4, 8, 16, 32, 64, 192, and 384.

In this example, you modify the scaling configuration of an Aurora Serverless v1 DB cluster named `sample-cluster`.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster --db-cluster-identifier sample-cluster --scaling-configuration MinCapacity=8,MaxCapacity=64,SecondsUntilAutoPause=500,TimeoutAction='ForceApplyCapacityChange',AutoPause=true
```

---

6. Choose **Continue**.
7. Choose **Modify cluster**.

The change is applied immediately.

**AWS CLI**

To modify the scaling configuration of an Aurora Serverless v1 DB cluster using the AWS CLI, run the `modify-db-cluster` AWS CLI command. Specify the `--scaling-configuration` option to configure the minimum capacity, maximum capacity, and automatic pause when there are no connections. Valid capacity values include the following:

- **Aurora MySQL**: 1, 2, 4, 8, 16, 32, 64, 128, and 256.
- **Aurora PostgreSQL**: 2, 4, 8, 16, 32, 64, 192, and 384.

In this example, you modify the scaling configuration of an Aurora Serverless v1 DB cluster named `sample-cluster`.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster --db-cluster-identifier sample-cluster --scaling-configuration MinCapacity=8,MaxCapacity=64,SecondsUntilAutoPause=500,TimeoutAction='ForceApplyCapacityChange',AutoPause=true
```
For Windows:

```
aws rds modify-db-cluster --db-cluster-identifier sample-cluster ^
  --scaling-configuration
  MinCapacity=8,MaxCapacity=64,SecondsUntilAutoPause=500,TimeoutAction='ForceApplyCapacityChange',AutoPause=true
```

### RDS API

You can modify the scaling configuration of an Aurora DB cluster with the `ModifyDBCluster` API operation. Specify the `ScalingConfiguration` parameter to configure the minimum capacity, maximum capacity, and automatic pause when there are no connections. Valid capacity values include the following:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128, and 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192, and 384.

### Scaling Aurora Serverless v1 DB cluster capacity manually

Typically, Aurora Serverless v1 DB clusters scale seamlessly based on the workload. However, capacity might not always scale fast enough to meet sudden extremes, such as an exponential increase in transactions. In such cases you can initiate the scaling operation manually by setting a new capacity value. After you set the capacity explicitly, Aurora Serverless v1 automatically scales the DB cluster. It does so based on the cooldown period for scaling down.

You can explicitly set the capacity of an Aurora Serverless v1 DB cluster to a specific value with the AWS Management Console, the AWS CLI, or the RDS API.

#### Console

You can set the capacity of an Aurora DB cluster with the AWS Management Console.

**To modify an Aurora Serverless v1 DB cluster**

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. Choose the Aurora Serverless v1 DB cluster that you want to modify.
4. For **Actions**, choose **Set capacity**.
5. In the **Scale database capacity** window, choose the following:

   a. For the **Scale DB cluster to** drop-down selector, choose the new capacity that you want for your DB cluster.

   b. For the **If a seamless scaling point cannot be found...** checkbox, choose the behavior you want for your Aurora Serverless v1 DB cluster's `TimeoutAction` setting, as follows:

      - Uncheck this option if you want your capacity to remain unchanged if Aurora Serverless v1 can't find a scaling point before timing out.
      - Check this option if you want to force your Aurora Serverless v1 DB cluster change its capacity even if it can't find a scaling point before timing out. This option can result Aurora Serverless v1 dropping connections that prevent it from finding a scaling point.
c. In the seconds field, enter the amount of time you want to allow your Aurora Serverless v1 DB cluster to look for a scaling point before timing out. You can specify anywhere from 10 seconds to 600 seconds (10 minutes). The default is five minutes (300 seconds). This following example forces the Aurora Serverless v1 DB cluster to scale down to 2 ACUs even if it can’t find a scaling point within five minutes.

6. Choose Apply.

To learn more about scaling points, TimeoutAction, and cooldown periods, see Autoscaling for Aurora Serverless (p. 140).

AWS CLI

To set the capacity of an Aurora Serverless v1 DB cluster using the AWS CLI, run the modify-current-db-cluster-capacity AWS CLI command, and specify the --capacity option. Valid capacity values include the following:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128, and 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192, and 384.

In this example, you set the capacity of an Aurora Serverless v1 DB cluster named sample-cluster to 64.

```bash
aws rds modify-current-db-cluster-capacity --db-cluster-identifier sample-cluster --capacity 64
```
RDS API

You can set the capacity of an Aurora DB cluster with the `ModifyCurrentDBClusterCapacity` API operation. Specify the `Capacity` parameter. Valid capacity values include the following:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128, and 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192, and 384.

Viewing Aurora Serverless v1 DB clusters

After you create one or more Aurora Serverless v1 DB clusters, you can view which DB clusters are type `Serverless` and which are type `Instance`. You can also view the current number of Aurora capacity units (ACUs) each Aurora Serverless v1 DB cluster is using. Each ACU is a combination of processing (CPU) and memory (RAM) capacity.

To view your Aurora Serverless v1 DB clusters

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region in which you created the Aurora Serverless v1 DB clusters.
3. In the navigation pane, choose Databases.

   For each DB cluster, the DB cluster type is shown under Role. The Aurora Serverless v1 DB clusters show `Serverless` for the type. You can view an Aurora Serverless v1 DB cluster’s current capacity under Size.

4. Choose the name of an Aurora Serverless v1 DB cluster to display its details.

   On the Connectivity & security tab, note the database endpoint. Use this endpoint to connect to your Aurora Serverless v1 DB cluster.

Choose the Configuration tab to view the capacity settings.
A 

A *scaling event* is generated when the DB cluster scales up, scales down, pauses, or resumes. Choose the *Logs & events* tab to see recent events. The following image shows examples of these events.

Monitoring capacity and scaling events for your Aurora Serverless v1 DB cluster

You can view your Aurora Serverless v1 DB cluster in CloudWatch to monitor the capacity allocated to the DB cluster with the `ServerlessDatabaseCapacity` metric. You can also monitor all of the standard Aurora CloudWatch metrics, such as `CPUUtilization`, `DatabaseConnections`, `Queries`, and so on. To learn more about how to monitor Aurora DB clusters through CloudWatch, see *Monitoring log events in Amazon CloudWatch (p. 827).*

You can have Aurora publish some or all database logs to CloudWatch. You select the logs to publish by enabling the configuration parameters such as `general_log` and `slow_query_log` in the DB cluster parameter group associated with the Aurora Serverless v1 cluster. Unlike provisioned clusters, Aurora Serverless v1 clusters don't require you to specify in the DB cluster settings which log types to upload to CloudWatch. Aurora Serverless v1 clusters automatically upload all the available logs. When you disable a log configuration parameter, publishing of the log to CloudWatch stops. You can also delete the logs in CloudWatch if they are no longer needed. For more information about Aurora Serverless v1 DB cluster parameter groups, see *Aurora Serverless v1 and parameter groups (p. 142).*

To connect to an Aurora Serverless v1 DB cluster, use the database endpoint. For more information, see *Connecting to an Amazon Aurora DB cluster (p. 253).*

**Note**

You can't connect directly to specific DB instances in your Aurora Serverless v1 DB clusters.

Deleting an Aurora Serverless v1 DB cluster

When you create an Aurora Serverless v1 DB cluster using the AWS Management Console, the *Enable default protection* option is enabled by default unless you deselect it. That means that you can't immediately delete an Aurora Serverless v1 DB cluster that has *Deletion protection* enabled. To delete Aurora Serverless v1 DB clusters that have deletion protection by using the AWS Management Console, you first modify the cluster to remove this protection. For information about using the AWS CLI for this task, see *AWS CLI (p. 161).*
To disable deletion protection using the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **DB clusters**.
3. Choose your Aurora Serverless v1 DB cluster from the list.
4. Choose **Modify** to open your DB cluster's configuration. The Modify DB cluster page opens the Settings, Capacity settings, and other configuration details for your Aurora Serverless v1 DB cluster. Deletion protection is in the **Additional configuration** section.
5. Uncheck the **Enable deletion protection** option in the **Additional configuration** properties card.
6. Choose **Continue**. The **Summary of modifications** appears.
7. Choose **Modify cluster** to accept the summary of modifications. You can also choose **Back** to modify your changes or **Cancel** to discard your changes.

After deletion protection is no longer active, you can delete your Aurora Serverless v1 DB cluster by using the AWS Management Console.

**Console**

To delete an Aurora Serverless v1 DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the **Resources** section, choose **DB Clusters**.
3. Choose the Aurora Serverless v1 DB cluster that you want to delete.
4. For **Actions**, choose **Delete**. You're prompted to confirm that you want to delete your Aurora Serverless v1 DB cluster.
5. We recommend that you keep the preselected options:
   - **Yes** for **Create final snapshot**?
   - Your Aurora Serverless v1 DB cluster name plus `-final-snapshot` for **Final snapshot name**. However, you can change the name for your final snapshot in this field.

If you choose **No** for **Create final snapshot**? you can't restore your DB cluster using snapshots or point-in-time recovery.

6. Choose **Delete DB cluster**.

Aurora Serverless v1 deletes your DB cluster. If you chose to have a final snapshot, you see your Aurora Serverless v1 DB cluster's status change to "Backing-up" before it's deleted and no longer appears in the list.
AWS CLI

Before you begin, configure your AWS CLI with your AWS Access Key ID, AWS Secret Access Key, and the AWS Region where your Aurora Serverless v1 DB cluster For more information, see Configuration basics in the AWS Command Line Interface User Guide.

You can't delete an Aurora Serverless v1 DB cluster until after you first disable deletion protection for clusters configured with this option. If you try to delete a cluster that has this protection option enabled, you see the following error message.

An error occurred (InvalidParameterCombination) when calling the DeleteDBCluster operation: Cannot delete protected Cluster, please disable deletion protection and try again.

You can change your Aurora Serverless v1 DB cluster's deletion-protection setting by using the modify-db-cluster AWS CLI command as shown in the following:

```
aws rds modify-db-cluster --db-cluster-identifier your-cluster-name --no-deletion-protection
```

This command returns the revised properties for the specified DB cluster. You can now delete your Aurora Serverless v1 DB cluster.

We recommend that you always create a final snapshot whenever you delete an Aurora Serverless v1 DB cluster. The following example of using the AWS CLI delete-db-cluster shows you how. You provide the name of your DB cluster and a name for the snapshot.

For Linux, macOS, or Unix:

```
aws rds delete-db-cluster --db-cluster-identifier your-cluster-name --no-skip-final-snapshot --final-db-snapshot-identifier name-your-snapshot
```

For 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 and Aurora database engine versions

Aurora Serverless v1 is available in certain AWS Regions and for specific Aurora MySQL and Aurora PostgreSQL versions only. For the current list of AWS Regions that support Aurora Serverless v1 and the specific Aurora MySQL and Aurora PostgreSQL versions available in each Region, see Aurora Serverless v1 (p. 21).

Aurora Serverless v1 uses its associated Aurora database engine to identify specific supported releases for each database engine supported, as follows:

- Aurora MySQL Serverless
- Aurora PostgreSQL Serverless

When minor releases of the database engines become available for Aurora Serverless v1, they are applied automatically in the various AWS Regions where Aurora Serverless v1 is available. In other words,
you don’t need to upgrade your Aurora Serverless v1 DB cluster to get a new minor release for your cluster’s DB engine when it’s available for Aurora Serverless v1.

**Aurora MySQL Serverless**

If you want to use Aurora with MySQL compatibility for your Aurora Serverless v1 DB cluster, you can choose between Aurora MySQL 5.6-compatible or Aurora MySQL 5.7-compatible versions. These two editions of Aurora MySQL differ significantly. We recommend that you compare their differences before creating your Aurora Serverless v1 DB cluster so that you make the right choice for your use case. To learn about enhancements and bug fixes for Aurora MySQL Serverless 5.6 and 5.7, see Database engine updates for Aurora MySQL Serverless clusters (p. 977).

**Aurora PostgreSQL Serverless**

If you want to use Aurora PostgreSQL for your Aurora Serverless v1 DB cluster, you have a single version available to use. Minor releases for Aurora with PostgreSQL compatibility include only changes that are backward-compatible. Your Aurora Serverless v1 DB cluster is transparently upgraded when an Aurora PostgreSQL minor release becomes available for Aurora Serverless v1 in your Region.

For example, the minor version Aurora PostgreSQL 10.12 release was transparently applied to all Aurora Serverless v1 DB clusters running the prior Aurora PostgreSQL version. For more information about the Aurora PostgreSQL version 10.12 update, see Version 2.5, compatible with PostgreSQL 10.12 (p. 1163).

**Using the Data API for Aurora Serverless**

By using the Data API for Aurora Serverless, you can work with a web-services interface to your Aurora Serverless DB cluster. The Data API doesn’t require a persistent connection to the DB cluster. Instead, it provides a secure HTTP endpoint and integration with AWS SDKs. You can use the endpoint to run SQL statements without managing connections.

All calls to the Data API are synchronous. By default, a call times out if it’s not finished processing within 45 seconds. However, you can continue running a SQL statement if the call times out by using the `continueAfterTimeout` parameter. For an example, see Running a SQL transaction (p. 182).

Users don’t need to pass credentials with calls to the Data API, because the Data API uses database credentials stored in AWS Secrets Manager. To store credentials in Secrets Manager, users must be granted the appropriate permissions to use Secrets Manager, and also the Data API. For more information about authorizing users, see Authorizing access to the Data API (p. 163).

You can also use Data API to integrate Aurora Serverless with other AWS applications such as AWS Lambda, AWS AppSync, and AWS Cloud9. The API provides a more secure way to use AWS Lambda. It enables you to access your DB cluster without your needing to configure a Lambda function to access resources in a virtual private cloud (VPC). For more information, see AWS Lambda, AWS AppSync, and AWS Cloud9.

You can enable the Data API when you create the Aurora Serverless cluster. You can also modify the configuration later. For more information, see Enabling the Data API (p. 166).

After you enable the Data API, you can also use the query editor for Aurora Serverless. For more information, see Using the query editor for Aurora Serverless (p. 188).

**Topics**

- Data API availability (p. 163)
- Authorizing access to the Data API (p. 163)
- Enabling the Data API (p. 166)
Creating an Amazon VPC endpoint for the Data API (AWS PrivateLink) (p. 167)

Calling the Data API (p. 169)

Using the Java client library for Data API (p. 184)

Troubleshooting Data API issues (p. 185)

Data API availability

The Data API can be enabled for Aurora Serverless DB clusters using specific Aurora MySQL and Aurora PostgreSQL versions only. For more information, see Data API for Aurora Serverless (p. 23).

The following table shows the AWS Regions where the Data API is currently available for Aurora Serverless. To access the Data API in these Regions, use the HTTPS protocol.

<table>
<thead>
<tr>
<th>Region</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>rds-data.ap-southeast-1.amazonaws.com</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>rds-data.ap-southeast-2.amazonaws.com</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>rds-data.ap-northeast-1.amazonaws.com</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>rds-data.ap-south-1.amazonaws.com</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>rds-data.eu-central-1.amazonaws.com</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>rds-data.eu-west-1.amazonaws.com</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>rds-data.eu-west-2.amazonaws.com</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>rds-data.eu-west-3.amazonaws.com</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>rds-data.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td>US East (Ohio)</td>
<td>rds-data.us-east-2.amazonaws.com</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>rds-data.us-west-1.amazonaws.com</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>rds-data.us-west-2.amazonaws.com</td>
</tr>
</tbody>
</table>

Authorizing access to the Data API

Users can invoke Data API operations only if they are authorized to do so. You can give a user permission to use the Data API by attaching an AWS Identity and Access Management (IAM) policy that defines their privileges. You can also attach the policy to a role if you're using IAM roles. An AWS managed policy, AmazonRDSDataFullAccess, includes permissions for the RDS Data API.

The AmazonRDSDataFullAccess policy also includes permissions for the user to get the value of a secret from AWS Secrets Manager. Users need to use Secrets Manager to store secrets that they can use in their calls to the Data API. Using secrets means that users don't need to include database credentials for the resources that they target in their calls to the Data API. The Data API transparently calls Secrets Manager, which allows (or denies) the user's request for the secret. For information about setting up secrets to use with the Data API, see Storing database credentials in AWS Secrets Manager (p. 165).

The AmazonRDSDataFullAccess policy provides complete access (through the Data API) to resources. You can narrow the scope by defining your own policies that specify the Amazon Resource Name (ARN) of a resource.
For example, the following policy shows an example of the minimum required permissions for a user to access the Data API for the DB cluster identified by its ARN. The policy includes the needed permissions to access Secrets Manager and get authorization to the DB instance for the user.

```json
{
    "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"
            ],
        }
    ]
}
```

We recommend that you use a specific ARN for the "Resources" element in your policy statements (as shown in the example) rather than a wildcard (*).

**Working with tag-based authorization**

The Data API and Secrets Manager both support tag-based authorization. *Tags* are key-value pairs that label a resource, such as an RDS cluster, with an additional string value, for example:

- environment:production
- environment:development

You can apply tags to your resources for cost allocation, operations support, access control, and many other reasons. (If you don’t already have tags on your resources and you want to apply them, you can learn more at [Tagging Amazon RDS resources](https:)). You can use the tags in your policy statements to limit access to the RDS clusters that are labeled with these tags. As an example, an Aurora DB cluster might have tags that identify its environment as either production or development.

The following example shows how you can use tags in your policy statements. This statement requires that both the cluster and the secret passed in the Data API request have an `environment:production` tag.

Here's how the policy gets applied: When a user makes a call using the Data API, the request is sent to the service. The Data API first verifies that the cluster ARN passed in the request is tagged with `environment:production`. It then calls Secrets Manager to retrieve the value of the user's secret in the request. Secrets Manager also verifies that the user's secret is tagged with `environment:production`. If so, Data API then uses the retrieved value for the user's DB password. Finally, if that's also correct, the Data API request is invoked successfully for the user.

```json
{
    "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"
            ],
        }
    ]
}
```
"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:*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }
]
}

The example shows separate actions for rds-data and secretsmanager for the Data API and Secrets Manager. However, you can combine actions and define tag conditions in many different ways to support your specific use cases. For more information, see Using identity-based policies (IAM policies) for Secrets Manager.

In the "Condition" element of the policy, you can choose tag keys from among the following:

- **aws:TagKeys**
- **aws:ResourceTag/${TagKey}**

To learn more about resource tags and how to use aws:TagKeys, see Controlling access to AWS resources using resource tags.

**Note**
Both the Data API and AWS Secrets Manager authorize users. If you don’t have permissions for all actions defined in a policy, you get an AccessDeniedException error.

### Storing database credentials in AWS Secrets Manager

When you call the Data API, you can pass credentials for the Aurora Serverless DB cluster by using a secret in Secrets Manager. To pass credentials in this way, you specify the name of the secret or the Amazon Resource Name (ARN) of the secret.

**To store DB cluster credentials in a secret**

1. **Use Secrets Manager to create a secret that contains credentials for the Aurora DB cluster.**

   For instructions, see Creating a Basic Secret in the AWS Secrets Manager User Guide.

2. **Use the Secrets Manager console to view the details for the secret you created, or run the aws secretsmanager describe-secret AWS CLI command.**

   Note the name and ARN of the secret. You can use them in calls to the Data API.
For more information about using Secrets Manager, see the AWS Secrets Manager User Guide.

To understand how Amazon Aurora manages identity and access management, see How Amazon Aurora works with IAM.

For more information about creating an IAM policy, see Creating IAM Policies in the IAM User Guide. For information about adding an IAM policy to a user, see Adding and Removing IAM Identity Permissions in the IAM User Guide.

Enabling the Data API

To use the Data API, enable it for your Aurora Serverless DB cluster. You can enable the Data API when you create or modify the DB cluster.

Console

You can enable the Data API by using the RDS console when you create or modify an Aurora Serverless DB cluster. When you create an Aurora Serverless DB cluster, you do so by enabling the Data API in the RDS console's Connectivity section. When you modify an Aurora Serverless DB cluster, you do so by enabling the Data API in the RDS console's Network & Security section.

The following screenshot shows the enabled Data API when modifying an Aurora Serverless DB cluster.

For instructions, see Creating an Aurora Serverless v1 DB cluster (p. 145) and Modifying an Aurora Serverless v1 DB cluster (p. 154).

AWS CLI

When you create or modify an Aurora Serverless DB cluster using AWS CLI commands, the Data API is enabled when you specify -enable-http-endpoint.

You can specify the -enable-http-endpoint using the following AWS CLI commands:

- create-db-cluster
- modify-db-cluster

The following example modifies sample-cluster to enable the Data API.

For Linux, macOS, or Unix:
aws rds modify-db-cluster \
   --db-cluster-identifier sample-cluster \
   --enable-http-endpoint

For Windows:

aws rds modify-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --enable-http-endpoint

RDS API

When you create or modify an Aurora Serverless DB cluster using Amazon RDS API operations, you enable the Data API by setting the `EnableHttpEndpoint` value to `true`.

You can set the `EnableHttpEndpoint` value using the following API operations:

- `CreateDBCluster`
- `ModifyDBCluster`

Creating an Amazon VPC endpoint for the Data API (AWS PrivateLink)

Amazon VPC enables you to launch AWS resources, such as Aurora DB clusters and applications, into a virtual private cloud (VPC). AWS PrivateLink provides private connectivity between VPCs and AWS services with high security on the Amazon network. Using AWS PrivateLink, you can create Amazon VPC endpoints, which enable you to connect to services across different accounts and VPCs based on Amazon VPC. For more information about AWS PrivateLink, see VPC Endpoint Services (AWS PrivateLink) in the Amazon Virtual Private Cloud User Guide.

You can call the Data API with Amazon VPC endpoints. Using an Amazon VPC endpoint keeps traffic between applications in your Amazon VPC and the Data API in the AWS network, without using public IP addresses. Amazon VPC endpoints can help you meet compliance and regulatory requirements related to limiting public internet connectivity. For example, if you use an Amazon VPC endpoint, you can keep traffic between an application running on an Amazon EC2 instance and the Data API in the VPCs that contain them.

After you create the Amazon VPC endpoint, you can start using it without making any code or configuration changes in your application.

To create an Amazon VPC endpoint for the Data API

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose Endpoints, and then choose Create Endpoint.
3. On the Create Endpoint page, for Service category, choose AWS services. For Service Name, choose rds-data.
4. For **VPC**, choose the VPC to create the endpoint in.

Choose the VPC that contains the application that makes Data API calls.

5. For **Subnets**, choose the subnet for each Availability Zone (AZ) used by the AWS service that is running your application.

To create an Amazon VPC endpoint, specify the private IP address range in which the endpoint will be accessible. To do this, choose the subnet for each Availability Zone. Doing so restricts the VPC endpoint to the private IP address range specific to each Availability Zone and also creates an Amazon VPC endpoint in each Availability Zone.

6. For **Enable DNS name**, select **Enable for this endpoint**.

Private DNS resolves the standard Data API DNS hostname (`https://rds-data.region.amazonaws.com`) to the private IP addresses associated with the DNS hostname specific to your Amazon VPC endpoint. As a result, you can access the Data API VPC endpoint using the AWS CLI or AWS SDKs without making any code or configuration changes to update the Data API endpoint URL.

7. For **Security group**, choose a security group to associate with the Amazon VPC endpoint.
Choose the security group that allows access to the AWS service that is running your application. For example, if an Amazon EC2 instance is running your application, choose the security group that allows access to the Amazon EC2 instance. The security group enables you to control the traffic to the Amazon VPC endpoint from resources in your VPC.

8. For **Policy**, choose **Full Access** to allow anyone inside the Amazon VPC to access the Data API through this endpoint. Or choose **Custom** to specify a policy that limits access.

   If you choose **Custom**, enter the policy in the policy creation tool.

9. Choose **Create endpoint**.

After the endpoint is created, choose the link in the AWS Management Console to view the endpoint details.

The endpoint **Details** tab shows the DNS hostnames that were generated while creating the Amazon VPC endpoint.

You can use the standard endpoint (**rds-data.region.amazonaws.com**) or one of the VPC-specific endpoints to call the Data API within the Amazon VPC. The standard Data API endpoint automatically routes to the Amazon VPC endpoint. This routing occurs because the Private DNS hostname was enabled when the Amazon VPC endpoint was created.

When you use an Amazon VPC endpoint in a Data API call, all traffic between your application and the Data API remains in the Amazon VPCs that contain them. You can use an Amazon VPC endpoint for any type of Data API call. For information about calling the Data API, see **Calling the Data API** (p. 169).

**Calling the Data API**

After you enable the Data API for an Aurora Serverless DB cluster, you can call the Data API or the AWS CLI to run SQL statements on the DB cluster. The Data API supports the programming languages supported by the AWS SDK. For more information, see **Tools to build on AWS**.

**Note**

Currently, the Data API doesn't support arrays of Universal Unique Identifiers (UUIDs).
The Data API provides the following operations to perform SQL statements.

<table>
<thead>
<tr>
<th>Data API operation</th>
<th>AWS CLI command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExecuteStatement</td>
<td>aws rds-data execute-statement</td>
<td>Runs a SQL statement against a database.</td>
</tr>
<tr>
<td>BatchExecuteStatement</td>
<td>aws rds-data batch-execute-statement</td>
<td>Runs a batch SQL statement over an array of data for bulk update and insert operations. You can run a DML statement with array of parameter sets. A batch SQL statement can provide a significant performance improvement over individual insert and update statements.</td>
</tr>
</tbody>
</table>

You can run both operations for performing a SQL statement independently, or you can run them in a transaction. The Data API provides the following operations to support transactions.

<table>
<thead>
<tr>
<th>Data API operation</th>
<th>AWS CLI command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BeginTransaction</td>
<td>aws rds-data begin-transaction</td>
<td>Starts a SQL transaction.</td>
</tr>
<tr>
<td>CommitTransaction</td>
<td>aws rds-data commit-transaction</td>
<td>Ends a SQL transaction and commits the changes.</td>
</tr>
<tr>
<td>RollbackTransaction</td>
<td>aws rds-data rollback-transaction</td>
<td>Performs a rollback of a transaction.</td>
</tr>
</tbody>
</table>

The operations for performing SQL statements and supporting transactions have the following common Data API parameters and AWS CLI options. Some operations support other parameters or options.

<table>
<thead>
<tr>
<th>Data API operation parameter</th>
<th>AWS CLI command option</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>resourceArn</td>
<td>--resource-arn</td>
<td>Yes</td>
<td>The Amazon Resource Name (ARN) of the Aurora Serverless DB cluster.</td>
</tr>
<tr>
<td>secretArn</td>
<td>--secret-arn</td>
<td>Yes</td>
<td>The name or ARN of the secret that enables access to the DB cluster.</td>
</tr>
</tbody>
</table>

You can use parameters in Data API calls to ExecuteStatement and BatchExecuteStatement, and when you run the AWS CLI commands execute-statement and batch-execute-statement. To use a parameter, you specify a name-value pair in the SqlParameter data type. You specify the value with the Field data type. The following table maps Java Database Connectivity (JDBC) data types to the data types you specify in Data API calls.

<table>
<thead>
<tr>
<th>JDBC data type</th>
<th>Data API data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTEGER, TINYINT, SMALLINT, BIGINT</td>
<td>LONG</td>
</tr>
</tbody>
</table>
### JDBC data type | Data API data type
--- | ---
FLOAT, REAL, DOUBLE | DOUBLE
DECIMAL | STRING
BOOLEAN, BIT | BOOLEAN
BLOB, BINARY, LONGVARBINARY, VARBINARY | BLOB
CLOB | STRING
Other types (including types related to date and time) | STRING

For some specific types, such as DECIMAL or TIME, a hint might be required to instruct the Data API that the String value should be passed to the database as a different type. You can do this by including values in typeHint in the SqlParameter data type. The possible values for typeHint are the following:

- **DECIMAL** – The corresponding String parameter value is sent as an object of DECIMAL type to the database.
- **TIMESTAMP** – The corresponding String parameter value is sent as an object of TIMESTAMP type to the database. The accepted format is YYYY-MM-DD HH:MM:SS [.FFF].
- **TIME** – The corresponding String parameter value is sent as an object of TIME type to the database. The accepted format is HH:MM:SS [.FFF].
- **DATE** – The corresponding String parameter value is sent as an object of DATE type to the database. The accepted format is YYYY-MM-DD.

**Note**
For Amazon Aurora PostgreSQL, the Data API always returns the Aurora PostgreSQL datatype TIMESTAMPTZ in UTC timezone.

**Examples**
- Calling the Data API with the AWS CLI (p. 171)
- Calling the Data API from a Python application (p. 178)
- Calling the Data API from a Java application (p. 181)

**Note**
These examples are not exhaustive.

**Calling the Data API with the AWS CLI**

You can call the Data API using the AWS Command Line Interface (AWS CLI).

The following examples use the AWS CLI for the Data API. For more information, see AWS Command Line Interface reference for the Data API.

In each example, replace the DB cluster ARN with the ARN for your Aurora Serverless DB cluster. Also, replace the secret ARN with the ARN of the secret in Secrets Manager that allows access to the DB cluster.

**Note**
The AWS CLI can format responses in JSON.
- Starting a SQL transaction (p. 172)
- Running a SQL statement (p. 172)
- Running a batch SQL statement over an array of data (p. 176)
- Committing a SQL transaction (p. 177)
- Rolling back a SQL transaction (p. 178)

**Starting a SQL transaction**

You can start a SQL transaction using the `aws rds-data begin-transaction` CLI command. The call returns a transaction identifier.

**Important**

A transaction times out if there are no calls that use its transaction ID in three minutes. If a transaction times out before it's committed, it's rolled back automatically. DDL statements inside a transaction cause an implicit commit. We recommend that you run each DDL statement in a separate `execute-statement` command with the `--continue-after-timeout` option.

In addition to the common options, specify the following option:

- `--database` (optional) – The name of the database.

For example, the following CLI command starts a SQL transaction.

For Linux, macOS, or Unix:

```bash
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret"
```

For Windows:

```bash
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret"
```

The following is an example of the response.

```json
{
  "transactionId": "ABC1234567890xyz"
}
```

**Running a SQL statement**

You can run a SQL statement using the `aws rds-data execute-statement` CLI command.

You can run the SQL statement in a transaction by specifying the transaction identifier with the `--transaction-id` option. You can start a transaction using the `aws rds-data begin-transaction` CLI command. You can end and commit a transaction using the `aws rds-data commit-transaction` CLI command.
Important

If you don't specify the `--transaction-id` option, changes that result from the call are committed automatically.

In addition to the common options, specify the following options:

- `--sql` (required) – A SQL statement to run on the DB cluster.
- `--transaction-id` (optional) – The identifier of a transaction that was started using the `begin-transaction` CLI command. Specify the transaction ID of the transaction that you want to include in the SQL statement in.
- `--parameters` (optional) – The parameters for the SQL statement.
- `--include-result-metadata | --no-include-result-metadata` (optional) – A value that indicates whether to include metadata in the results. The default is `--no-include-result-metadata`.
- `--database` (optional) – The name of the database.
- `--continue-after-timeout | --no-continue-after-timeout` (optional) – A value that indicates whether to continue running the statement after the call times out. The default is `--no-continue-after-timeout`.

For data definition language (DDL) statements, we recommend continuing to run the statement after the call times out to avoid errors and the possibility of corrupted data structures.

The DB cluster returns a response for the call.

Note

The response size limit is 1 MB. If the call returns more than 1 MB of response data, the call is terminated.

The maximum number of requests per second is 1,000.

For example, the following CLI command runs a single SQL statement and omits the metadata in the results (the default).

For Linux, macOS, or Unix:

```
  --database "mydb" --secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" \
  --sql "select * from mytable"
```

For Windows:

```
  --database "mydb" --secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" ^
  --sql "select * from mytable"
```

The following is an example of the response.

```json
{
  "numberOfRecordsUpdated": 0,
}
```
"records": [
  [
    { "stringValue": "ValueOne" },
    { "stringValue": "ValueTwo" },
    { "stringValue": "ValueThree" }
  ],
  [
    { "stringValue": "ValueOne" },
    { "stringValue": "ValueTwo" },
    { "stringValue": "ValueThree" }
  ],
  [
    { "stringValue": "ValueOne" },
    { "stringValue": "ValueTwo" },
    { "stringValue": "ValueThree" }
  ]
]

The following CLI command runs a single SQL statement in a transaction by specifying the --transaction-id option.

For Linux, macOS, or Unix:

```
--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"
```

For Windows:

```
--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"
```

The following is an example of the response.

```
{
  "numberOfRecordsUpdated": 1
}
```

The following CLI command runs a single SQL statement with parameters.
For Linux, macOS, or Unix:

```bash
```

For Windows:

```bash
```

The following is an example of the response.

```json
{
  "numberOfRecordsUpdated": 1
}
```

The following CLI command runs a data definition language (DDL) SQL statement. The DDL statement renames column job to column role.

**Important**

For DDL statements, we recommend continuing to run the statement after the call times out. When a DDL statement terminates before it is finished running, it can result in errors and possibly corrupted data structures. To continue running a statement after a call times out, specify the --continue-after-timeout option.

For Linux, macOS, or Unix:

```bash
```

For Windows:

```bash
```

The following is an example of the response.
Note
The generatedFields data isn't supported by Aurora PostgreSQL. To get the values of generated fields, use the RETURNING clause. For more information, see Returning data from modified rows in the PostgreSQL documentation.

Running a batch SQL statement over an array of data

You can run a batch SQL statement over an array of data by using the aws rds-data batch-execute-statement CLI command. You can use this command to perform a bulk import or update operation.

You can run the SQL statement in a transaction by specifying the transaction identifier with the --transaction-id option. You can start a transaction by using the aws rds-data begin-transaction CLI command. You can end and commit a transaction by using the aws rds-data commit-transaction CLI command.

Important
If you don't specify the --transaction-id option, changes that result from the call are committed automatically.

In addition to the common options, specify the following options:

- --sql (required) – A SQL statement to run on the DB cluster.
- --transaction-id (optional) – The identifier of a transaction that was started using the begin-transaction CLI command. Specify the transaction ID of the transaction that you want to include the SQL statement in.
- --parameter-set (optional) – The parameter sets for the batch operation.
- --database (optional) – The name of the database.

The DB cluster returns a response to the call.

Note
The response size limit is 1 MB. If the call returns more than 1 MB of response data, the call is terminated.

The maximum number of requests per second is 1,000.

For example, the following CLI command runs a batch SQL statement over an array of data with a parameter set.

For Linux, macOS, or Unix:

```bash
--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\": {"longValue": 1}}], [{"name": "id", "value": {"longValue": 2}},{"name": "val", "value": 
{"longValue": 2}},{"name": "val", "value": 2}]], [{"name": "id", "value": {"longValue": 3}},{"name": "val", "value": 
{"longValue": 3}},{"name": "val", "value": 3}]]"
```
For Windows:

```bash
--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**

Don't include line breaks in the `--parameter-sets` option.

### Committing a SQL transaction

Using the `aws rds-data commit-transaction` CLI command, you can end a SQL transaction that you started with `aws rds-data begin-transaction` and commit the changes.

In addition to the common options, specify the following option:

- `--transaction-id` (required) – The identifier of a transaction that was started using the `begin-transaction` CLI command. Specify the transaction ID of the transaction that you want to end and commit.

For example, the following CLI command ends a SQL transaction and commits the changes.

For Linux, macOS, or Unix:

```bash
--secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" \ 
--transaction-id "ABC1234567890xyz"
```

For Windows:

```bash
--secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" ^ 
--transaction-id "ABC1234567890xyz"
```

The following is an example of the response.

```json
{
"transactionStatus": "Transaction Committed"
}
```
Rolling back a SQL transaction

Using the `aws rds-data rollback-transaction` CLI command, you can roll back a SQL transaction that you started with `aws rds-data begin-transaction`. Rolling back a transaction cancels its changes.

**Important**

If the transaction ID has expired, the transaction was rolled back automatically. In this case, an `aws rds-data rollback-transaction` command that specifies the expired transaction ID returns an error.

In addition to the common options, specify the following option:

- `--transaction-id` (required) – The identifier of a transaction that was started using the `begin-transaction` CLI command. Specify the transaction ID of the transaction that you want to roll back.

For example, the following AWS CLI command rolls back a SQL transaction.

For Linux, macOS, or Unix:

```
--secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" \ 
--transaction-id "ABC1234567890xyz"
```

For Windows:

```
--secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" \ 
--transaction-id "ABC1234567890xyz"
```

The following is an example of the response.

```
{
   "transactionStatus": "Rollback Complete"
}
```

Calling the Data API from a Python application

You can call the Data API from a Python application.

The following examples use the AWS SDK for Python (Boto). For more information about Boto, see the AWS SDK for Python (Boto 3) documentation.

In each example, replace the DB cluster's Amazon Resource Name (ARN) with the ARN for your Aurora Serverless DB cluster. Also, replace the secret ARN with the ARN of the secret in Secrets Manager that allows access to the DB cluster.

**Topics**

- Running a SQL query (p. 179)
- Running a DML SQL statement (p. 180)
Running a SQL query

You can run a SELECT statement and fetch the results with a Python application.

The following example runs a SQL query.

```python
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'])
[
    [
        {'stringValue': 'ROSALEZ'},
        {'stringValue': 'ALEJANDRO'},
        {'stringValue': '2016-02-15 04:34:33.0'}
    ],
    [
        {'stringValue': 'DOE'},
        {'stringValue': 'JANE'},
        {'stringValue': '2014-05-09 04:34:33.0'}
    ],
    [
        {'stringValue': 'STILES'},
        {'stringValue': 'JOHN'},
        {'stringValue': '2017-09-20 04:34:33.0'}
    ]
]```
Running a DML SQL statement

You can run a data manipulation language (DML) statement to insert, update, or delete data in your database. You can also use parameters in DML statements.

**Important**

If a call isn't part of a transaction because it doesn't include the `transactionID` parameter, changes that result from the call are committed automatically.

The following example runs an insert SQL statement and uses parameters.

```python
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'])
```

Running a SQL transaction

You can start a SQL transaction, run one or more SQL statements, and then commit the changes with a Python application.

**Important**

A transaction times out if there are no calls that use its transaction ID in three minutes. If a transaction times out before it's committed, it's rolled back automatically. If you don't specify a transaction ID, changes that result from the call are committed automatically.

The following example runs a SQL transaction that inserts a row in a table.

```python
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**

If you run a data definition language (DDL) statement, we recommend continuing to run the statement after the call times out. When a DDL statement terminates before it is finished running, it can result in errors and possibly corrupted data structures. To continue running a statement after a call times out, set the `continueAfterTimeout` parameter to `true`.

### Calling the Data API from a Java application

You can call the Data API from a Java application.

The following examples use the AWS SDK for Java. For more information, see the [AWS SDK for Java Developer Guide](https://docs.aws.amazon.com/aws-java-sdk/latest/developer-guide/index.html).

In each example, replace the DB cluster's Amazon Resource Name (ARN) with the ARN for your Aurora Serverless DB cluster. Also, replace the secret ARN with the ARN of the secret in Secrets Manager that allows access to the DB cluster.

**Topics**

- Running a SQL query (p. 181)
- Running a SQL transaction (p. 182)
- Running a batch SQL operation (p. 183)

### Running a SQL query

You can run a SELECT statement and fetch the results with a Java application.

The following example runs a SQL query.

```java
package com.amazonaws.rdsdata.examples;

import com.amazonaws.services.rdsdata.AWSSRDSData;
import com.amazonaws.services.rdsdata.AWSSRDSDataClient;
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 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));
        }
    }
}

Running a SQL transaction

You can start a SQL transaction, run one or more SQL statements, and then commit the changes with a Java application.

**Important**
A transaction times out if there are no calls that use its transaction ID in three minutes. If a transaction times out before it's committed, it's rolled back automatically.
If you don't specify a transaction ID, changes that result from the call are committed automatically.

The following example runs a SQL transaction.

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 void main(String[] args) {
        AWSRDSData rdsData = AWSRDSDataClient.builder().build();

        BeginTransactionRequest beginTransactionRequest = new BeginTransactionRequest()
            .withResourceArn(RESOURCE_ARN)
            .withSecretArn(SECRET_ARN)
            .withDatabase("mydb");

        // Execute statements and commit the transaction
    }
}
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
If you run a data definition language (DDL) statement, we recommend continuing to run the
statement after the call times out. When a DDL statement terminates before it is finished
running, it can result in errors and possibly corrupted data structures. To continue running a
statement after a call times out, set the continueAfterTimeout parameter to true.

Running a batch SQL operation
You can run bulk insert and update operations over an array of data with a Java application. You can run
a DML statement with array of parameter sets.

Important
If you don't specify a transaction ID, changes that result from the call are committed
automatically.

The following example runs a batch insert operation.

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.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 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);

Using the Java client library for Data API

You can download and use a Java client library for the Data API. This Java client library provides an alternative way to use the Data API. Using this library, you can map your client-side classes to requests and responses of the Data API. This mapping support can ease integration with some specific Java types, such as Date, Time, and BigDecimal.

Downloading the Java client library for Data API

The Data API Java client library is open source in GitHub at the following location:

You can build the library manually from the source files, but the best practice is to consume the library using Apache Maven dependency management. Add the following dependency to your Maven POM file:

```xml
<dependency>
    <groupId>software.amazon.rdsdata</groupId>
    <artifactId>rds-data-api-client-library-java</artifactId>
    <version>1.0.4</version>
</dependency>
```

Java client library examples

Following, you can find some common examples of using the Data API Java client library. These examples assume that you have a table accounts with two columns: accountId and name. You also have the following data transfer object (DTO).

```java
public class Account {
    int accountId;
    String name;
    // getters and setters omitted
}
```

The client library enables you to pass DTOs as input parameters. The following example shows how customer DTOs are mapped to input parameters sets.
var account1 = new Account(1, "John");
var account2 = new Account(2, "Mary");
client.forSql("INSERT INTO accounts(accountId, name) VALUES(:accountId, :name)"
  .withParams(account1, account2)
  .execute();

In some cases, it's easier to work with simple values as input parameters. You can do so with the following syntax.

client.forSql("INSERT INTO accounts(accountId, name) VALUES(:accountId, :name)"
  .withParam("accountId", 3)
  .withParam("name", "Zhang")
  .execute();

The following is another example that works with simple values as input parameters.

client.forSql("INSERT INTO accounts(accountId, name) VALUES(?, ?)", 4, "Carlos")
  .execute();

The client library provides automatic mapping to DTOs when a result is returned. The following examples show how the result is mapped to your DTOs.

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);

**Troubleshooting Data API issues**

Use the following sections, titled with common error messages, to help troubleshoot problems that you have with the Data API.

**Topics**
- Transaction <transaction_ID> is not found (p. 185)
- Packet for query is too large (p. 186)
- Database response exceeded size limit (p. 186)
- HttpEndpoint is not enabled for cluster <cluster_ID> (p. 186)

**Transaction <transaction_ID> is not found**

In this case, the transaction ID specified in a Data API call wasn't found. The cause for this issue is almost always one of the following:

- The specified transaction ID wasn't created by a BeginTransaction call.
- The specified transaction ID has expired.

A transaction expires if no call uses the transaction ID within three minutes.
To solve the issue, make sure that your call has a valid transaction ID. Also make sure that each transaction call runs within three minutes of the last one.

For information about running transactions, see Calling the Data API (p. 169).

**Packet for query is too large**

In this case, the result set returned for a row was too large. The Data API size limit is 64 KB per row in the result set returned by the database.

To solve this issue, make sure that each row in a result set is 64 KB or less.

**Database response exceeded size limit**

In this case, the size of the result set returned by the database was too large. The Data API limit is 1 MB in the result set returned by the database.

To solve this issue, make sure that calls to the Data API return 1 MB of data or less. If you need to return more than 1 MB, you can use multiple `ExecuteStatement` calls with the `LIMIT` clause in your query.

For more information about the `LIMIT` clause, see SELECT syntax in the MySQL documentation.

**HttpEndpoint is not enabled for cluster `<cluster_ID>`**

The cause for this issue is almost always one of the following:

- The Data API isn't enabled for the Aurora Serverless DB cluster. To use the Data API with an Aurora Serverless DB cluster, the Data API must be enabled for the DB cluster.
- The DB cluster was renamed after the Data API was enabled for it.

If the Data API has not been enabled for the DB cluster, enable it.

If the DB cluster was renamed after the Data API was enabled for the DB cluster, disable the Data API and then enable it again.

For information about enabling the Data API, see Enabling the Data API (p. 166).

**Logging Data API calls with AWS CloudTrail**

Data API is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Data API. CloudTrail captures all API calls for Data API as events, including calls from the Amazon RDS console and from code calls to the Data API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Data API. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the data collected by CloudTrail, you can determine a lot of information. This information includes the request that was made to Data API, the IP address the request was made from, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

**Working with Data API information in CloudTrail**

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Data API, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail event history in the AWS CloudTrail User Guide.

For an ongoing record of events in your AWS account, including events for Data API, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all AWS Regions in the
AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following topics in the AWS CloudTrail User Guide:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions and Receiving CloudTrail log files from multiple accounts

All Data API operations are logged by CloudTrail and documented in the Amazon RDS data service API reference. For example, calls to the BatchExecuteStatement, BeginTransaction, CommitTransaction, and ExecuteStatement operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding Data API log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the ExecuteStatement operation.

```json
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AKIAIOSFODNN7EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/johndoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHEXAMPLE",
    "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": [],
    "schema": "**********",
```
Using the query editor for Aurora Serverless

With the query editor for Aurora Serverless, you can run SQL queries in the RDS console. You can run any valid SQL statement on the Aurora Serverless DB cluster, including data manipulation and data definition statements.

The query editor requires an Aurora Serverless DB cluster with the Data API enabled. For information about creating an Aurora Serverless DB cluster with the Data API enabled, see Using the Data API for Aurora Serverless (p. 162).

Availability of the query editor

The query editor is only available for the following Aurora Serverless DB clusters:

- Aurora with MySQL version 5.6 compatibility
- Aurora with MySQL version 5.7 compatibility
- Aurora with PostgreSQL version 10.7 compatibility

The query editor is currently available for Aurora Serverless in the following AWS Regions:

- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Asia Pacific (Mumbai)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

Authorizing access to the query editor

A user must be authorized to run queries in the query editor. You can authorize a user to run queries in the query editor by adding the AmazonRDSDataFullAccess policy, a predefined AWS Identity and Access Management (IAM) policy, to that user.

You can also create an IAM policy that grants access to the query editor. After you create the policy, add it to each user that requires access to the query editor.

The following policy provides the minimum required permissions for a user to access the query editor.
For information about creating an IAM policy, see Creating IAM policies in the AWS Identity and Access Management User Guide.

For information about adding an IAM policy to a user, see Adding and removing IAM identity permissions in the AWS Identity and Access Management User Guide.

Running queries in the query editor

You can run SQL statements on an Aurora Serverless DB cluster in the query editor.

To run a query in the query editor

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region in which you created the Aurora Serverless DB clusters that you want to query.
3. In the navigation pane, choose **Databases**.
4. Choose the Aurora Serverless DB cluster that you want to run SQL queries against.
5. For **Actions**, choose **Query**. If you haven't connected to the database before, the **Connect to database** page opens.

6. Enter the following information:
   a. For **Database instance or cluster**, choose the Aurora Serverless DB cluster that you want to run SQL queries on.
   b. For **Database username**, choose the user name of the database user to connect with, or choose **Add new database credentials**. If you choose **Add new database credentials**, enter the user name for the new database credentials in **Enter database username**.
   c. For **Enter database password**, enter the password for the database user that you chose.
   d. In the last box, enter the name of the database or schema that you want to use for the Aurora DB cluster.
   e. Choose **Connect to database**.

   **Note**
   If your connection is successful, your connection and authentication information are stored in AWS Secrets Manager. You don't need to enter the connection information again.
7. In the query editor, enter the SQL query that you want to run on the database.

Each SQL statement can commit automatically, or you can run SQL statements in a script as part of a transaction. To control this behavior, choose the gear icon above the query window.

The **Query Editor Settings** window appears.
If you choose **Auto-commit**, every SQL statement commits automatically. If you choose **Transaction**, you can run a group of statements in a script. Statements are automatically committed at the end of the script unless explicitly committed or rolled back before then. Also, you can choose to stop a running script if an error occurs by enabling **Stop on error**.

**Note**
In a group of statements, data definition language (DDL) statements can cause previous data manipulation language (DML) statements to commit. You can also include **COMMIT** and **ROLLBACK** statements in a group of statements in a script.

After you make your choices in the **Query Editor Settings** window, choose **Save**.

8. Choose **Run** or press Ctrl+Enter, and the query editor displays the results of your query.

After running the query, save it to **Saved queries** by choosing **Save**.

Export the query results to spreadsheet format by choosing **Export to csv**.

You can find, edit, and rerun previous queries. To do so, choose the **Recent** tab or the **Saved queries** tab, choose the query text, and then choose **Run**.

To change the database, choose **Change database**.
Using Amazon Aurora Serverless v2 (preview)

Amazon Aurora Serverless v2 with MySQL compatibility is in preview release and is subject to change. Aurora Serverless v2 (preview) is not covered by the Amazon RDS service level agreement (SLA). Don’t use Aurora Serverless v2 (preview) for production databases. All resources and data will be deleted when the preview ends.

Continuously monitoring and adjusting capacity for multiple databases so you stay within budget can be a daunting task. You don't want to pay for more computing resources than you use. But you also can't afford to spend a lot of time reallocating resources to achieve a better price-performance ratio. For unpredictable workloads, multi-tenant, and distributed database environments that can have wide variances in consumption, this task is especially challenging.

By using Amazon Aurora Serverless v2 (Amazon Aurora Serverless version 2), now in preview, you can get optimal cost performance for your database clusters. Capacity is adjusted automatically based on application demand, and you're charged only for the resources that your DB clusters consume.

Topics

• How Aurora Serverless v2 (preview) works (p. 193)
• Limitations of Aurora Serverless v2 (preview) (p. 196)
• Creating an Aurora Serverless v2 (preview) DB cluster (p. 197)
• Creating a snapshot of an Aurora Serverless v2 (preview) DB cluster (p. 200)
• Modifying an Aurora Serverless v2 (preview) DB cluster (p. 201)
• Deleting an Aurora Serverless v2 (preview) DB cluster (p. 203)
• Restoring an Aurora Serverless v2 (preview) DB cluster to a point in time (p. 204)

How Aurora Serverless v2 (preview) works

Amazon Aurora Serverless v2 has been architected from the ground up to support serverless DB clusters that are instantly scalable. The Aurora Serverless v2 (preview) architecture rests on a lightweight foundation that's been engineered to provide the security and isolation needed in multi-tenant serverless cloud environments. This foundation has very little overhead so it can respond quickly. It's also powerful enough to meet dramatic increases in processing demand.

Instant autoscaling

When you create your Aurora Serverless v2 (preview) DB cluster, you define its capacity as a range between minimum and maximum number of Aurora capacity units (ACUs):

• Minimum Aurora capacity units – The smallest number of ACUs down to which your Aurora Serverless v2 (preview) DB cluster can scale.
• Maximum Aurora capacity units – The largest number of ACUs up to which your Aurora Serverless v2 (preview) DB cluster can scale.
Each ACU provides 2 GiB (gibibytes) of memory (RAM) and associated virtual processor (vCPU) with networking.

Unlike Aurora Serverless v1, which scales by doubling ACUs each time the DB cluster reaches a threshold, Aurora Serverless v2 (preview) can increase ACUs incrementally. When your workload demand begins to reach the current resource capacity, your Aurora Serverless v2 (preview) DB cluster scales the number of ACUs. Your cluster scales ACUs in the increments required to provide the best performance for the resources consumed.

The following screenshot shows instant autoscaling in action. It's an extract from Amazon CloudWatch comparing processing load to the number of ACUs consumed by an Aurora Serverless v2 (preview) DB cluster over time for a simulated “flash sale” scenario. The simulation models an order system that processes about 10 orders per second (using 4 ACUs) during regular operations. A load testing tool generates various increases in orders mimicking a “flash sale,” until the system is processing 275 orders per second (and 22 ACUs) at its peak.

In the screenshot, these numbers indicate this information:

1. Orders processed each second – Processing load as customers respond to a “flash sale” for a product. The line shows the number of orders being processed each second. Order processing involves multiple database actions. These include checking inventory, processing the new order, creating a shipment order, adjusting the inventory amount, and initiating shipping by notifying the warehouse system.
2. Aurora capacity units (ACUs) – Memory and CPU applied over time to increasing and decreasing demand. The line shows the surge of ACUs applied to the workload (line 1) when orders reach their highest point, about 275 per second.

An ACU is made up of both memory (RAM) and processor (CPU). Increases in CPU utilization respond immediately to workload demands. When the demand starts to decline from its peak, the scale down from the maximum ACU occurs more slowly, as memory is more gradually released (than CPU). This is a deliberate architectural choice. Aurora Serverless v2 (preview) releases memory more gradually as demand lessens to avoid affecting the workload.

Logging with Amazon CloudWatch

As with all Aurora DB clusters, error logs for Aurora Serverless v2 (preview) are enabled by default. However, unlike with provisioned Aurora DB clusters, you can’t view the logs for Aurora Serverless v2 (preview) in the Amazon RDS console. Aurora Serverless v2 (preview) automatically uploads the error logs to Amazon CloudWatch.

Aurora Serverless v2 (preview) also uploads your Aurora MySQL log data to CloudWatch for the types of logs that you specify. You choose the logs for uploading by changing values for several log-related DB cluster parameters for your Aurora Serverless v2 (preview) DB cluster. As with any type of Aurora DB cluster, you can’t modify the default DB cluster parameter group. Instead, create your own DB cluster parameter group based on a default parameter for your DB cluster and engine type. For Aurora Serverless v2 (preview) and Aurora Serverless v1, you use a DB cluster parameter group only.
We recommend that you create your custom DB cluster parameter group before creating your Aurora Serverless v2 (preview) DB cluster, so that it's available to choose when you create a database on the console.

You can also modify your Aurora Serverless v2 (preview) DB cluster later to use your custom DB cluster parameter group. For more information, see Modifying your DB cluster to use a custom DB cluster parameter group (p. 202).

For Aurora MySQL logging, you can activate the following parameters:
- `general_log` – Set to 1 to turn on the general log (default is off, or 0).
- `slow_query_log` – Set to 1 to turn on the slow query log. (default is off, or 0).
- `server_audit_logging` – Set to 1 to turn on server audit logging. If you turn this on, you can specify the audit events to send to CloudWatch by listing them in the `server_audit_events` parameter.
- `server_audit_events` – The list of events to capture in the logs.

For more information, see Using advanced auditing with an Amazon Aurora MySQL DB cluster (p. 727).

After you apply your modified DB cluster parameter group to your Aurora Serverless v2 (preview) DB cluster, you can view the logs in CloudWatch.

To view logs for your Aurora Serverless v2 (preview) DB cluster

2. Choose US East (N. Virginia) for the Region.
3. Choose Log groups.
4. Choose your Aurora Serverless v2 (preview) DB cluster log from the list. For error logs, the naming pattern is as follows.

/aws/rds/cluster/cluster-name/error

For more information on viewing details on your logs, see Monitoring log events in Amazon CloudWatch (p. 827).

Monitoring capacity with Amazon CloudWatch

Aurora Serverless v2 (preview) introduces a new metric for monitoring Aurora DB cluster capacity, `ServerlessDatabaseCapacity`. You can use CloudWatch to view your DB cluster’s capacity as it scales up and down. You can also compare `ServerlessDatabaseCapacity` to other metrics to see how changes in workloads affect resource consumption.

To monitor your Aurora Serverless v2 (preview) DB cluster’s capacity

2. Choose the US East (N. Virginia) Region.
3. Choose Metrics. All available metrics appear as cards in the console, grouped by service name.
4. Choose RDS.

You can also use the Search box to find `ServerlessDatabaseCapacity`.

We recommend that you set up a CloudWatch dashboard to monitor your Aurora Serverless v2 (preview) DB cluster capacity using this new metric. To learn how, see Building dashboards with CloudWatch. You
can compare ServerlessDatabaseCapacity to DatabaseUsedMemory, DatabaseConnections, and DMLThroughput to assess how your DB cluster is responding during operations.

To learn more about using Amazon CloudWatch with Amazon Aurora, see Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs (p. 824).

Limitations of Aurora Serverless v2 (preview)

Amazon Aurora Serverless v2 with MySQL compatibility is in preview release and is subject to change. Aurora Serverless v2 (preview) is not covered by the Amazon RDS service level agreement (SLA). Don’t use Aurora Serverless v2 (preview) for production databases. All resources and data will be deleted when the preview ends.

The following limitations apply to Amazon Aurora Serverless v2 (preview):

- You can work with Amazon Aurora Serverless v2 (preview) in the preview environment only. You are limited to working with Aurora Serverless v2 (preview) in this environment. To use any of your other existing AWS services, such as Amazon EC2 and Amazon CloudWatch, access them through the AWS Management Console in the US East (N. Virginia) Region.
- You can work with Amazon Aurora Serverless v2 (preview) using the console only. AWS CLI commands and Amazon RDS API operations for creating and working Aurora Serverless v2 (preview) DB clusters aren’t currently available.
- You can create only Aurora MySQL 5.7 (2.07) DB clusters using Aurora Serverless v2 (preview). Aurora PostgreSQL isn’t currently available for Aurora Serverless v2 (preview).
- Your Aurora Serverless v2 (preview) DB clusters have a default capacity that ranges from a minimum of 4 Aurora capacity units (ACUs) to 32 ACUs. Each ACU provides the equivalent of approximately 2 gibibytes (GiB) of RAM and associated CPU and networking.
- You can’t give an Aurora Serverless v2 (preview) DB cluster a public IP address.
- You must create your Aurora Serverless v2 (preview) DB cluster in a virtual private cloud (VPC) based on the Amazon VPC service. You can access your Aurora Serverless v2 (preview) DB cluster only from within a VPC based on Amazon VPC.
- Aurora Serverless v2 (preview) databases are accessible only through port 3306. Aurora Serverless v2 (preview) assigns port 3306 to any Aurora MySQL DB instances that you create. You can’t change the port number.
- Aurora Serverless v2 (preview) doesn’t support the following Aurora features:
  - Amazon RDS Performance Insights
  - Amazon RDS Proxy
  - Aurora backtracking
  - Aurora cloning
  - Aurora global databases
  - Aurora multi-master
  - Aurora Replicas
  - AWS Identity and Access Management (IAM) database authentication
  - Data API for Aurora Serverless v1
  - Exporting snapshots created from Aurora Serverless v2 (preview) DB clusters to Amazon S3 buckets
  - Importing data from Amazon S3 into Aurora Serverless v2 (preview) DB cluster tables
  - Invoking AWS Lambda functions from within your Aurora Serverless v2 (preview) database
  - Query editor for Aurora Serverless v1
  - Restoring snapshots from Aurora provisioned DB clusters
Creating an Aurora Serverless v2 (preview) DB cluster

Amazon Aurora Serverless v2 with MySQL compatibility is in preview release and is subject to change. Aurora Serverless v2 (preview) is not covered by the Amazon RDS service level agreement (SLA). Don't use Aurora Serverless v2 (preview) for production databases. All resources and data will be deleted when the preview ends.

To work with Amazon Aurora Serverless v2 (preview), you must apply for access. For more information, see the Aurora Serverless v2 (preview) page.

After you've been approved for access, you can sign in to the preview using the console. Currently, you can create an Amazon Aurora Serverless v2 (preview) DB cluster with the console only.

To create an Aurora Serverless v2 (preview) DB cluster

1. Sign in to the preview using the AWS Management Console and open the Amazon RDS console.
2. Choose Create Database. For this preview, you see the available choices preselected for Engine options:
   - Amazon Aurora for Engine type
   - Amazon Aurora with MySQL compatibility for Edition
   - Aurora Serverless v2 (preview) for Capacity configuration
   - Aurora (MySQL 5.7) 2.07.1 for Version

3. For Settings, do the following:
   a. Accept the default DB cluster identifier or choose your own.
   b. Enter your own password for the default admin account for the DB cluster, or have Aurora Serverless v2 (preview) generate one for you. If you choose Auto generate a password, you get an option to copy the password.
4. For **Capacity settings**, you can accept the default range (4 ACUs minimum to 32 ACUs maximum). Or you can choose other values for minimum and maximum capacity units.

   For more information about Aurora Serverless v2 (preview) capacity units, see Instant autoscaling (p. 193).

5. For **Connectivity**, choose the virtual private cloud (VPC) based on Amazon VPC that defines the virtual networking environment for this DB instance. You can choose the defaults to simplify this task.

   To use your own VPC, we recommend that you create it along with related subnets, subnet group, and security group in advance. If you do this, these are available for you to choose when you're creating your Aurora Serverless v2 (preview) DB cluster.

   To learn how, see How to create a VPC for use with Amazon Aurora.
6. For **Additional configuration**, enter a name for **Initial database name** to create a database for your Aurora Serverless v2 (preview) cluster.

   If you created a custom DB cluster parameter group, choose it for **DB cluster parameter group**. If you want to view your Aurora MySQL logs in Amazon CloudWatch, make sure to use a custom DB cluster parameter group. For more information, see Logging with Amazon CloudWatch (p. 194).

   ![Additional configuration](image)

   The Aurora Serverless v2 (preview) cluster volume is always encrypted. You can't disable encryption, but you can choose your own encryption key. For more information, see Encrypting Amazon Aurora resources.

7. Acknowledge the limited service agreement.

   ![Aurora Serverless v2 is now available to preview](image)

   You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

8. Choose **Create database** to create your Aurora Serverless v2 (preview) DB cluster.

   You can connect to your Aurora Serverless v2 (preview) DB cluster by using its endpoint. The endpoint is listed on the **Connectivity & security** tab of the console, under **Endpoint & Port**. For more information about how to connect to Aurora DB clusters, see Connecting to an Amazon Aurora DB cluster (p. 253).

   Aurora Serverless v2 (preview) creates your DB instance using port 3306. Make sure to configure the security group for your Aurora Serverless v2 (preview) DB cluster to allow access to the MySQL/Aurora port (3306).

   However, you can't access the Amazon VPC configurations directly from the preview console.

   **To modify your security group settings**

   2. Choose the US East (N. Virginia) Region.
3. For **Security Group**, choose the security group associated with your Aurora Serverless v2 (preview) DB cluster.

4. Edit values for **Inbound rules** and **Outbound rules** as needed.

To learn more about configuring your VPC for Aurora, see Amazon Virtual Private Cloud VPCs and Amazon Aurora.

**Creating a snapshot of an Aurora Serverless v2 (preview) DB cluster**

Amazon Aurora Serverless v2 with MySQL compatibility is in preview release and is subject to change. Aurora Serverless v2 (preview) is not covered by the Amazon RDS service level agreement (SLA). Don't use Aurora Serverless v2 (preview) for production databases. All resources and data will be deleted when the preview ends.

Amazon Aurora Serverless v2 (preview) routinely creates snapshots of your DB cluster as backups. Unlike automated backups, manual snapshots aren't subject to the backup retention period. Snapshots don't expire. For more information about snapshots in general, see Creating a DB cluster snapshot (p. 418).

Currently, you can create an Aurora Serverless v2 (preview) DB cluster snapshot using the console only.

**To create a DB cluster snapshot**

1. Sign in to the preview using the AWS Management Console and open the Amazon RDS console.
2. In the navigation pane, choose **Databases**.
3. Choose the Aurora Serverless v2 (preview) DB cluster use for your snapshot.
4. Choose **Actions**, and then choose **Take snapshot**.

The **Take DB Snapshot** window appears.

5. For **Snapshot name**, enter the name of your Aurora Serverless v2 (preview) DB cluster.

6. Choose **Take Snapshot**.
Modifying an Aurora Serverless v2 (preview) DB cluster

Amazon Aurora Serverless v2 with MySQL compatibility is in preview release and is subject to change. Aurora Serverless v2 (preview) is not covered by the Amazon RDS service level agreement (SLA). Don’t use Aurora Serverless v2 (preview) for production databases. All resources and data will be deleted when the preview ends.

You can change configuration settings for your Aurora Serverless v2 (preview) DB cluster at any time, such as to do the following:

- Change your Aurora Serverless v2 (preview) DB cluster name.
- Enable (or disable) deletion protection for your Aurora Serverless v2 (preview) DB cluster.
- Modify your Aurora Serverless v2 (preview) DB cluster’s capacity settings.
- Modify Additional configuration settings, such as choosing a custom DB cluster parameter group.

The only configuration option you can't change for Aurora Serverless v2 (preview) DB cluster is its virtual private cloud (VPC) that you chose when you created it.

Use the following procedure to modify your Aurora Serverless v2 (preview) DB cluster's configuration by using the console.

To modify your Aurora Serverless v2 (preview) DB cluster’s configuration

1. Sign in to the preview using the AWS Management Console and open the Amazon RDS console.
2. In the navigation pane, choose DB clusters.
3. Choose your Aurora Serverless v2 (preview) DB cluster from the list.

The configuration settings for your Aurora Serverless v2 (preview) DB cluster appear, and you can change its name, password, credentials, and other settings.

Modifying Aurora Serverless v2 (preview) DB cluster capacity

Currently, you can modify the capacity of your Aurora Serverless v2 (preview) DB clusters with the console only.

To modify the capacity of your Aurora Serverless v2 (preview) DB cluster

1. Sign in to the preview using the AWS Management Console and open the Amazon RDS console.
2. In the navigation pane, choose DB Clusters.
3. Choose your Aurora Serverless v2 (preview) DB cluster from the list, and then choose **Modify** to open its configuration.

4. For **Capacity settings**, change the minimum number of ACUs or the maximum number of ACUs that you now want for your Aurora Serverless v2 (preview) DB cluster.

5. Choose **Continue**. The **Summary of modifications** appears.

6. Choose **Modify cluster** to accept the summary of modifications. You can also choose **Back** to modify your changes or **Cancel** to discard your changes.

To learn more about ACUs and scaling for Aurora Serverless v2 (preview), see **Instant autoscaling** (p. 193).

### Modifying your DB cluster to use a custom DB cluster parameter group

To use a custom DB cluster parameter group after your Aurora Serverless v2 (preview) is running, modify your existing Aurora Serverless v2 (preview) DB cluster.

Before you can use the following procedure, your custom DB cluster parameter group must exist. To learn how to create a custom DB cluster parameter group, see **Aurora Serverless v1 and parameter groups** (p. 142).

**To modify your Aurora Serverless v2 (preview) DB cluster to use a custom DB cluster parameter group**

1. Sign in to the preview using the AWS Management Console and open the Amazon RDS console.
2. In the navigation pane, choose **DB Clusters**.
3. Choose your Aurora Serverless v2 (preview) DB cluster from the list, and then choose **Modify**.
4. Under **Additional configuration**, choose your custom DB cluster parameter group.
Deleting an Aurora Serverless v2 (preview) DB cluster

Amazon Aurora Serverless v2 with MySQL compatibility is in preview release and is subject to change. Aurora Serverless v2 (preview) is not covered by the Amazon RDS service level agreement (SLA). Don’t use Aurora Serverless v2 (preview) for production databases. All resources and data will be deleted when the preview ends.

When you create your Aurora Serverless v2 (preview) DB clusters, you can choose to disable deletion protection or keep it as is. If the Aurora Serverless v2 (preview) DB cluster that you want to delete was created with deletion protection, make sure to modify your DB cluster to remove deletion protection or you can’t delete it. To learn how do this, see Modifying an Aurora Serverless v2 (preview) DB cluster (p. 201).

Currently, you can delete an Amazon Aurora Serverless v2 (preview) DB cluster with the console only.

To delete an Aurora Serverless v2 (preview) DB cluster

1. Sign in to the preview using the AWS Management Console and open the Amazon RDS console.
2. In the Resources section, choose DB Clusters.
3. Choose the Aurora Serverless v2 (preview) DB cluster that you want to delete.
4. For **Actions**, choose **Delete**. You're prompted to confirm that you want to delete your Aurora Serverless v2 (preview) DB cluster.

5. We recommend that you keep the preselected options:

   - **Yes** for **Create final snapshot**?
   - Your Aurora Serverless v2 (preview) DB cluster name plus `-final-snapshot` for **Final snapshot name**. However, you can change the name for your final snapshot in this field.

6. Choose **Delete DB cluster**.

   Aurora Serverless v2 (preview) deletes your DB cluster.

---

Restoring an Aurora Serverless v2 (preview) DB cluster to a point in time

Amazon Aurora Serverless v2 with MySQL compatibility is in preview release and is subject to change. Aurora Serverless v2 (preview) is not covered by the Amazon RDS service level agreement (SLA). Don't use Aurora Serverless v2 (preview) for production databases. All resources and data will be deleted when the preview ends.

You can create a new Aurora Serverless v2 (preview) DB cluster by restoring an existing DB cluster to a specific point in time. You can also use this approach to recover from a failure by recreating your Aurora Serverless v2 (preview) DB cluster from its most recent log files.

To restore your DB cluster to a specific point in time, Aurora creates a new DB cluster. It then applies all transactions from the logs of the existing DB cluster to the new cluster. Depending on the quantity and scope of transactions contained in the logs, this operation might take several hours to complete. For more information about point-in-time restore, see [Restoring a DB cluster to a specified time](#).

Currently, you can restore your Aurora Serverless v2 (preview) DB cluster using the console only.

**To restore an Aurora Serverless v2 (preview) DB cluster to a specified point in time**

1. Sign in to the preview using the AWS Management Console and open the Amazon RDS console.
2. Choose **Databases**.
3. Choose the Aurora Serverless v2 (preview) DB cluster that you want to restore.
4. For Actions, choose Restore to point in time. The Restore DB cluster page appears.

5. Choose Latest restorable time. Or choose Custom and specify a date and time that is earlier than the latest restorable time.
6. For Instance specifications, keep Aurora MySQL selected for the database engine.
7. For DB cluster identifier, enter the name for your newly restored DB cluster.
8. In the Capacity settings section, choose the minimum and maximum values that you want for your restored Aurora Serverless v2 (preview) DB cluster.

9. In the Connectivity section, accept the defaults.
10. For Additional configuration, choose the encryption key that you used for the DB cluster you're restoring. Choose the default key unless you used your own key when creating the DB cluster.
11. When you complete the settings on the page, choose Restore DB Cluster.
Using Amazon Aurora global databases

Amazon Aurora global databases span multiple AWS Regions, enabling low latency global reads and providing fast recovery from any outage that might affect any single AWS Region. An Aurora global database has a primary DB cluster in one Region, and secondary DB clusters in one or more different Regions.

Topics
- Overview of Amazon Aurora global databases (p. 206)
- Advantages of Amazon Aurora global databases (p. 207)
- Limitations of Amazon Aurora global databases (p. 207)
- Getting started with Amazon Aurora global databases (p. 208)
- Managing an Amazon Aurora global database (p. 227)
- Connecting to an Amazon Aurora global database (p. 232)
- Using write forwarding in an Amazon Aurora global database (p. 233)
- Disaster recovery for Amazon Aurora global databases (p. 244)
- Monitoring an Amazon Aurora global database (p. 248)
- Using Amazon Aurora global databases with other AWS services (p. 251)

Overview of Amazon Aurora global databases

By using an Amazon Aurora global database, you can have a single Aurora database that spans multiple AWS Regions to support your globally distributed applications.

An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only secondary AWS Regions. You issue write operations directly to the primary DB cluster in the primary AWS Region. Aurora replicates data to the secondary AWS Regions using dedicated infrastructure, with latency typically under a second.

You can also change the configuration of your Aurora global database while it’s running to support various use cases. For example, you might want the read/write capabilities to move from one Region to another, say, in different time zones, to ‘follow the sun.’ Or, you might need to respond to an outage in one Region. With Aurora global database, you can promote one of the secondary Regions to the primary role to take full read/write workloads in under a minute.

The following diagram shows an example Aurora global database that spans two AWS Regions.

You can scale up each secondary cluster independently, by adding one or more Aurora Replicas (read-only Aurora DB instances) to serve read-only workloads.
Only the primary cluster performs write operations. Clients that perform write operations connect to the DB cluster endpoint of the primary DB cluster.

Aurora global database is designed for applications with a worldwide footprint. The read-only secondary DB clusters (AWS Regions) allow you to support read operations closer to application users. With features such as write forwarding, you can also configure an Aurora MySQL–based global database so that secondary clusters send data to the primary. For more information, see Using write forwarding in an Amazon Aurora global database (p. 233).

Advantages of Amazon Aurora global databases

Aurora global databases can provide you with the following advantages:

• **Global reads with local latency** – Enterprises with offices around the world can use an Aurora global database to keep their main sources of information updated in the primary Region. Offices in other Regions can access the information in their own AWS Region, with local latency.

• **Scalable secondary Aurora DB clusters** – You can scale your secondary clusters by adding more read-only instances (Aurora Replicas) to a secondary AWS Region. The secondary cluster is read-only, so it can support up to 16 read-only Aurora Replica instances rather than the usual limit of 15 for a single Aurora cluster.

• **Fast replication from primary to secondary Aurora DB clusters** – The replication performed by an Aurora global database has little performance impact on the primary DB cluster. The resources of the DB instances are fully devoted to serve application read and write workloads.

• **Disaster recovery from Region–wide outages** – The secondary clusters enable fast failover for disaster recovery. You can promote a secondary cluster and make it available for writes in under a minute.

Limitations of Amazon Aurora global databases

The following limitations currently apply to Aurora global databases:

• Aurora global database is available in certain AWS Regions and for specific Aurora MySQL and Aurora PostgreSQL versions only. For more information, see Aurora global databases (p. 14).

• Aurora global databases currently don’t support the following Aurora features:
  • Aurora multi-master clusters
  • Aurora Serverless v1
  • Backtracking in Aurora

• You can start database activity streams on Aurora global databases running the following Aurora MySQL and Aurora PostgreSQL versions only:

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Primary AWS Region</th>
<th>Secondary AWS Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora MySQL</td>
<td>Aurora MySQL 5.7 (version 2.08 and later)</td>
<td>Aurora MySQL 5.7 (version 2.08 and later)</td>
</tr>
<tr>
<td>Aurora PostgreSQL</td>
<td>Aurora PostgreSQL 10.11 (and later)</td>
<td>Aurora PostgreSQL 10.14 (and later)</td>
</tr>
<tr>
<td></td>
<td>Aurora PostgreSQL 11.7 (and later)</td>
<td>Aurora PostgreSQL 11.9 (and later)</td>
</tr>
</tbody>
</table>

For information about database activity streams, see Using Database Activity Streams with Amazon Aurora (p. 565).
Getting started with Amazon Aurora global databases

To get started with Aurora global databases, you first decide which Aurora DB engine you want to use and in which AWS Regions. Only specific versions of the Aurora MySQL and Aurora PostgreSQL database engines in certain AWS Regions support Aurora global databases. For the complete list, see Aurora global databases (p. 14).

You can create an Aurora global database in one of the following ways:

- **Create a new Aurora global database with new Aurora DB clusters and Aurora DB instances.**

  You can do this by following the steps in Creating an Amazon Aurora global database (p. 209). After you create the primary Aurora DB cluster, you then add the secondary AWS Region by following the steps in Adding an AWS Region to an Amazon Aurora global database (p. 223).

- **Use an existing Aurora DB cluster that supports the Aurora global database feature and add an AWS Region to it.**

  You can do this only if your existing Aurora DB cluster uses a DB engine version that supports the Aurora 'global' mode or is global-compatible. For some DB engine versions, this mode is explicit, but for others, it's not. If you can choose Add region from the Action menu on the AWS Management Console when your Aurora DB cluster is selected, then you can use that Aurora DB cluster for your Aurora global cluster. For more information, see Adding an AWS Region to an Amazon Aurora global database (p. 223).

Before creating an Aurora global database, we recommend that you understand all configuration requirements.

Topics

- Configuration requirements of an Amazon Aurora global database (p. 209)
- Creating an Amazon Aurora global database (p. 209)
Configuration requirements of an Amazon Aurora global database

An Aurora global database spans at least two AWS Regions. The primary AWS Region supports an Aurora DB cluster that has one writer Aurora DB instance. A secondary AWS Region runs a read-only Aurora DB cluster made up entirely of Aurora Replicas. At least one secondary AWS Region is required, but an Aurora global database can have up to five secondary AWS Regions. The table lists the maximum Aurora DB clusters, Aurora DB instances, and Aurora Replicas allowed in an Aurora global database.

<table>
<thead>
<tr>
<th>Description</th>
<th>Primary AWS Region</th>
<th>Secondary AWS Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora DB clusters</td>
<td>1</td>
<td>1 (minimum; required); 5 (maximum)</td>
</tr>
<tr>
<td>Writer instances</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Read-only instances (Aurora replicas), per Aurora DB cluster</td>
<td>15 (max)</td>
<td>16 (total)</td>
</tr>
<tr>
<td>Read-only instances (max allowed, given actual number of secondary regions)</td>
<td>15 - s</td>
<td>s = total number of secondary AWS Regions</td>
</tr>
</tbody>
</table>

The Aurora DB clusters that make up an Aurora global database have the following specific requirements:

- **DB instance class requirements** – An Aurora global database requires DB instance classes that are optimized for memory-intensive applications. You can use `db.r4` or `db.r5` DB instance classes only. For more information, see DB instance classes.

- **AWS Region requirements** – An Aurora global database needs a primary Aurora DB cluster in one AWS Region, and at least one secondary Aurora DB cluster in a different Region. You can create up to five secondary (read-only) Aurora DB clusters, and each must be in a different Region. In other words, no two Aurora DB clusters in an Aurora global database can be in the same AWS Region.

- **Naming requirements** – The names you choose for each of your Aurora DB clusters must be unique, across all AWS Regions. You can’t use the same name for different Aurora DB clusters even though they’re in different Regions.

Before you can follow the procedures in this section, you need an AWS account. Complete the setup tasks for working with Amazon Aurora. For more information, see Setting up your environment for Amazon Aurora (p. 73). You also need to complete other preliminary steps for creating any Aurora DB cluster. To learn more, see Creating an Amazon Aurora DB cluster (p. 118).

Creating an Amazon Aurora global database

If you have an existing Aurora provisioned DB cluster running an Aurora database engine that’s global-compatible, you can add another AWS Region to it to create your Aurora global database. To do so, see Adding an AWS Region to an Amazon Aurora global database (p. 223).

You can create an Aurora global database using the AWS Management Console, the AWS CLI, or the RDS API by following the steps below.
Console

The steps for creating an Aurora global database begin by signing in to an AWS Region that supports the Aurora global database feature. For a complete list, see Aurora global databases (p. 14).

One of the steps below is choosing a virtual private cloud (VPC) based on Amazon VPC for your Aurora DB cluster. To use your own VPC, we recommend that you create it in advance, along with related subnets, subnet group, and security group, so it's available for you to choose. To learn how, see How to create a VPC for use with Amazon Aurora.

For general information about creating an Aurora DB cluster, see Creating an Amazon Aurora DB cluster (p. 118).

To create an Aurora global database

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Create database. On the Create database page:
   - Choose Standard create for the database creation method. (Don't choose Easy create.)
   - Choose Amazon Aurora for the Engine type in the Engine options section.

You then choose Amazon Aurora with MySQL compatibility or Amazon Aurora with PostgreSQL compatibility and continue creating the Aurora global database by using the steps from the following examples.

Topics
- Example for Aurora MySQL (p. 211)
- Example for Aurora PostgreSQL (p. 215)
Example for Aurora MySQL

The following steps apply to all versions of Aurora MySQL except for Aurora MySQL 5.6.10a. To use Aurora MySQL 5.6.10a for your Aurora global database, see Using Aurora MySQL 5.6.10a for an Aurora global database (p. 213).

To create an Aurora global database using Aurora MySQL

Complete the Create database page.

1. For Engine options:
   a. Choose Amazon Aurora with MySQL compatibility for the Edition option.
   b. Choose Provisioned for the Capacity type.
   c. Leave Replication features set to the default (single-master replication).
   d. Activate the Show versions that support the global database feature slider.
   e. For Version, choose the version of Aurora MySQL that you want to use for your Aurora global database.

2. For Templates, choose Production. Or, you can choose Dev/Test if appropriate for your use case. Don't use Dev/Test in production environments.

3. For Settings, do the following:
   a. Enter a meaningful name for the DB cluster identifier. When you finish creating the Aurora global database, this name identifies the primary DB cluster.
   b. Enter your own password for the admin user account for the DB instance, or let Aurora generate one for you. If you choose Auto generate a password, you get an option to copy the password.
4. For **DB instance size**, choose `db.r4`, `db.r5`, or another memory optimized DB instance size. If necessary, choose **Include previous generation classes** to select the DB instance class you want to use.

5. For **Availability & durability**, we recommend that you choose to have Aurora create an Aurora Replica in a different AZ for you. If you don't create an Aurora Replica now, you'll need to do it later.

6. For **Connectivity**, choose the virtual private cloud (VPC) based on Amazon VPC that defines the virtual networking environment for this DB instance. You can choose the defaults to simplify this task.

7. Complete the **Database authentication** settings for your use case. To simplify the process, you can choose **Password authentication** now and set up AWS Identity and Access Management later.

8. For **Additional configuration**, do the following:

   a. Enter a name for **Initial database name** to create the primary Aurora DB instance for this cluster. This is the writer node for the Aurora primary DB cluster.

      Leave the defaults selected for the DB cluster parameter group and DB parameter group, unless you have your own custom parameter groups that you want to use.

   b. You can accept all other default settings for **Additional configuration**, except for the following:

      - Uncheck the **Enable backtrack** option if it's selected. Aurora global databases don't support backtracking.

9. Choose **Create database**. It can take several minutes for Aurora to complete the process of creating the Aurora DB instance, its Aurora Replica, and the Aurora DB cluster. When the Aurora DB cluster is ready to use as the primary DB cluster in an Aurora global database, its status and that of the writer and Replica node display status of Available, as shown in the screenshot below.
When your primary DB cluster is available, create the Aurora global database by adding a secondary cluster to it, by following the steps in Adding an AWS Region to an Amazon Aurora global database (p. 223).

Using Aurora MySQL 5.6.10a for an Aurora global database

The following steps apply to the 5.6.10a version of Aurora MySQL only. For other versions of Aurora MySQL, see Example for Aurora MySQL (p. 211).

To create an Aurora global database using Aurora MySQL 5.6.10a

Complete the Create database page.

1. For Engine options:
   a. Choose Amazon Aurora with MySQL compatibility for the Edition option.
   b. Choose Provisioned for the Capacity type.
   c. Leave Replication features set to the default (single-master replication).
   d. Activate the Show versions that support the global database feature slider.
   e. Choose Aurora (MySQL 5.6) global_10a for Version.

2. For Templates, choose Production.

3. For Global database settings, do the following:
   a. For Global database identifier, enter a meaningful name.
   b. For Credentials Settings, enter your own password for the postgres user account for the DB instance, or let Aurora generate one for you. If you choose Auto generate a password, you get an option to copy the password.
4. For **Encryption**, enable or disable encryption as needed for your use case.

5. The remaining sections of the Create database page configure the **Primary region settings**. Complete these as follows:
   a. For **DB instance size**, choose `db.r4`, `db.r5`, or another memory optimized DB instance size. If necessary, choose **Include previous generation classes** to select the DB instance class you want to use.
   b. For **Availability & durability**, we recommend that you choose to have Aurora create an Aurora Replica in a different AZ for you. If you don't create an Aurora Replica now, you'll need to do it later.
   c. For **Connectivity**, choose the virtual private cloud (VPC) based on Amazon VPC that defines the virtual networking environment for this DB instance. You can choose the defaults to simplify this task.
d. For **Encryption key**, choose the key to use. If you didn’t choose Encryption in the previous step, you can disregard this entry.

e. Complete the **Database authentication** settings for your use case. To simplify the process, you can choose **Password authentication** now and set up AWS Identity and Access Management later.

f. For **Additional configuration**, do the following:

i. For **DB instance identifier**, enter a name for the database instance, or use the default provided. This is the writer instance for the Aurora primary DB cluster for this Aurora global database.

ii. For **DB cluster identifier**, enter a meaningful name or accept the default provided.

iii. Leave the defaults selected for the DB cluster parameter group and DB parameter group, unless you have your own custom parameter groups that you want to use.

iv. You can accept all other default settings for **Additional configuration**.

g. Choose **Create database**. It can take several minutes for Aurora to complete the process of creating the Aurora DB instance, its Aurora Replica, and the Aurora DB cluster. When the Aurora DB cluster is ready to use as the primary DB cluster in an Aurora global database, its status and that of the writer and Replica node display status of Available, as shown in the screenshot below.

This Aurora global database still needs a secondary Aurora DB cluster. You can add that now, by following the steps in [Adding an AWS Region to an Amazon Aurora global database](p. 223).

**Example for Aurora PostgreSQL**

**To create an Aurora global database using Aurora PostgreSQL**

Complete the **Create database** page.

1. For **Engine options**:

   a. Choose **Amazon Aurora with PostgreSQL compatibility** for the Edition option.

   b. Choose ** Provisioned** for the Capacity type.

   c. Activate the **Show versions that support the global database feature** slider.

   d. For **Version**, choose the version of Aurora PostgreSQL that you want to use for your Aurora global database.
2. For Templates, choose Production. Or, you can choose Dev/Test if appropriate for your use case. Don’t use Dev/Test in production environments.

3. For Settings, do the following:
   a. Enter a meaningful name for the DB cluster identifier. When you finish creating the Aurora global database, this name identifies the primary DB cluster.
   b. Enter your own password for the default admin account for the DB cluster, or let Aurora generate one for you. If you choose Auto generate a password, you get an option to copy the password.
4. For **DB instance size**, choose `db.r4`, `db.r5`, or another memory optimized DB instance size. If necessary, choose **Include previous generation classes** to select the DB instance class you want to use.

5. For **Availability & durability**, we recommend that you choose to have Aurora create an Aurora Replica in a different AZ for you. If you don't create an Aurora Replica now, you'll need to do it later.

6. For **Connectivity**, choose the virtual private cloud (VPC) based on Amazon VPC that defines the virtual networking environment for this DB instance. You can choose the defaults to simplify this task.

7. Complete the **Database authentication** settings for your use case. To simplify the process, you can choose **Password authentication** now and set up AWS Identity and Access Management or Password and Kerberos authentication later.

8. For **Additional configuration**, do the following:
   a. Enter a name for **Initial database name** to create the primary Aurora DB instance for this cluster. This is the writer node for the Aurora primary DB cluster.

   Leave the defaults selected for the DB cluster parameter group and DB parameter group, unless you have your own custom parameter groups that you want to use.

   b. You can accept all other default settings for **Additional configuration**, such as Monitoring, Log exports, and so on.

9. Choose **Create database**. It can take several minutes for Aurora to complete the process of creating the Aurora DB instance, its Aurora Replica, and the Aurora DB cluster. When the cluster is ready
to use, the Aurora DB cluster and its writer and Replica nodes all display "Available" status. This
becomes the primary DB cluster of your Aurora global database, after you add a secondary.

When your primary DB cluster is available, create one or more secondary clusters by following the steps in Adding an AWS Region to an Amazon Aurora global database (p. 223).

AWS CLI

The AWS CLI commands in the examples below accomplish the following tasks:

1. Create an Aurora global database, giving it name and specifying the Aurora database engine type you plan to use.
2. Create an Aurora DB cluster for the Aurora global database.
3. Create the Aurora DB instance for the cluster.
4. Create an Aurora DB instance for the Aurora DB cluster.
5. Create a second DB instance for Aurora DB cluster. This is a Reader to complete the Aurora DB cluster.
6. Create a second Aurora DB cluster in another Region and then add it to your Aurora global database, by following the steps in Adding an AWS Region to an Amazon Aurora global database (p. 223).

Follow the example for your Aurora database engine.

CLI examples

- Example for Aurora MySQL (p. 149)
- Example for Aurora PostgreSQL (p. 150)

Example for Aurora MySQL

To create an Aurora global database using Aurora MySQL

1. Use the `create-global-cluster` CLI command, passing the name of the AWS Region, Aurora database engine and version. Choose your parameters from those shown in the table for the version of Aurora MySQL that you want to use.

Other options for Aurora MySQL depend on the version of the Aurora MySQL database engine, as shown in the table.
Amazon Aurora User Guide for Aurora
Getting started with Aurora global databases

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Aurora MySQL 5.6.10a</th>
<th>Aurora MySQL 5.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>--engine</td>
<td>aurora</td>
<td>aurora-mysql</td>
</tr>
<tr>
<td>--engine-mode</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>--engine-version</td>
<td>5.6.10a,</td>
<td>5.7.mysql_aurora.2.07.0,</td>
</tr>
<tr>
<td></td>
<td>5.6.mysql_aurora.1.22.0, 5.7.mysql_aurora.2.07.1,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.6.mysql_aurora.1.22.1, 5.7.mysql_aurora.2.07.2,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.6.mysql_aurora.1.22.2, 5.7.mysql_aurora.2.07.3,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.6.mysql_aurora.1.22.3, 5.7.mysql_aurora.2.08.0,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.6.mysql_aurora.1.23.0, 5.7.mysql_aurora.2.08.1,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.6.mysql_aurora.1.23.1, 5.7.mysql_aurora.2.08.1,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and later versions</td>
<td>5.7.mysql_aurora.2.08.3,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.7.mysql_aurora.2.09.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.7.mysql_aurora.2.08.1,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and later versions</td>
</tr>
</tbody>
</table>

For Linux, macOS, or Unix:

```bash
aws rds create-global-cluster --region primary_region \ 
    --global-cluster-identifier global_database_id \ 
    --engine aurora \ 
    --engine-version version # optional
```

For Windows:

```bash
aws rds create-global-cluster ^ 
    --global-cluster-identifier global_database_id ^ 
    --engine aurora ^ 
    --engine-version version # optional
```

This creates an "empty" Aurora global database, with just a name (identifier) and Aurora database engine. It can take a few minutes for the Aurora global database to be available. Before going to the next step, use the `describe-global-clusters` CLI command to see if it's available.

```bash
aws rds describe-global-clusters --region primary_region --global-cluster-identifier global_database_id
```

When the Aurora global database is available, you can create its primary Aurora DB cluster.

2. To create a primary Aurora DB cluster, use the `create-db-cluster` CLI command. Include the name of your Aurora global database by using the `--global-cluster-identifier`.

For Linux, macOS, or Unix:

```bash
aws rds create-db-cluster \ 
    --region primary_region \ 
    --db-cluster-identifier db_cluster_id \ 
    --master-username userid \ 
    --master-user-password password \ 
    --engine { aurora | aurora-mysql } \ 
    --engine-mode global # Required for --engine-version 5.6.10a only \ 
    --engine-version version \ 
```
Getting started with Aurora global databases

--global-cluster-identifier global_database_id

For Windows:

```
aws rds create-db-cluster ^
--region primary_region ^
--db-cluster-identifier db_cluster_id ^
--master-username userid ^
--master-user-password password ^
--engine { aurora | aurora-mysql } ^
--engine-mode global # Required for --engine-version 5.6.10a only ^
--engine-version version ^
--global-cluster-identifier global_database_id
```

Other options for Aurora MySQL depend on the version of the Aurora MySQL database engine.

Use the `describe-db-clusters` AWS CLI command to confirm that the Aurora DB cluster is ready. To single out a specific Aurora DB cluster, use the `--db-cluster-identifier` parameter. Or you can leave out the Aurora DB cluster name in the command to get details about all your Aurora DB clusters in the given Region.

```
aws rds describe-db-clusters --region primary_region --db-cluster-identifier db_cluster_id
```

When the response shows "Status": "available" for the cluster, it's ready to use.

3. Next, you can create the DB instance for your primary Aurora DB cluster. To do so, use the `create-db-instance` CLI command. Give the command your Aurora DB cluster's name, and specify the configuration details for the instance. You don't need to pass the `--master-username` and `--master-user-password` parameters in the command, because it gets those from the Aurora DB cluster.

For Linux, macOS, or Unix:

```
aws rds create-db-instance \\
--db-cluster-identifier db_cluster_id \\
--db-instance-class instance_class \\
--db-instance-identifier db_instance_id \\
--engine { aurora | aurora-mysql } \\
--engine-mode global # Required for --engine-version 5.6.10a only \\
--engine-version version \\
--region primary_region
```

For Windows:

```
aws rds create-db-instance ^
--db-cluster-identifier db_cluster_id ^
--db-instance-class instance_class ^
--db-instance-identifier db_instance_id ^
--engine { aurora | aurora-mysql } ^
--engine-mode global # Required for --engine-version 5.6.10a only ^
--engine-version version ^
--region primary_region
```

For the `--db-instance-class`, you can use only those from `db.r4` and `db.r5` classes, such as `db.r4.large`. For more complete information, see `DB instance classes`.

220
This command may take some time to complete. Check the status to see if the Aurora DB instance is available before continuing.

```
aws rds describe-db-clusters --db-cluster-identifier sample_secondary_db_cluster
```

When the command returns a status of "available," you can create another Aurora DB instance for your primary DB cluster. This is the reader instance (the Aurora Replica) for the Aurora DB cluster.

4. To create another Aurora DB instance for the cluster, use the `create-db-instance` CLI command:

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--db-cluster-identifier sample_secondary_db_cluster \
--db-instance-class instance_class \
--db-instance-identifier sample_replica_db \
--engine aurora
```

For Windows:

```
aws rds create-db-instance ^
   --db-cluster-identifier sample_secondary_db_cluster ^
   --db-instance-class instance_class ^
   --db-instance-identifier sample_replica_db ^
   --engine aurora
```

When the DB instance is available, replication begins from the writer node to the Replica. Before continuing, check that the DB instance is available with the `describe-db-instances` CLI command.

At this point, you have an Aurora global database with its primary Aurora DB cluster containing a writer DB instance and an Aurora Replica. You can now add a read-only Aurora DB cluster in a different Region to complete your Aurora global database. To do so, follow the steps in Adding an AWS Region to an Amazon Aurora global database (p. 223).

Example for Aurora PostgreSQL

When you create the Aurora objects for an Aurora global database by using the commands in this section, it can take a few minutes for each one to become available. We recommend that after completing any given command, you check the specific Aurora object's status before going to the next command, to make sure that its status is "available." To do so, use the `describe-global-clusters` CLI command:

```
aws rds describe-global-clusters --region primary_region \
   --global-cluster-identifier global_database_id
```

To create an Aurora global database using Aurora PostgreSQL

1. Use the `create-global-cluster` CLI command:

For Linux, macOS, or Unix:

```
aws rds create-global-cluster --region primary_region \
   --global-cluster-identifier global_database_id \
   --engine aurora-postgresql \
   --engine-version version # optional
```
For Windows:

```bash
aws rds create-global-cluster ^
   --global-cluster-identifier global_database_id ^
   --engine aurora-postgresql ^
   --engine-version version # optional
```

When the Aurora global database is available, you can create its primary Aurora DB cluster.

2. To create a primary Aurora DB cluster, use the `create-db-cluster` CLI command. Include the name of your Aurora global database by using the `--global-cluster-identifier`.

For Linux, macOS, or Unix:

```bash
aws rds create-db-cluster \
   --region primary_region \
   --db-cluster-identifier db_cluster_id \
   --master-username userid \
   --master-user-password password \
   --engine aurora-postgresql \
   --engine-version version \
   --global-cluster-identifier global_database_id
```

For Windows:

```bash
aws rds create-db-cluster ^
   --region primary_region ^
   --db-cluster-identifier db_cluster_id ^
   --master-username userid ^
   --master-user-password password ^
   --engine aurora-postgresql ^
   --engine-version version ^
   --global-cluster-identifier global_database_id
```

Check that the Aurora DB cluster is ready. When the response from the following command shows "Status": "available" for the Aurora DB cluster, you can continue.

```bash
aws rds describe-db-clusters --region primary_region --db-cluster-identifier db_cluster_id
```

3. Create the DB instance for your primary Aurora DB cluster. To do so, use the `create-db-instance` CLI command.

- Pass the name of your Aurora DB cluster with the `--db-instance-identifier` parameter

  You don't need to pass the `--master-username` and `--master-user-password` parameters in the command, because it gets those from the Aurora DB cluster.

  For `--db-instance-class`, use only `db.r4` and `db.r5` classes, such as `db.r4.large`. For more information, see DB instance classes.

  For Linux, macOS, or Unix:

```bash
aws rds create-db-instance \
   --db-cluster-identifier db_cluster_id \
   --db-instance-class instance_class \
   --db-instance-identifier db_instance_id \
   --engine aurora-postgresql \
   --engine-version version \
```
For Windows:

```bash
aws rds create-db-instance ^
   --db-cluster-identifier db_cluster_id ^
   --db-instance-class instance_class ^
   --db-instance-identifier db_instance_id ^
   --engine aurora-postgresql ^
   --engine-version version ^
   --region primary_region
```

4. Check the status of the Aurora DB instance before continuing.

```bash
aws rds describe-db-clusters --db-cluster-identifier sample_secondary_db_cluster
```

If the response shows that Aurora DB instance status is "available," you can create another Aurora DB instance for your primary DB cluster.

5. To create an Aurora Replica for Aurora DB cluster, use the `create-db-instance` CLI command.

For Linux, macOS, or Unix:

```bash
aws rds create-db-instance \
   --db-cluster-identifier sample_secondary_db_cluster \
   --db-instance-class instance_class \
   --db-instance-identifier sample_replica_db \
   --engine aurora-postgresql
```

For Windows:

```bash
aws rds create-db-instance ^
   --db-cluster-identifier sample_secondary_db_cluster ^
   --db-instance-class instance_class ^
   --db-instance-identifier sample_replica_db ^
   --engine aurora-postgresql
```

When the DB instance is available, replication begins from the writer node to the Replica. Before continuing, check that the DB instance is available with the `describe-db-instances` CLI command.

Your Aurora global database exists, but it has only its primary Region with an Aurora DB cluster made up of a writer DB instance and an Aurora Replica. You can now add a read-only Aurora DB cluster in a different Region to complete your Aurora global database. To do so, follow the steps in Adding an AWS Region to an Amazon Aurora global database (p. 223).

**RDS API**

To create an Aurora global database with the RDS API, run the `CreateGlobalCluster` operation.

**Adding an AWS Region to an Amazon Aurora global database**

An Aurora global database needs at least one secondary Aurora DB cluster in a different AWS Region than the primary Aurora DB cluster. You can attach up to five secondary DB clusters to your Aurora global database. For each secondary DB cluster that you add to your Aurora global database, reduce the number of Aurora Replicas allowed to the primary DB cluster by one.
For example, if your Aurora global database has 5 secondary Regions, your primary DB cluster can have only 10 (rather than 15) Replicas. For more information, see Configuration requirements of an Amazon Aurora global database (p. 209).

You can't add a secondary cluster to an Aurora global database if the combined total of reader instances in the primary cluster and reader instances in all secondary clusters is 15.

**Console**

**To add an AWS Region to an Aurora global database**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane of the AWS Management Console, choose Databases.
3. Choose the Aurora global database that needs a secondary Aurora DB cluster. Ensure that the primary Aurora DB cluster is Available.
4. For Actions, choose Add region.

5. On the Add a region page, choose the secondary AWS Region. You can't choose an AWS Region that already has a secondary Aurora DB cluster for the same Aurora global database, and it can't be the same Region as the primary Aurora DB cluster.

6. Complete the remaining fields for the secondary Aurora cluster in the new AWS Region, and then choose Add region.

After you finish adding the Region to your Aurora global database, you can see it in the list of Databases in the AWS Management Console as shown in the screenshot.
AWS CLI

To add a secondary AWS Region to an Aurora global database

1. Use the `create-db-cluster` CLI command with the name (`--global-cluster-identifier`) of your Aurora global database. For other parameters, do the following:
2. For `--region`, choose a different AWS Region than that of your Aurora primary Region.
3. For an Aurora MySQL5.6.10a–based Aurora global database only, use the following parameters:
   - `--engine - aurora`
   - `--engine-mode - global`
   - `--engine-version - 5.6.10a`
4. For an Aurora global database based on other Aurora DB engines, choose values for the `--engine` and `--engine-version` parameters that are same as those for the primary Aurora DB cluster in your Aurora global database. The table summarizes some the options currently available.
5. For an encrypted cluster, specify your primary AWS Region as the `--source-region` for encryption.

The following example creates a new Aurora DB cluster and attaches it to an Aurora global database as a read-only secondary Aurora DB cluster. In the last step, an Aurora DB instance is added to the new Aurora DB cluster.

For Linux, macOS, or Unix:

```
aws rds --region secondary_region \
create-db-cluster \
```
Getting started with Aurora global databases

```bash
aws rds --region secondary_region
    create-db-cluster
        --db-cluster-identifier secondary_cluster_id
        --global-cluster-identifier global_database_id
        --engine { aurora | aurora-mysql | aurora-postgresql }
        --engine-version version
```

For Windows:

```bash
aws rds --region secondary_region
    create-db-cluster
        --db-cluster-identifier secondary_cluster_id
        --global-cluster-identifier global_database_id
        --engine { aurora | aurora-mysql | aurora-postgresql }
        --engine-version version
```

RDS API

To add a new AWS Region to an Aurora global database with the RDS API, run the `CreateDBCluster` operation. Specify the identifier of the existing global database using the `GlobalClusterIdentifier` parameter.

Using a snapshot for your Amazon Aurora global database

You can restore a snapshot of an Aurora DB cluster or from an Amazon RDS DB instance to use as the starting point for your Aurora global database. You restore the snapshot and create a new Aurora provisioned DB cluster at the same time. You then add another AWS Region to the restored DB cluster, thus turning it into an Aurora global database. Any Aurora DB cluster that you create using a snapshot in this way becomes the primary cluster of your Aurora global database.

The snapshot that you use can be from a provisioned or from a serverless Aurora DB cluster.

**Note**

You can't create a provisioned Aurora DB cluster from a snapshot made from an Aurora MySQL 5.6.10a–based global database. A snapshot from an Aurora MySQL 5.6.10a–based global database can only be restored as an Aurora global database.

During the restore process, choose the same DB engine type as the snapshot. So, for example, to restore a snapshot that was made from an Aurora Serverless v1 DB cluster running Aurora PostgreSQL, you create an Aurora PostgreSQL DB cluster using that same Aurora DB engine and version.

The restored DB cluster assumes the role of primary cluster for Aurora global database when you add an AWS Regions to it. All data contained in this primary cluster is replicated to any secondary clusters that you add to your Aurora global database.
Managing an Amazon Aurora global database

You perform most management operations on the individual clusters that make up an Aurora global database. When you choose Group related resources on the Databases page in the console, you see the primary cluster and secondary clusters grouped under the associated global database object.

The Configuration tab for an Aurora global database shows the AWS Regions where its Aurora DB clusters are running, the Aurora DB engine and version, and the global database identifier.

Topics
- Modifying an Amazon Aurora global database (p. 228)
- Modifying parameters for an Aurora global database (p. 228)
- Removing a cluster from an Amazon Aurora global database (p. 228)
Modifying an Amazon Aurora global database

The Databases page in the AWS Management Console lists all your Aurora global databases, showing the primary cluster and secondary clusters for each one. The Aurora global database is an object that has its own configuration settings, in particular the AWS Regions associated with the primary and secondary clusters.

When you make changes to the Aurora global database, you have a chance to cancel changes, as shown in the following screenshot.

![Modify global database: lab-east-west-global](image)

When you choose Continue, you confirm the changes.

Modifying parameters for an Aurora global database

You can configure the Aurora DB cluster parameter groups independently for each Aurora cluster within the Aurora global database. Most parameters work the same as for other kinds of Aurora clusters. We recommend that you keep settings consistent among all the clusters in a global database, to avoid unexpected behavior changes if you promote a secondary cluster to be the primary.

For example, use the same settings for time zones and character sets to avoid inconsistent behavior if a different cluster takes over as the primary cluster.

The `aurora_enable_repl_bin_log_filtering` and `aurora_enable_replica_log_compression` configuration settings have no effect.

Removing a cluster from an Amazon Aurora global database

You can remove Aurora DB clusters from your Aurora global database for several different reasons. For example, you might want to remove an Aurora DB cluster from an Aurora global database if the primary
Removing an Aurora DB cluster from an Aurora global database has different results, depending on whether it's the primary DB cluster or a secondary DB cluster.

- Removing a secondary cluster detaches it from the Aurora global database and promotes it to the primary cluster role. It's no longer synchronized with the primary, and instead has full read/write capabilities. You can then use it as the primary for a new Aurora global database.
- Removing a primary cluster detaches it from the Aurora global database and makes it a standalone Aurora DB cluster.

You can remove Aurora DB clusters from your Aurora global database using the AWS Management Console, the AWS CLI, or the RDS API.

**Console**

**To remove an Aurora cluster from an Aurora global database**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose the cluster on the **Databases** page.
3. For **Actions**, choose **Remove from Global**.

4. You see a prompt to confirm that you want to detach the secondary from the Aurora global database.
5. Choose **Remove and promote** to remove the cluster from the global database.

The Aurora DB cluster is no longer serving as a secondary in the Aurora global database, and is no longer synchronized with the primary DB cluster. It is a standalone Aurora DB cluster with full read/write capability.

After you remove or delete all secondary clusters, then you can remove the primary cluster the same way. You can't detach (remove) the primary Aurora DB cluster from an Aurora global database until after you remove all secondary clusters.

The Aurora global database might remain in the Databases list, with 0 Regions and AZs. You can delete if you no longer want to use this Aurora global database. For more information, see *Deleting an Amazon Aurora global database* (p. 231).

**AWS CLI**

To remove an Aurora cluster from an Aurora global database, run the `remove-from-global-cluster` CLI command with the following parameters:

- `--global-cluster-identifier` – The name (identifier) of your Aurora global database.
- `--db-cluster-identifier` – The name of each Aurora DB cluster to remove from the Aurora global database. Remove all secondary Aurora DB clusters before removing the primary.

The following examples first remove a secondary cluster and then the primary cluster from an Aurora global database.

For Linux, macOS, or Unix:

```bash
aws rds --region secondary_region \
remove-from-global-cluster \
  --db-cluster-identifier secondary_cluster_ARN \
  --global-cluster-identifier global_database_id
```
Managing an Aurora global database

aws rds --region primary_region \  
  remove-from-global-cluster \  
  --db-cluster-identifier primary_cluster_ARN \  
  --global-cluster-identifier global_database_id

Repeat the `remove-from-global-cluster --db-cluster-identifier secondary_cluster_ARN` command for each secondary AWS Region in your Aurora global database.

For 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

Repeat the `remove-from-global-cluster --db-cluster-identifier secondary_cluster_ARN` command for each secondary AWS Region in your Aurora global database.

RDS API

To remove an Aurora cluster from an Aurora global database with the RDS API, run the `RemoveFromGlobalCluster` action.

Deleting an Amazon Aurora global database

Because an Aurora global database typically holds business-critical data, you can’t delete the global database and its associated clusters in a single step. To complete delete an Aurora global database, do the following:

- Remove all secondary DB clusters from the Aurora global database. Each cluster becomes a standalone Aurora DB cluster. To learn how, see Removing a cluster from an Amazon Aurora global database (p. 228).
- From each standalone Aurora DB cluster, delete all Aurora Replicas.
- Remove the primary DB cluster from the Aurora global database. This becomes a standalone Aurora DB cluster.
- From the Aurora primary DB cluster, first delete all Aurora Replicas, then delete the writer DB instance.

Deleting the writer instance from the newly standalone Aurora DB cluster also typically removes the Aurora DB cluster and the Aurora global database.

For more general information, see Deleting an Aurora DB cluster or a DB instance (p. 398).

To delete an Aurora global database, you can use the AWS Management Console, the AWS CLI, or the RDS API.

Console

To delete an Aurora global database

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose **Databases** and find the Aurora global database you want to delete in the listing.

3. Confirm that all clusters are removed from the Aurora global database. The Aurora global database should show 0 Regions and A2s and a Size of 0 clusters.

   If the Aurora global database contains any Aurora DB clusters, you can't delete it. If necessary, detach the primary and secondary Aurora DB clusters from the Aurora global database. For more information, see Removing a cluster from an Amazon Aurora global database (p. 228).

4. Choose your Aurora global database in the list, and then choose **Delete** from the Actions menu.

---

### AWS CLI

To delete an Aurora global database, run the `delete-global-cluster` CLI command with the name of the AWS Region and the Aurora global database identifier, as shown in the following example.

For Linux, macOS, or Unix:

```
aws rds --region primary_region delete-global-cluster \
    --global-cluster-identifier global_database_id
```

For Windows:

```
aws rds --region primary_region delete-global-cluster ^
    --global-cluster-identifier global_database_id
```

### RDS API

To delete a cluster that is part of an Aurora global database, run the `DeleteGlobalCluster` API operation.

---

### Connecting to an Amazon Aurora global database

How you connect to an Aurora global database depends on whether you need to write to the database or read from the database.

- For read-only requests or queries, you connect to the reader endpoint for the Aurora cluster in your AWS Region.
- To run data manipulation language (DML) or data definition language (DDL) statements, you connect to the cluster endpoint for the primary cluster. This endpoint might be in a different AWS Region than your application.

When you view an Aurora global database in the console, you can see all the general-purpose endpoints associated with all of its clusters. The following screenshot shows an example. There is a single cluster endpoint associated with the primary cluster that you use for write operations. The primary cluster
and each secondary cluster has a reader endpoint that you use for read-only queries. To minimize latency, choose whichever reader endpoint is in your AWS Region or the AWS Region closest to you. The following shows an Aurora MySQL example.

Using write forwarding in an Amazon Aurora global database

You can reduce the number of endpoints that you need to manage for applications running on your Aurora global database, by using write forwarding. This feature of Aurora MySQL lets secondary clusters in an Aurora global database forward SQL statements that perform write operations to the primary cluster. The primary cluster updates the source and then propagates resulting changes back to all secondary AWS Regions.

The write forwarding configuration saves you from implementing your own mechanism to send write operations from a secondary AWS Region to the primary Region. Aurora handles the cross-Region networking setup. Aurora also transmits all necessary session and transactional context for each statement. The data is always changed first on the primary cluster and then replicated to the secondary clusters in the Aurora global database. This way, the primary cluster is the source of truth and always has an up-to-date copy of all your data.

Note
Write forwarding requires Aurora MySQL version 2.08.1 or later.

Topics
- Enabling write forwarding (p. 233)
- Checking if a secondary cluster has write forwarding enabled (p. 235)
- Application and SQL compatibility with write forwarding (p. 236)
- Isolation and consistency for write forwarding (p. 237)
- Running multipart statements with write forwarding (p. 240)
- Transactions with write forwarding (p. 240)
- Configuration parameters for write forwarding (p. 241)
- Amazon CloudWatch metrics for write forwarding (p. 242)

Enabling write forwarding

By default, write forwarding isn't enabled when you add a secondary cluster to an Aurora global database.

To enable write forwarding using the AWS Management Console, choose the Enable read replica write forwarding option when you perform the Add a Region action for a global database. For an existing secondary cluster, modify the cluster to use the Enable read replica write forwarding option. To turn off write forwarding, clear the Enable read replica write forwarding check box when adding the Region or modifying the secondary cluster.

To enable write forwarding using the AWS CLI, use the --enable-global-write-forwarding option. This option works when you create a new secondary cluster using the create-db-cluster command.
It also works when you modify an existing secondary cluster using the `modify-db-cluster` command. It requires that the global database uses an Aurora version that supports write forwarding. You can turn write forwarding off by using the `--no-enable-global-write-forwarding` option with these same CLI commands.

To enable write forwarding using the Amazon RDS API, set the `EnableGlobalWriteForwarding` parameter to `true`. This parameter works when you create a new secondary cluster using the `CreateDBCluster` operation. It also works when you modify an existing secondary cluster using the `ModifyDBCluster` operation. It requires that the global database uses an Aurora version that supports write forwarding. You can turn write forwarding off by setting the `EnableGlobalWriteForwarding` parameter to `false`.

**Note**
For a database session to take advantage of write forwarding, make sure that you also specify a setting for the `aurora_replica_read_consistency` configuration parameter. Do this in every session that uses the write forwarding feature. For information about this parameter, see Isolation and consistency for write forwarding (p. 237).

The following CLI examples show how you can set up an Aurora global database with write forwarding enabled or disabled. The highlighted items represent the commands and options that are important to specify and keep consistent when setting up the infrastructure for an Aurora global database.

The following example creates an Aurora global database, a primary cluster, and a secondary cluster with write forwarding enabled. Substitute your own choices for the user name, password, and primary and secondary AWS Regions.

```
# Create overall global database.
aws rds create-global-cluster --global-cluster-identifier write-forwarding-test \\   --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.08.1 \\   --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.2.08.1 \\   --master-username my_user_name --master-user-password my_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.2.08.1 \\   --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.2.08.1 \\   --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.2.08.1 \\   --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.2.08.1 \\   --region us-east-2 \\   --enable-global-write-forwarding
```

234
Using write forwarding in an Aurora global database

```bash
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.2.08.1
   --region us-east-2

aws rds modify-db-cluster --db-cluster-identifier write-forwarding-test-cluster-2
   --region us-east-2
   --enable-global-write-forwarding
```

The following example continues from the previous one. It creates a secondary cluster without write forwarding enabled, then enables write forwarding. After this example finishes, all secondary clusters in the global database have write forwarding enabled.

```bash
# Create secondary cluster, in a different AWS Region than the global database, without write forwarding enabled.
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.2.08.1
   --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.2.08.1
   --region us-west-1

aws rds modify-db-cluster --db-cluster-identifier write-forwarding-test-cluster-2
   --region us-west-1
   --enable-global-write-forwarding
```

Checking if a secondary cluster has write forwarding enabled

To determine whether you can use write forwarding from a secondary cluster, you can check whether the cluster has the attribute "GlobalWriteForwardingStatus": "enabled".

In the AWS Management Console, you see Read replica write forwarding on the Configuration tab of the details page for the cluster. To see the status of the global write forwarding setting for all of your clusters, run the following AWS CLI command.

A secondary cluster shows the value "enabled" or "disabled" to indicate if write forwarding is turned on or off. A value of null indicates that write forwarding isn't available for that cluster. Either the cluster isn't part of a global database, or is the primary cluster instead of a secondary cluster. The value can also be "enabling" or "disabling" if write forwarding is in the process of being turned on or off.

Example

```bash
aws rds describe-db-clusters --query '{[
{DBClusterIdentifier:DBClusterIdentifier,GlobalWriteForwardingStatus:GlobalWriteForwardingStatus}]
|
{ "GlobalWriteForwardingStatus": "enabled",
  "DBClusterIdentifier": "aurora-write-forwarding-test-replica-1"
},
```

235
To find all secondary clusters that have global write forwarding enabled, run the following command. This command also returns the cluster's reader endpoint. You use the secondary cluster's reader endpoint to when you use write forwarding from the secondary to the primary in your Aurora global database.

Example

```bash
aws rds describe-db-clusters --query 'DBClusters[].
{DBClusterIdentifier:DBClusterIdentifier,GlobalWriteForwardingStatus:GlobalWriteForwardingStatus,ReaderEndpoint:ReaderEndpoint}
| [?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"
 }
]
```

Application and SQL compatibility with write forwarding

Certain statements aren't allowed or can produce stale results when you use them in a global database with write forwarding. Thus, the `EnableGlobalWriteForwarding` setting is turned off by default for secondary clusters. Before turning it on, check to make sure that your application code isn't affected by any of these restrictions.

You can use the following kinds of SQL statements with write forwarding:

- Data manipulation language (DML) statements, such as `INSERT`, `DELETE`, and `UPDATE`. There are some restrictions on the properties of these statements that you can use with write forwarding, as described following.
- `SELECT ... LOCK IN SHARE MODE` and `SELECT FOR UPDATE` statements.
- `PREPARE` and `EXECUTE` statements.

The following restrictions apply to the SQL statements you use with write forwarding. In some cases, you can use the statements on secondary clusters with write forwarding enabled at the cluster level. This approach works if write forwarding isn't turned on within the session by the `aurora_replica_read_consistency` configuration parameter. Trying to use a statement when it's not allowed because of write forwarding causes an error message with the following format.

```
ERROR 1235 (42000): This version of MySQL doesn't yet support 'operation with write forwarding'.
```

Data definition language (DDL)

Connect to the primary cluster to run such statements.
Updating a permanent table using data from a temporary table

You can use temporary tables on secondary clusters with write forwarding enabled. However, you can't use a DML statement to modify a permanent table if the statement refers to a temporary table. For example, you can't use an INSERT ... SELECT statement that takes the data from a temporary table. The temporary table exists on the secondary cluster and isn't available when the statement runs on the primary cluster.

**XA transactions**

You can't use the following statements on a secondary cluster when write forwarding is turned on within the session. You can use these statements on secondary clusters that don't have write forwarding enabled, or within sessions where the `aurora_replica_read_consistency` setting is empty. Before turning on write forwarding within a session, check if your code uses these statements.

```
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 statements for permanent tables**

You can't use the following statements on a secondary cluster with write forwarding enabled.

```
LOAD DATA INFIL 'data.txt' INTO TABLE t1;
LOAD XML LOCAL INFIL 'test.xml' INTO TABLE t1;
```

You can load data into a temporary table on a secondary cluster. However, make sure that you run any LOAD statements that refer to permanent tables only on the primary cluster.

**Plugin statements**

You can't use the following statements on a secondary cluster with write forwarding enabled.

```
INSTALL PLUGIN example SONAME 'ha_example.so';
UNINSTALL PLUGIN example;
```

**SAVEPOINT statements**

You can't use the following statements on a secondary cluster when write forwarding is turned on within the session. You can use these statements on secondary clusters that don't have write forwarding enabled, or within sessions where the `aurora_replica_read_consistency` setting is blank. Check if your code uses these statements before turning on write forwarding within a session.

```
SAVEPOINT t1_save;
ROLLBACK TO SAVEPOINT t1_save;
RELEASE SAVEPOINT t1_save;
```

**Isolation and consistency for write forwarding**

In sessions that use write forwarding, you can only use the REPEATABLE READ isolation level. Although you can also use the READ COMMITTED isolation level with read-only clusters in secondary AWS Regions,
that isolation level doesn't work with write forwarding. For information about the REPEATABLE READ and READ COMMITTED isolation levels, see Aurora MySQL isolation levels (p. 865).

You can control the degree of read consistency on a secondary cluster. The read consistency level determines how much waiting the secondary cluster does before each read operation to ensure that some or all changes are replicated from the primary cluster. You can adjust the read consistency level to ensure that all forwarded write operations from your session are visible in the secondary cluster before any subsequent queries. You can also use this setting to ensure that queries on the secondary cluster always see the most current updates from the primary cluster, even those submitted by other sessions or other clusters. To specify this type of behavior for your application, you choose a value for the session-level parameter `aurora_replica_read_consistency`.

**Important**

Make sure that you set the `aurora_replica_read_consistency` parameter in each session that uses write forwarding. Otherwise, Aurora doesn't enable write forwarding for that session. This parameter has an empty default value. For it to take effect, choose a specific value. The `aurora_replica_read_consistency` parameter has an effect only on secondary clusters where write forwarding is enabled.

For the `aurora_replica_read_consistency` parameter, you can specify the values EVENTUAL, SESSION, and GLOBAL.

As you increase the consistency level, your application spends more time waiting for changes to be propagated between AWS Regions. You can choose the balance between fast response time and ensuring that changes made in other locations are fully available before your queries run.

With the read consistency set to EVENTUAL, queries in a secondary AWS Region that uses write forwarding might see data that is slightly stale due to replication lag. Results of write operations in the same session aren't visible until the write operation is performed on the primary Region and replicated to the current Region. The query doesn't wait for the updated results to be available. Thus, it might retrieve the older data or the updated data, depending on the timing of the statements and the amount of replication lag.

With the read consistency set to SESSION, all queries in a secondary AWS Region that uses write forwarding see the results of all changes made in that session. The changes are visible regardless of whether the transaction is committed. If necessary, the query waits for the results of forwarded write operations to be replicated to the current Region. It doesn't wait for updated results from write operations performed in other Regions or in other sessions within the current Region.

With the read consistency set to GLOBAL, a session in a secondary AWS Region sees changes made by that session. It also sees all committed changes from both the primary AWS Region and other secondary AWS Regions. Each query might wait for a period that varies depending on the amount of session lag. The query proceeds when the secondary cluster is up-to-date with all committed data from the primary cluster, as of the time that the query began.

For more information about all the parameters involved with write forwarding, see Configuration parameters for write forwarding (p. 241).

**Examples of using write forwarding**

In this example, the primary cluster is in the AWS Region US East (N. Virginia). The secondary cluster is in the AWS Region US East (Ohio). The example shows the effects of running INSERT statements followed by SELECT statements. Depending on the value of the `aurora_replica_read_consistency` setting, the results might differ depending on the timing of the statements. To achieve higher consistency, you might wait briefly before issuing the SELECT statement, or Aurora can automatically wait until the results finish replicating before proceeding with the SELECT.

In this example, with a read consistency setting of eventual, running an INSERT statement immediately followed by a SELECT statement still returns the value of COUNT(*) reflecting the number
of rows before the new row is inserted. Running the SELECT again a short time later does return the updated row count. The SELECT statements don't do any waiting.

```
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)
```

With a read consistency setting of session, a SELECT statement immediately after an INSERT does wait until the changes from the INSERT statement are visible. Subsequent SELECT statements don't do any waiting.

```
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)
```

With the read consistency setting still set to session, introducing a brief wait after performing an INSERT statement makes the updated row count available by the time the next SELECT statement runs.

```
mysql> insert into t1 values (6); select sleep(2); select count(*) from t1;
Query OK, 1 row affected (0.07 sec)
+----------+
| count(*) |
+----------+
|        7 |
+----------+
1 row in set (0.00 sec)
```
With a read consistency setting of `global`, each `SELECT` statement waits to ensure that all data changes as of the start time of the statement are visible before performing the query. The amount of waiting for each `SELECT` statement varies, depending on the amount of replication lag between the primary and secondary clusters.

Running multipart statements with write forwarding

A DML statement might consist of multiple parts, such as a `INSERT ... SELECT` statement or a `DELETE ... WHERE` statement. In this case, the entire statement is forwarded to the primary cluster and run there.

Transactions with write forwarding

Whether the transaction is forwarded to the primary cluster depends on the access mode of the transaction. You can specify the access mode for the transaction by using the `SET TRANSACTION` statement or the `START TRANSACTION` statement. You can also specify the transaction access mode by changing the value of the Aurora MySQL session variable `tx_read_only`. You can only change this session value while you're connected to a secondary cluster that has write forwarding enabled.

If a long-running transaction doesn't issue any statement for a substantial period of time, it might exceed the idle timeout period. This period has a default of one minute. You can increase it up to one day. A transaction that exceeds the idle timeout is canceled by the primary cluster. The next subsequent statement you submit receives a timeout error. Then Aurora rolls back the transaction.
This type of error can occur in other cases when write forwarding becomes unavailable. For example, Aurora cancels any transactions that use write forwarding if you restart the primary cluster or if you turn off the write forwarding configuration setting.

Configuration parameters for write forwarding

The Aurora cluster parameter groups contain some new settings for the write forwarding feature. Because these are cluster parameters, all DB instances in each cluster have the same values for these variables. To control the incoming write requests from secondary clusters, use these settings on the primary cluster:

- `aurora_fwd_master_max_connections_pct`: The upper limit on database connections that can be used on a writer DB instance to handle queries forwarded from readers. It's expressed as a percentage of the `max_connections` setting for the writer DB instance in the primary cluster. For example, if `max_connections` is 800 and `aurora_fwd_master_max_connections_pct` is 10, then the writer allows a maximum of 80 simultaneous forwarded sessions. These connections come from the same connection pool managed by the `max_connections` setting.

  This setting applies only on the primary cluster, when one or more secondary clusters have write forwarding enabled. If you decrease the value, existing connections aren't affected. Aurora takes the new value of the setting into account when attempting to create a new connection from a secondary cluster. The default value is 10, representing 10% of the `max_connections` value. If you enable query forwarding on any of the secondary clusters, this setting must have a nonzero value for write operations from secondary clusters to succeed. If the value is zero, the write operations receive the error code `ER_CON_COUNT_ERROR` with the message Not enough connections on master to handle your request.

- `aurora_fwd_master_idle_timeout`: The number of seconds the primary cluster waits for activity on a connection that's forwarded from a secondary cluster before closing it. If the session remains idle beyond this period, Aurora cancels the session.

The following new parameter is a session-level parameter:

- `aurora_replica_read_consistency`: A value that enables write forwarding. For write forwarding to happen, set it in each session. For more details, see Isolation and consistency for write forwarding (p. 237).

  Specifies the level of read consistency. You can specify one of the following values:

  - `EVENTUAL`
  - `SESSION`
  - `GLOBAL`

  For information about the meaning of the consistency levels, see Isolation and consistency for write forwarding (p. 237).

The following rules apply to this parameter:

- This is a session-level parameter. The default value is " (empty).

- Write forwarding is available in a session only if `aurora_replica_read_consistency` is set to `EVENTUAL` or `SESSION` or `GLOBAL`. This parameter is relevant only in reader instances of secondary clusters that have write forwarding enabled and that are in an Aurora global database.

- You can't set this variable (when empty) or unset (when already set) inside a multistatement transaction. However, you can change it from one valid value (`EVENTUAL`, `SESSION`, or `GLOBAL`) to another valid value (`EVENTUAL`, `SESSION`, or `GLOBAL`) during such a transaction.

- The variable can't be `SET` when write forwarding isn't enabled on the secondary cluster.

- Setting the session variable on a primary cluster doesn't have any effect. If you try to modify this variable on a primary cluster, you receive an error.
The following table shows details for these parameters.

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Type</th>
<th>Default value</th>
<th>Valid values</th>
</tr>
</thead>
<tbody>
<tr>
<td>aurora_replica_read_consistency</td>
<td>Session</td>
<td>Enum</td>
<td>&quot;</td>
<td>EVENTUAL, SESSION, GLOBAL</td>
</tr>
<tr>
<td>aurora_fwd_master_max_connections</td>
<td>Global</td>
<td>unsigned long integer</td>
<td>10</td>
<td>0–90</td>
</tr>
<tr>
<td>aurora_fwd_master_idle_timeout</td>
<td>Global</td>
<td>unsigned integer</td>
<td>60</td>
<td>1–86,400</td>
</tr>
</tbody>
</table>

Amazon CloudWatch metrics for write forwarding

The following Amazon CloudWatch metrics apply to the primary cluster when you use write forwarding on one or more secondary clusters. These metrics are all measured on the writer DB instance in the primary cluster.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Aurora MySQL status variable</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>ForwardingMasterDMLLatency</td>
<td></td>
<td>Average time to process each forwarded DML statement on the writer DB instance. It doesn't include the time for the secondary cluster to forward the write request. It also doesn't include the time to replicate changes back to the secondary cluster.</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>ForwardingMasterOpenSessions</td>
<td></td>
<td>Number of forwarded sessions on the writer DB instance.</td>
<td>Count</td>
</tr>
<tr>
<td>ForwardingMasterDMLThroughput</td>
<td></td>
<td>Number of forwarded DML statements processed each second by this writer DB instance.</td>
<td>Count per second</td>
</tr>
<tr>
<td>Aurora_fwd_master_dml_stmt_duration</td>
<td></td>
<td>Total duration of DML statements forwarded to this writer DB instance.</td>
<td>Microseconds</td>
</tr>
<tr>
<td>Aurora_fwd_master_dml_stmt_count</td>
<td></td>
<td>Total number of DML statements forwarded to this writer DB instance.</td>
<td></td>
</tr>
<tr>
<td>Aurora_fwd_master_select_stmt_duration</td>
<td></td>
<td>Total duration of SELECT statements</td>
<td>Microseconds</td>
</tr>
</tbody>
</table>
### Using write forwarding in an Aurora global database

<table>
<thead>
<tr>
<th>Metric</th>
<th>Aurora MySQL status variable</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aurora_fwd_master_select_stmt_count</td>
<td>Total number of SELECT statements forwarded to this writer DB instance.</td>
<td></td>
</tr>
</tbody>
</table>

The following CloudWatch metrics apply to each secondary cluster. These metrics are measured on each reader DB instance in a secondary cluster with write forwarding enabled.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Aurora MySQL status variable</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ForwardingReplicaDMLLatency</td>
<td>Average response time in milliseconds of forwarded DMLs on replica.</td>
<td>Milliseconds</td>
</tr>
<tr>
<td></td>
<td>ForwardingReplicaReadWaitLatency</td>
<td>Average wait time in milliseconds that a SELECT statement on a reader DB instance waits to catch up to the primary cluster. The degree to which the reader DB instance waits before processing a query depends on the aurora_replica_read_consistency setting.</td>
<td>Milliseconds</td>
</tr>
<tr>
<td></td>
<td>ForwardingReplicaDMLThroughput</td>
<td>Number of forwarded DML statements processed per second.</td>
<td>Count per second</td>
</tr>
<tr>
<td></td>
<td>ForwardingReplicaReadWaitThroughput</td>
<td>Number of SELECT statements processed per second in sessions with write forwarding enabled.</td>
<td>Count per second</td>
</tr>
<tr>
<td></td>
<td>ForwardingReplicaOpenSessions</td>
<td>The number of sessions that are using write forwarding on a reader DB instance.</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td>Aurora_fwd_replica_dml_stmt_count</td>
<td>Total number of DML statements forwarded from this reader DB instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aurora_fwd_replica_dml_stmt_duration</td>
<td>Total duration of DML statements forwarded</td>
<td>Microseconds</td>
</tr>
</tbody>
</table>
### Disaster recovery for Amazon Aurora global databases

In some cases, your Aurora global database might include more than one secondary AWS Region. If so, you can choose which AWS Region to fail over to if an outage affects the primary AWS Region. To help determine which secondary AWS Region to choose, you can monitor the replication lag for all your secondary Regions. In some cases, one secondary Region might have substantially less replication lag than the others. If so, that’s a good indication that the associated Aurora cluster has enough database and network capacity to take over the full read/write workload for your application.

When your global database has multiple secondary Regions, make sure that you detach all the secondary Regions if the primary AWS Region experiences an outage. Then, you promote one of those secondary Regions to be the new primary AWS Region. Finally, you create new clusters in each of the other secondary Regions and attach those clusters to your global database.

When you promote a secondary cluster to be the primary cluster, you also need to update the endpoints that your applications use to connect to the global database. To get a new writer endpoint from a newly promoted cluster, you can convert a former reader endpoint by removing `-ro` from the endpoint string. For example, if a former reader endpoint is `global-16rr-test-cluster-1.cluster-ro-12345678901.us-west-2.rds.amazonaws.com`, then the new promoted writer endpoint is `global-16rr-test-cluster-1.cluster-cps2igpwyrwa.us-west-2.rds.amazonaws.com`.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuroraMySQLstatusvariable</td>
<td>from this reader DB instance.</td>
<td></td>
</tr>
<tr>
<td>Aurora_fwd_replica_select_stmt_duration</td>
<td>Total duration of SELECT statements forwarded from this reader DB instance.</td>
<td>Microseconds</td>
</tr>
<tr>
<td>Aurora_fwd_replica_select_stmt_count</td>
<td>Total number of SELECT statements forwarded from this reader DB instance.</td>
<td></td>
</tr>
<tr>
<td>Aurora_fwd_replica_read_wait_duration</td>
<td>Total duration of waits due to the read consistency setting on this reader DB instance</td>
<td>Microseconds</td>
</tr>
<tr>
<td>Aurora_fwd_replica_read_wait_count</td>
<td>Total number of read-after-write waits on this reader DB instance.</td>
<td></td>
</tr>
<tr>
<td>Aurora_fwd_replica_errors_session_limit</td>
<td>Number of sessions rejected by the primary cluster due to the error conditions master full or Too many forwarded statements in progress.</td>
<td></td>
</tr>
</tbody>
</table>
Failover for Amazon Aurora global databases

Aurora global databases offer a higher level of failover capability than a default Aurora cluster. If an entire cluster in one AWS Region becomes unavailable, you can promote another cluster in the global database to have read/write capability.

You can manually activate the failover mechanism if a cluster in a different AWS Region is a better choice to be the primary cluster. For example, you might increase the capacity of one of the secondary clusters and then promote it to be the primary cluster. Or the balance of activity among the AWS Regions might change, so that switching the primary cluster to a different AWS Region might give lower latency for write operations.

The following procedure outlines what to do to promote one of the secondary clusters in an Aurora global database.

To promote a secondary cluster

Before you begin the procedure, the primary cluster fails or otherwise becomes unavailable.

1. Remove the secondary cluster from the Aurora global database. Doing so promotes the cluster to full read/write capability. To learn how to remove an Aurora cluster from a global database, see Removing a cluster from an Amazon Aurora global database (p. 228).
2. Reconfigure your application to divert write traffic to the newly promoted cluster.
   
   **Important**
   At this point, stop issuing any DML statements or other write operations to the cluster that became unavailable. To avoid data inconsistencies between the clusters, known as a "split-brain" scenario, avoid writing to the former primary cluster, even if it comes back online.
3. Create a new Aurora global database with the newly promoted cluster as the primary cluster. To learn how to create an Aurora global database, see Creating an Amazon Aurora global database (p. 209).
4. Add to the Aurora global database the AWS Region of the cluster that encountered the issue. Now that AWS Region contains a new secondary cluster. To learn how to add an AWS Region to an Aurora global database, see Adding an AWS Region to an Amazon Aurora global database (p. 223).
5. When the outage is resolved and you're ready to assign your original AWS Region as the primary cluster again, perform the same steps in reverse:
   a. Remove one of the secondary clusters from the Aurora global database.
   b. Make that cluster the primary cluster of a new Aurora global database in the original AWS Region.
   c. Redirect all the write traffic to the primary cluster in the original AWS Region.
   d. Add an AWS Region to set up one or more secondary clusters in the same AWS Regions as before.

Managing recovery for Aurora global databases

You can control the point at which a global database resumes, in case of disasters such as network or hardware failures that affect the primary DB cluster. You manage recovery by setting a recovery point objective (RPO) for the global database.
Note
Managing the RPO is currently supported for Amazon Aurora with PostgreSQL compatibility. For a list of supported Aurora PostgreSQL versions and AWS Regions, see Limitations of Amazon Aurora global databases (p. 207).

The recovery point objective is the oldest age of data that you want recoverable from a secondary DB cluster. The RPO is used when your database resumes operations in a new AWS Region after a failover. It represents the amount of data loss measured in time that you're willing to accept on a database failover.

By using a managed RPO, you can control the maximum amount of data loss as the secondary DB clusters lag behind the primary DB cluster. This data loss is measured in time and is called the RPO lag time. When you set the RPO, Aurora PostgreSQL enforces it on your global database as follows:

1. Aurora PostgreSQL allows transactions to commit on the primary DB cluster if the RPO lag time of at least one secondary DB cluster is less than the RPO time.
2. Aurora PostgreSQL blocks transaction commits if there is no secondary DB cluster that has an RPO lag time less than the RPO time. If Aurora PostgreSQL starts blocking commits, it inserts an event into the PostgreSQL log file. It then emits wait events that show the sessions that are blocked.
3. Aurora PostgreSQL allows transactions to commit again on the primary DB cluster when the RPO lag time of at least one secondary DB cluster becomes less than the RPO time.

This approach ensures that Aurora PostgreSQL doesn't allow transaction commits to complete that would result in a violation of your chosen RPO time.

Topics
- Viewing the recovery point objective (p. 246)
- Setting the recovery point objective (p. 246)
- Disabling the recovery point objective (p. 247)

Viewing the recovery point objective
The recovery point objective (RPO) of a global database is stored in the rds.global_db_rpo parameter. To view the current RPO setting of the rds.global_db_rpo parameter and other parameters of the cluster parameter group, see Viewing parameter values for a DB cluster parameter group (p. 316).

Setting the recovery point objective
You can set the global database's RPO using the AWS Management Console, the AWS CLI, or the RDS API. For more information, see Modifying parameters in a DB cluster parameter group (p. 305).

Console

To set the RPO
1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Identify the primary DB cluster's parameter group of the global database. For more information about a cluster's configuration settings, see Modifying an Amazon Aurora global database (p. 228).
3. Open the primary DB cluster parameter group and set the rds.global_db_rpo parameter. For more information, see Modifying parameters in a DB cluster parameter group (p. 305).
4. Set the rds.global_db_rpo parameter value to the number of seconds you want for the recovery point objective. Valid values are from 20 seconds up to the maximum integer value of 2,147,483,647 (68 years).
AWS CLI

To set the `rds.global_db_rpo` parameter, use the AWS CLI, use the `modify-db-cluster-parameter-group` command.

The following example sets the RPO to 5,000 seconds for the primary DB cluster parameter group named `global_db_cluster_parameter_group`. Valid values are from 20 seconds up to the maximum integer value of 2,147,483,647 (68 years).

For Linux, macOS, or Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name global_db_cluster_parameter_group \
  --parameters "ParameterName=rds.global_db_rpo,ParameterValue=5000,ApplyMethod=immediate"
```

For Windows:

```
aws rds modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name global_db_cluster_parameter_group ^
  --parameters "ParameterName=rds.global_db_rpo,ParameterValue=5000,ApplyMethod=immediate"
```

RDS API

To modify the `rds.global_db_rpo` parameter, use the Amazon RDS ModifyDBClusterParameterGroup API operation.

Disabling the recovery point objective

To disable the RPO, reset the `rds.global_db_rpo` parameter. You can reset parameters using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To disable the RPO

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.
3. In the list, choose your primary DB cluster parameter group.
4. Choose Edit parameters.
5. Choose the box next to the `rds.global_db_rpo` parameter.
6. Choose Reset.
7. When the screen shows Reset parameters in DB parameter group, choose Reset parameters.

For more information on how to reset a parameter with the console, see Modifying parameters in a DB cluster parameter group (p. 305).

AWS CLI

To reset the `rds.global_db_rpo` parameter, use the `reset-db-cluster-parameter-group` command.

For Linux, macOS, or Unix:

```
aws rds reset-db-cluster-parameter-group \
  --db-cluster-parameter-group-name global_db_cluster_parameter_group \
```

For Windows:

```
aws rds reset-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name global_db_cluster_parameter_group ^
```

```
**Monitoring an Aurora global database**

When you create the Aurora DB clusters that make up your Aurora global database, you can choose many options that let you monitor your DB cluster’s performance. These options include the following:

- **Amazon RDS Performance Insights** – Enables performance schema in the underlying Aurora database engine. To learn more about Performance Insights and Aurora global databases, see [Monitoring an Amazon Aurora global database with Amazon RDS Performance Insights](p. 249).
- **Enhanced monitoring** – Generates metrics for process or thread utilization on the CPU.
- **Amazon CloudWatch Logs** – Publishes specified log types to CloudWatch Logs. Error logs are published by default, but you can choose other logs specific to your Aurora database engine.
  - For Aurora MySQL–based Aurora DB clusters, you can export the audit log, general log, and slow query log.
  - For Aurora PostgreSQL–based Aurora DB clusters, you can export the Postgresql log.
  - For Aurora PostgreSQL–based global databases, you can use certain functions to check status of your Aurora global database and its instances. To learn how, see [Monitoring Aurora PostgreSQL-based Amazon Aurora global databases](p. 249).

The following screenshot shows some of the options available on the Monitoring tab of a primary Aurora DB cluster in an Aurora global database.
Monitoring an Amazon Aurora global database with Amazon RDS Performance Insights

You can use Amazon RDS Performance Insights for your Aurora global databases. You enable this feature individually, for each Aurora DB cluster in your Aurora global database. To do so, you choose Enable Performance Insights in the Additional configuration section of the Create database page. Or, you can Modify your Aurora DB clusters to use this feature after they are up and running. You can enable or turn off Performance Insights for each cluster that's part of your Aurora global database.

The reports created by Performance Insights apply to each cluster in the global database. When you add a new secondary AWS Region to an Aurora global database that's already using Performance Insights, be sure that you enable Performance Insights in the newly added cluster. It doesn't inherit the Performance Insights setting from the existing global database.

You can switch AWS Regions while viewing the Performance Insights page for a DB instance that's attached to a global database. However, you might not see performance information immediately after switching AWS Regions. Although the DB instances might have identical names in each AWS Region, the associated Performance Insights URL is different for each DB instance. After switching AWS Regions, choose the name of the DB instance again in the Performance Insights navigation pane.

For DB instances associated with a global database, the factors affecting performance might be different in each AWS Region. For example, the DB instances in each AWS Region might have different capacity.

To learn more about using Performance Insights, see Using Amazon RDS Performance Insights (p. 514).

Monitoring Aurora PostgreSQL-based Amazon Aurora global databases

To view the status of a global database, use the aurora_global_db_status and aurora_global_db_instance_status functions.

**Note**
Only Aurora PostgreSQL supports the aurora_global_db_status and aurora_global_db_instance_status functions.

**To monitor an Aurora PostgreSQL-based global database**

1. Connect to the global database primary cluster endpoint using a PostgreSQL utility such as psql. For more information about how to connect, see Connecting to an Amazon Aurora global database (p. 232).
2. Use the aurora_global_db_status function in a psql command to list the primary and secondary volumes. This shows the lag times of the global database secondary DB clusters.

```sql
postgres=> select * from aurora_global_db_status();
```

<table>
<thead>
<tr>
<th>aws_region</th>
<th>highest_lsn_written</th>
<th>durability_lag_in_msec</th>
<th>rpo_lag_in_msec</th>
<th>last_lag_calculation_time</th>
<th>feedback_epoch</th>
<th>feedback_xmin</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-1</td>
<td>93763984222</td>
<td>-1</td>
<td>-1</td>
<td>1970-01-01 00:00:00+00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>us-west-2</td>
<td>93763984222</td>
<td>900</td>
<td>1090</td>
<td>2020-05-12 22:49:14.328+00</td>
<td>3315479243</td>
<td></td>
</tr>
</tbody>
</table>
```
The output includes a row for each DB cluster of the global database containing the following columns:

- **aws_region** – The AWS Region that this DB cluster is in. For tables listing AWS Regions by engine, see [Regions and Availability Zones](#).
- **highest_lsn_written** – The highest log sequence number (LSN) currently written on this DB cluster.

A log sequence number (LSN) is a unique sequential number that identifies a record in the database transaction log. LSNs are ordered such that a larger LSN represents a later transaction.

- **durability_lag_in_msec** – The timestamp difference between the highest log sequence number written on a secondary DB cluster (highest_lsn_written) and the highest_lsn_written on the primary DB cluster.
- **rpo_lag_in_msec** – The recovery point objective (RPO) lag. This lag is the time difference between the most recent user transaction commit stored on a secondary DB cluster and the most recent user transaction commit stored on the primary DB cluster.
- **last_lag_calculation_time** – The timestamp when values were last calculated for replication_lag_in_msec and rpo_lag_in_msec.
- **feedback_epoch** – The epoch the secondary DB cluster uses when it generates hot standby information.

**Hot standby** is when a DB cluster can connect and query while the server is in recovery or standby mode. Hot standby feedback is information about the DB cluster when it’s in hot standby. For more information, see [Hot standby](#) in the PostgreSQL documentation.

- **feedback_xmin** – The minimum (oldest) active transaction ID used by the secondary DB cluster.

3. Use the `aurora_global_db_instance_status` function to list all secondary DB instances for both the primary DB cluster and secondary DB clusters.

```sql
postgres=> select * from aurora_global_db_instance_status();
```

<table>
<thead>
<tr>
<th>server_id</th>
<th>session_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>apg-global-db-rpo-mammothrw-elephantro-1-n1</td>
<td>MASTER_SESSION_ID</td>
</tr>
<tr>
<td>us-east-1</td>
<td>93763985102</td>
</tr>
<tr>
<td>apg-global-db-rpo-mammothrw-elephantro-1-n2</td>
<td>f38430cf-6576-479a-b296-dc06b1b1964a</td>
</tr>
<tr>
<td>us-east-1</td>
<td>93763985099</td>
</tr>
<tr>
<td>apg-global-db-rpo-elephantro-mammothrw-n1</td>
<td>0d9f1d98-04ad-4aa4-8fd6-e08674cbbf9f</td>
</tr>
<tr>
<td>us-west-2</td>
<td>93763985095</td>
</tr>
<tr>
<td>(3 rows)</td>
<td></td>
</tr>
</tbody>
</table>

The output includes a row for each DB instance of the global database containing the following columns:

- **server_id** – The server identifier for the DB instance.
- **session_id** – A unique identifier for the current session.
- **aws_region** – The AWS Region that this DB instance is in. For tables listing AWS Regions by engine, see [Regions and Availability Zones](#).
• **durable_lsn** – The LSN made durable in storage.
• **highest_lsn_rcvd** – The highest LSN received by the DB instance from the writer DB Instance.
• **feedback_epoch** – The epoch the DB instance uses when it generates hot standby information.

Hot standby is when a DB instance can connect and query while the server is in recovery or standby mode. Hot standby feedback is information about the DB instance when it's in hot standby. For more information, see the PostgreSQL documentation on [Hot standby](https://www.postgresql.org/docs/current/standby-replication.html).

• **feedback_xmin** – The minimum (oldest) active transaction ID used by the DB instance.
• **oldest_read_view_lsn** – The oldest LSN used by the DB instance to read from storage.
• **visibility_lag_in_msec** – How far this DB instance is lagging behind the writer DB instance.

To see how these values change over time, consider the following transaction block where a table insert takes an hour.

```sql
psql> BEGIN;
pql> INSERT INTO table1 SELECT Large_Data_That_Takes_1_Hr_To_Insert;
pql> COMMIT;
```

In some cases, there might be a network disconnect between the primary DB cluster and the secondary DB cluster after the `BEGIN` statement. If so, the secondary DB cluster's `replication_lag_in_msec` value starts increasing. At the end of the `INSERT` statement, the `replication_lag_in_msec` value is 1 hour. However, the `rpo_lag_in_msec` value is 0 because all the user data committed between the primary DB cluster and secondary DB cluster are still the same. As soon as the `COMMIT` statement completes, the `rpo_lag_in_msec` value increases.

**Using Amazon Aurora global databases with other AWS services**

You can use your Aurora global databases with other AWS services, such as Amazon S3 and AWS Lambda. Doing so requires that all Aurora DB clusters in your global database have the same privileges, external functions, and so on in the respective AWS Regions. Because a read-only Aurora secondary DB cluster in an Aurora global database can be promoted to the role of primary, we recommend that you set up write privileges ahead of time, on all Aurora DB clusters for any services you plan to use with your Aurora global database.

The following procedures summarize the actions to take for each AWS service.

**To invoke AWS Lambda functions from an Aurora global database**

1. For all the Aurora clusters that make up the Aurora global database, perform the procedures in [Invoking a Lambda function from an Amazon Aurora MySQL DB cluster](p. 818).
2. For each cluster in the Aurora global database, set the (ARN) of the new IAM (IAM) role.
3. To permit database users in an Aurora global database to invoke Lambda functions, associate the role that you created in [Creating an IAM role to allow Amazon Aurora to access AWS services](p. 799) with each cluster in the Aurora global database.
4. Configure each cluster in the Aurora global database to allow outbound connections to Lambda. For instructions, see [Enabling network communication from Amazon Aurora MySQL to other AWS services](p. 803).
To load data from Amazon S3

1. For all the Aurora clusters that make up the Aurora global database, perform the procedures in Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804).

2. For each Aurora cluster in the global database, set either the aurora_load_from_s3_role or aws_default_s3_role DB cluster parameter to the Amazon Resource Name (ARN) of the new IAM role. If an IAM role isn't specified for aurora_load_from_s3_role, Aurora uses the IAM role specified in aws_default_s3_role.

3. To permit database users in an Aurora global database to access S3, associate the role that you created in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799) with each Aurora cluster in the global database.

4. Configure each Aurora cluster in the global database to allow outbound connections to S3. For instructions, see Enabling network communication from Amazon Aurora MySQL to other AWS services (p. 803).

To save queried data to Amazon S3

1. For all the Aurora clusters that make up the Aurora global database, perform the procedures in Saving data from an Amazon Aurora MySQL DB cluster into text files in an Amazon S3 bucket (p. 812).

2. For each Aurora cluster in the global database, set either the aurora_select_into_s3_role or aws_default_s3_role DB cluster parameter to the Amazon Resource Name (ARN) of the new IAM role. If an IAM role isn't specified for aurora_select_into_s3_role, Aurora uses the IAM role specified in aws_default_s3_role.

3. To permit database users in an Aurora global database to access S3, associate the role that you created in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799) with each Aurora cluster in the global database.

4. Configure each Aurora cluster in the global database to allow outbound connections to S3. For instructions, see Enabling network communication from Amazon Aurora MySQL to other AWS services (p. 803).
Connecting to an Amazon Aurora DB cluster

You can connect to an Aurora DB cluster using the same tools that you use to connect to a MySQL or PostgreSQL database. You specify a connection string with any script, utility, or application that connects to a MySQL or PostgreSQL DB instance. You use the same public key for Secure Sockets Layer (SSL) connections.

In the connection string, you typically use the host and port information from special endpoints associated with the DB cluster. With these endpoints, you can use the same connection parameters regardless of how many DB instances are in the cluster. You also use the host and port information from a specific DB instance in your Aurora DB cluster for specialized tasks, such as troubleshooting.

**Note**
For Aurora Serverless v1 DB clusters, you connect to the database endpoint rather than to the DB instance. You can find the database endpoint for an Aurora Serverless v1 DB cluster on the Connectivity & security tab of the AWS Management Console. For more information, see Using Amazon Aurora Serverless v1 (p. 134).

Regardless of the Aurora DB engine and specific tools you use to work with the DB cluster or instance, the endpoint must be accessible. An Amazon Aurora DB cluster can be created only in a virtual private cloud (VPC) based on the Amazon VPC service. That means that you access the endpoint from either inside the VPC or outside the VPC using one of the following approaches.

- **Access the Amazon Aurora DB cluster inside the VPC** – Enable access to the Amazon Aurora DB cluster through the VPC. You do so by editing the Inbound rules on the Security group for the VPC to allow access to your specific Aurora DB cluster. To learn more, including how to configure your VPC for different Aurora DB cluster scenarios, see Amazon Virtual Private Cloud VPCs and Amazon Aurora.

- **Access the Amazon Aurora DB cluster outside the VPC** – To access an Amazon Aurora DB cluster from outside the VPC, use the public endpoint address of the Amazon Aurora DB cluster. You can also connect to an Amazon Aurora DB cluster that’s inside a VPC from an Amazon EC2 instance not in the VPC by using ClassicLink. For more information, see A DB instance in a VPC accessed by an EC2 instance not in a VPC (p. 1290).

For more information, see Troubleshooting Aurora connection failures (p. 258).

**Topics**
- Connecting to an Amazon Aurora MySQL DB cluster (p. 253)
- Connecting to an Amazon Aurora PostgreSQL DB cluster (p. 257)
- Troubleshooting Aurora connection failures (p. 258)
- Managing connections with Amazon RDS Proxy (p. 260)

**Connecting to an Amazon Aurora MySQL DB cluster**

To authenticate to your Aurora MySQL DB cluster, you can use either MySQL user name and password authentication or AWS Identity and Access Management (IAM) database authentication. For more information on using MySQL user name and password authentication, see Access control and account management in the MySQL documentation. For more information on using IAM database authentication, see IAM database authentication (p. 1238).

When you have a connection to your Amazon Aurora DB cluster with MySQL 5.6 compatibility, you can run SQL commands that are compatible with MySQL version 5.6. For more information about MySQL 5.6 SQL syntax, see the MySQL 5.6 reference manual.

When you have a connection to your Amazon Aurora DB cluster with MySQL 5.7 compatibility, you can run SQL commands that are compatible with MySQL version 5.7. For more information about MySQL 5.7
SQL syntax, see the MySQL 5.7 reference manual. For information about limitations that apply to Aurora MySQL 5.7, see Comparison of Aurora MySQL 5.7 and MySQL 5.7 (p. 636).

**Note**
For a helpful and detailed guide on connecting to an Amazon Aurora MySQL DB cluster, you can see the Aurora connection management handbook.

In the details view for your DB cluster, you can find the cluster endpoint, which you can use in your MySQL connection string. The endpoint is made up of the domain name and port for your DB cluster. For example, if an endpoint value is mycluster.cluster-123456789012.us-east-1.rds.amazonaws.com:3306, then you specify the following values in a MySQL connection string:

- For host or host name, specify mycluster.cluster-123456789012.us-east-1.rds.amazonaws.com
- For port, specify 3306 or the port value you used when you created the DB cluster

The cluster endpoint connects you to the primary instance for the DB cluster. You can perform both read and write operations using the cluster endpoint. Your DB cluster can also have up to 15 Aurora Replicas that support read-only access to the data in your DB cluster. The primary instance and each Aurora Replica has a unique endpoint that is independent of the cluster endpoint and allows you to connect to a specific DB instance in the cluster directly. The cluster endpoint always points to the primary instance. If the primary instance fails and is replaced, then the cluster endpoint points to the new primary instance.

To view the cluster endpoint (writer endpoint), choose Databases on the Amazon RDS console and choose the name of the DB cluster to show the DB cluster details.
Connection utilities for Aurora MySQL

Some connection utilities you can use are the following:

- **Command line** – You can connect to an Amazon Aurora DB cluster by using tools like the MySQL command line utility. For more information on using the MySQL utility, see the [mysql - the MySQL command line tool](https://dev.mysql.com/doc/) in the MySQL documentation.

- **GUI** – You can use the MySQL Workbench utility to connect by using a UI interface. For more information, see the [Download MySQL workbench](https://dev.mysql.com/downloads/workbench/) page.

- **Applications** – You can use the MariaDB Connector/J utility to connect your applications to your Aurora DB cluster. For more information, see the [MariaDB Connector/J download](https://dev.mysql.com/downloads/mariadb-connectors-java/) page.

  **Note**
  
  If you use the MariaDB Connector/J utility with an Aurora Serverless v1 DB cluster, use the prefix `jdbc:mariadb:aurora://` in your connection string. The `mariadb:aurora` parameter avoids the automatic DNS scan for failover targets. That scanning is not needed with Aurora Serverless v1 DB clusters and causes a delay in establishing the connection.
You can use SSL encryption on connections to an Amazon Aurora DB instance. For information, see Using SSL with a MySQL DB instance.

**Connecting with SSL for Aurora MySQL**

To connect using SSL, use the MySQL utility as described in the following procedure. If you are using IAM database authentication, you must use an SSL connection. For information, see IAM database authentication (p. 1238).

**Note**

To connect to the cluster endpoint using SSL, your client connection utility must support Subject Alternative Names (SAN). If your client connection utility doesn't support SAN, you can connect directly to the instances in your Aurora DB cluster. For more information on Aurora endpoints, see Amazon Aurora connection management (p. 24).

**To connect to a DB cluster with SSL using the MySQL utility**

1. Download the public key for the Amazon RDS signing certificate.

   For information about downloading certificates, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).

2. Type the following command at a command prompt to connect to the primary instance of a DB cluster with SSL using the MySQL utility. For the -h parameter, substitute the endpoint DNS name for your primary instance. For the --ssl_ca parameter, substitute the SSL certificate file name as appropriate. Type the master user password when prompted.

   ```
   mysql -h mycluster-primary.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=[full path]rds-combined-ca-bundle.pem --ssl-verify-server-cert
   ```

   You should see output similar to the following.

   ```
   Welcome to the MySQL monitor. Commands end with ; or \g.
   Your MySQL connection id is 350
   Server version: 5.6.10-log MySQL Community Server (GPL)
   Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
   mysql>
   ```

   For general instructions on constructing Amazon RDS MySQL connection strings and finding the public key for SSL connections, see Connecting to a DB instance running the MySQL database engine.

**Connecting with the Amazon Web Services JDBC Driver for MySQL (preview)**

*This is preview documentation for Amazon Web Services JDBC Driver for MySQL. It is subject to change.*

The AWS JDBC Driver for MySQL (preview) is a client driver designed for the high availability of Aurora MySQL. The AWS JDBC Driver for MySQL is drop-in compatible with the MySQL Connector/J driver.

The AWS JDBC Driver for MySQL takes full advantage of the failover capabilities of Aurora MySQL. The AWS JDBC Driver for MySQL fully maintains a cache of the DB cluster topology and each DB instance's
Amazon Aurora User Guide for Aurora
Connecting to Aurora PostgreSQL

role, either primary DB instance or Aurora Replica. It uses this topology to bypass the delays caused by
DNS resolution so that a connection to the new primary DB instance is established as fast as possible.

For more information about the AWS JDBC Driver for MySQL and complete instructions for using it, see
the AWS JDBC Driver for MySQL GitHub repository.

Connecting to an Amazon Aurora PostgreSQL DB
cluster

You can connect to a DB instance in your Amazon Aurora PostgreSQL DB cluster using the same tools
that you use to connect to a PostgreSQL database. As part of this, you use the same public key for
Secure Sockets Layer (SSL) connections. You can use the endpoint and port information from the primary
instance or Aurora Replicas in your Aurora PostgreSQL DB cluster in the connection string of any script,
utility, or application that connects to a PostgreSQL DB instance. In the connection string, specify the
DNS address from the primary instance or Aurora Replica endpoint as the host parameter. Specify the
port number from the endpoint as the port parameter.

When you have a connection to a DB instance in your Amazon Aurora PostgreSQL DB cluster, you can run
any SQL command that is compatible with PostgreSQL version 9.6.3.

In the details view for your Aurora PostgreSQL DB cluster you can find the cluster endpoint. You use this
endpoint in your PostgreSQL connection string. The endpoint is made up of the domain name and port
for your DB cluster. For example, if an endpoint value is mycluster.cluster-123456789012.us-
east-1.rds.amazonaws.com:5432, then you specify the following values in a PostgreSQL connection
string:

• For host or host name, specify mycluster.cluster-123456789012.us-
east-1.rds.amazonaws.com
• For port, specify 5432 or the port value you used when you created the DB cluster

The cluster endpoint connects you to the primary instance for the DB cluster. You can perform both read
and write operations using the cluster endpoint. Your DB cluster can also have up to 15 Aurora Replicas
that support read-only access to the data in your DB cluster. Each DB instance in the Aurora cluster
(that is, the primary instance and each Aurora Replica) has a unique endpoint that is independent of
the cluster endpoint. This unique endpoint allows you to connect to a specific DB instance in the cluster
directly. The cluster endpoint always points to the primary instance. If the primary instance fails and is
replaced, the cluster endpoint points to the new primary instance.

To view the cluster endpoint (writer endpoint), choose Databases on the Amazon RDS console and
choose the name of the DB cluster to show the DB cluster details.
Connection utilities for Aurora PostgreSQL

Some connection utilities you can use are the following:

- **Command line** – You can connect to an Amazon Aurora PostgreSQL DB instance by using tools like `psql`, the PostgreSQL interactive terminal. For more information on using the PostgreSQL interactive terminal, see `psql` in the PostgreSQL documentation.
- **GUI** – You can use the pgAdmin utility to connect to a PostgreSQL DB instance by using a UI interface. For more information, see the Download page from the pgAdmin website.
- **Applications** – You can use the PostgreSQL JDBC driver to connect your applications to your PostgreSQL DB instance. For more information, see the Download page from the PostgreSQL JDBC driver website.

Troubleshooting Aurora connection failures

Common causes of connection failures to a new Aurora DB cluster include the following:
• **Security group in the VPC doesn't allow access** – Your VPC needs to allow connections from your device or from an Amazon EC2 instance by proper configuration of the Security group in the VPC. To resolve, modify your VPC's Security group Inbound rules to allow connections. For an example, see Create a VPC and subnets (p. 1281).

• **Port blocked by firewall rules** – Check the value of the port configured for your Aurora DB cluster. If a firewall rule blocks that port, you can re-create the instance using a different port.

• **Incomplete or incorrect IAM configuration** – If you created your Aurora DB instance to use IAM–based authentication, make sure that it's properly configured. For more information, see IAM database authentication (p. 1238).

For more information about troubleshooting Aurora DB connection issues, see Can't connect to Amazon RDS DB instance (p. 1306).
Managing connections with Amazon RDS Proxy

By using Amazon RDS Proxy, you can allow your applications to pool and share database connections to improve their ability to scale. RDS Proxy makes applications more resilient to database failures by automatically connecting to a standby DB instance while preserving application connections. RDS Proxy also enables you to enforce AWS Identity and Access Management (IAM) authentication for databases, and securely store credentials in AWS Secrets Manager.

**Note**

RDS Proxy is fully compatible with MySQL and PostgreSQL. You can enable RDS Proxy for most applications with no code changes.

Using RDS Proxy, you can handle unpredictable surges in database traffic that otherwise might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool without the memory and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created.

RDS Proxy queues or throttles application connections that can’t be served immediately from the pool of connections. Although latencies might increase, your application can continue to scale without abruptly failing or overwhelming the database. If connection requests exceed the limits you specify, RDS Proxy rejects application connections (that is, it sheds load). At the same time, it maintains predictable performance for the load that can be served with the available capacity.

You can reduce the overhead to process credentials and establish a secure connection for each new connection. RDS Proxy can handle some of that work on behalf of the database.

**Topics**

- RDS Proxy concepts and terminology (p. 260)
- Planning for and setting up RDS Proxy (p. 264)
- Connecting to a database through RDS Proxy (p. 275)
- Managing an RDS Proxy (p. 277)
- Monitoring RDS Proxy using Amazon CloudWatch (p. 285)
- Command-line examples for RDS Proxy (p. 289)
- Troubleshooting for RDS Proxy (p. 291)
- Using RDS Proxy with AWS CloudFormation (p. 297)

**RDS Proxy concepts and terminology**

You can simplify connection management for your Amazon RDS DB instances and Amazon Aurora DB clusters by using RDS Proxy.

RDS Proxy handles the network traffic between the client application and the database. It does so in an active way first by understanding the database protocol. It then adjusts its behavior based on the SQL operations from your application and the result sets from the database.

RDS Proxy reduces the memory and CPU overhead for connection management on your database. The database needs less memory and CPU resources when applications open many simultaneous connections. It also doesn’t require logic in your applications to close and reopen connections that stay idle for a long time. Similarly, it requires less application logic to reestablish connections in case of a database problem.

The infrastructure for RDS Proxy is highly available and deployed over multiple Availability Zones (AZs). The computation, memory, and storage for RDS Proxy are independent of your RDS DB instances and
Aurora DB clusters. This separation helps lower overhead on your database servers, so that they can devote their resources to serving database workloads. The RDS Proxy compute resources are serverless, automatically scaling based on your database workload.

Topics
- Overview of RDS Proxy concepts (p. 261)
- Connection pooling (p. 262)
- RDS Proxy security (p. 262)
- Failover (p. 263)
- Transactions (p. 264)

Overview of RDS Proxy concepts

RDS Proxy handles the infrastructure to perform connection pooling and the other features described following. You see the proxies represented in the RDS console on the Proxies page.

Each proxy handles connections to a single RDS DB instance or Aurora DB cluster. The proxy automatically determines the current writer instance for RDS Multi-AZ DB instances and Aurora provisioned clusters. For Aurora multi-master clusters, the proxy connects to one of the writer instances and uses the other writer instances as hot standby targets.

The connections that a proxy keeps open and available for your database application to use form the connection pool.

By default, RDS Proxy can reuse a connection after each transaction in your session. This transaction-level reuse is called multiplexing. When RDS Proxy temporarily removes a connection from the connection pool to reuse it, that operation is called borrowing the connection. When it's safe to do so, RDS Proxy returns that connection to the connection pool.

In some cases, RDS Proxy can't be sure that it's safe to reuse a database connection outside of the current session. In these cases, it keeps the session on the same connection until the session ends. This fallback behavior is called pinning.

A proxy has an endpoint. You connect to this endpoint when you work with an RDS DB instance or Aurora DB cluster, instead of connecting to the read/write endpoint that connects directly to the instance or cluster. The special-purpose endpoints for an Aurora cluster remain available for you to use.

For example, you can still connect to the cluster endpoint for read/write connections without connection pooling. You can still connect to the reader endpoint for load-balanced read-only connections. You can still connect to the instance endpoints for diagnosis and troubleshooting of specific DB instances within an Aurora cluster. If you are using other AWS services such as AWS Lambda to connect to RDS databases, you change their connection settings to use the proxy endpoint. For example, you specify the proxy endpoint to allow Lambda functions to access your database while taking advantage of RDS Proxy functionality.

Each proxy contains a target group. This target group embodies the RDS DB instance or Aurora DB cluster that the proxy can connect to. For an Aurora cluster, by default the target group is associated with all the DB instances in that cluster. That way, the proxy can connect to whichever Aurora DB instance is promoted to be the writer instance in the cluster. The RDS DB instance associated with a proxy, or the Aurora DB cluster and its instances, are called the targets of that proxy. For convenience, when you create a proxy through the console, RDS Proxy also creates the corresponding target group and registers the associated targets automatically.

An engine family is a related set of database engines that use the same DB protocol. You choose the engine family for each proxy that you create.
Connection pooling

Each proxy performs connection pooling for the writer instance of its associated RDS or Aurora database. Connection pooling is an optimization that reduces the overhead associated with opening and closing connections and with keeping many connections open simultaneously. This overhead includes memory needed to handle each new connection. It also involves CPU overhead to close each connection and open a new one, such as Transport Layer Security/Secure Sockets Layer (TLS/SSL) handshaking, authentication, negotiating capabilities, and so on. Connection pooling simplifies your application logic. You don’t need to write application code to minimize the number of simultaneous open connections.

Each proxy also performs connection multiplexing, also known as connection reuse. With multiplexing, RDS Proxy perform all the operations for a transaction using one underlying database connection, then can use a different connection for the next transaction. You can open many simultaneous connections to the proxy, and the proxy keeps a smaller number of connections open to the DB instance or cluster. Doing so further minimizes the memory overhead for connections on the database server. This technique also reduces the chance of “too many connections” errors.

RDS Proxy security

RDS Proxy uses the existing RDS security mechanisms such as TLS/SSL and AWS Identity and Access Management (IAM). For general information about those security features, see Security in Amazon Aurora (p. 1205). If you aren’t familiar with how RDS and Aurora work with authentication, authorization, and other areas of security, make sure to familiarize yourself with how RDS and Aurora work with those areas first.

RDS Proxy can act as an additional layer of security between client applications and the underlying database. For example, you can connect to the proxy using TLS 1.2, even if the underlying DB instance supports only TLS 1.0 or 1.1. You can connect to the proxy using an IAM role, even if the proxy connects to the database using the native user and password authentication method. By using this technique, you can enforce strong authentication requirements for database applications without a costly migration effort for the DB instances themselves.

You store the database credentials used by RDS Proxy in AWS Secrets Manager. Each database user for the RDS DB instance or Aurora DB cluster accessed by a proxy must have a corresponding secret in Secrets Manager. You can also set up IAM authentication for users of RDS Proxy. By doing so, you can enforce IAM authentication for database access even if the databases use native password authentication. We recommend using these security features instead of embedding database credentials in your application code.

Using TLS/SSL with RDS Proxy

You can connect to RDS Proxy using the TLS/SSL protocol.

**Note**

RDS Proxy uses certificates from the AWS Certificate Manager (ACM). If you use RDS Proxy, when you rotate your TLS/SSL certificate you don't need to update applications that use RDS Proxy connections.

To enforce TLS for all connections between the proxy and your database, you can specify a setting Require Transport Layer Security when you create or modify a proxy.

RDS Proxy can also ensure that your session uses TLS/SSL between your client and the RDS Proxy endpoint. To have RDS Proxy do so, specify the requirement on the client side. SSL session variables are not set for SSL connections to a database using RDS Proxy.

- For Amazon RDS MySQL and Aurora MySQL, specify the requirement on the client side with the --ssl-mode parameter when you run the mysql command.
- For Amazon RDS PostgreSQL and Aurora PostgreSQL, specify sslmode=require as part of the conninfo string when you run the psql command.
RDS Proxy supports TLS protocol version 1.0, 1.1, and 1.2. You can connect to the proxy using a higher version of TLS than you use in the underlying database.

By default, client programs establish an encrypted connection with RDS Proxy, with further control available through the `--ssl-mode` option. From the client side, RDS Proxy supports all SSL modes.

For the client, the SSL modes are the following:

**PREFERRED**

SSL is the first choice, but it isn't required.

**DISABLED**

No SSL is allowed.

**REQUIRED**

Enforce SSL.

**VERIFY_CA**

Enforce SSL and verify the certificate authority (CA).

**VERIFY_IDENTITY**

Enforce SSL and verify the CA and CA hostname.

When using a client with `--ssl-mode` VERIFY_CA or VERIFY_IDENTITY, specify the `--ssl-ca` option pointing to a CA in .pem format. For a .pem file that you can use, download the Amazon root CA 1 trust store from Amazon Trust Services.

RDS Proxy uses wildcard certificates, which apply to a both a domain and its subdomains. If you use the `mysql` client to connect with SSL mode VERIFY_IDENTITY, currently you must use the MySQL 8.0-compatible `mysql` command.

**Failover**

*Failover* is a high-availability feature that replaces a database instance with another one when the original instance becomes unavailable. A failover might happen because of a problem with a database instance. It might also be part of normal maintenance procedures, such as during a database upgrade. Failover applies to RDS DB instances in a Multi-AZ configuration, and Aurora DB clusters with one or more reader instances in addition to the writer instance.

Connecting through a proxy makes your application more resilient to database failovers. When the original DB instance becomes unavailable, RDS Proxy connects to the standby database without dropping idle application connections. Doing so helps to speed up and simplify the failover process. The result is faster failover that's less disruptive to your application than a typical reboot or database problem.

Without RDS Proxy, a failover involves a brief outage. During the outage, you can't perform write operations on that database. Any existing database connections are disrupted and your application must reopen them. The database becomes available for new connections and write operations when a read-only DB instance is promoted to take the place of the one that's unavailable.

During DB failovers, RDS Proxy continues to accept connections at the same IP address and automatically directs connections to the new primary DB instance. Clients connecting through RDS Proxy are not susceptible to the following:

- Domain Name System (DNS) propagation delays on failover.
- Local DNS caching.
• Connection timeouts.
• Uncertainty about which DB instance is the current writer.
• Waiting for a query response from a former writer that became unavailable without closing connections.

For applications that maintain their own connection pool, going through RDS Proxy means that most connections stay alive during failovers or other disruptions. Only connections that are in the middle of a transaction or SQL statement are canceled. RDS Proxy immediately accepts new connections. When the database writer is unavailable, RDS Proxy queues up incoming requests.

For applications that don't maintain their own connection pools, RDS Proxy offers faster connection rates and more open connections. It offloads the expensive overhead of frequent reconnects from the database. It does so by reusing database connections maintained in the RDS Proxy connection pool. This approach is particularly important for TLS connections, where setup costs are significant.

Transactions

All the statements within a single transaction always use the same underlying database connection. The connection becomes available for use by a different session when the transaction ends. Using the transaction as the unit of granularity has the following consequences:

• Connection reuse can happen after each individual statement when the RDS MySQL or Aurora MySQL autocommit setting is enabled.
• Conversely, when the autocommit setting is disabled, the first statement you issue in a session begins a new transaction. Thus, if you enter a sequence of SELECT, INSERT, UPDATE, and other data manipulation language (DML) statements, connection reuse doesn't happen until you issue a COMMIT, ROLLBACK, or otherwise end the transaction.
• Entering a data definition language (DDL) statement causes the transaction to end after that statement completes.

RDS Proxy detects when a transaction ends through the network protocol used by the database client application. Transaction detection doesn't rely on keywords such as COMMIT or ROLLBACK appearing in the text of the SQL statement.

In some cases, RDS Proxy might detect a database request that makes it impractical to move your session to a different connection. In these cases, it turns off multiplexing for that connection the remainder of your session. The same rule applies if RDS Proxy can't be certain that multiplexing is practical for the session. This operation is called pinning. For ways to detect and minimize pinning, see Avoiding pinning (p. 283).

Planning for and setting up RDS Proxy

In the following sections, you can find how to set up RDS Proxy. You can also find how to set the related security options that control who can access each proxy and how each proxy connects to DB instances.

Topics

• Limitations for RDS Proxy (p. 265)
• Identifying DB instances, clusters, and applications to use with RDS Proxy (p. 266)
• Setting up network prerequisites (p. 266)
• Setting up database credentials in AWS Secrets Manager (p. 267)
• Setting up AWS Identity and Access Management (IAM) policies (p. 269)
• Creating an RDS Proxy (p. 271)
• Viewing an RDS Proxy (p. 274)

**Limitations for RDS Proxy**

The following limitations apply to RDS Proxy:

• RDS Proxy is available only in certain AWS Regions only. For more information, see Amazon RDS Proxy. You can have up to 20 proxies for each AWS account ID. If your application requires more proxies, you can request additional proxies by opening a ticket with the AWS Support organization.

• Each proxy can have up to 200 associated Secrets Manager secrets. Thus, each proxy can connect to with up to 200 different user accounts at any given time.

• In an Aurora cluster, all of the connections in the connection pool are handled by the Aurora writer instance. To perform load balancing for read-intensive workloads, you still use the reader endpoint directly for the Aurora cluster.

The same consideration applies for RDS DB instances in replication configurations. You can associate a proxy only with the writer DB instance, not a read replica.

• You can't use RDS Proxy with Aurora Serverless clusters.

• You can't use RDS Proxy with Aurora clusters that are part of an Aurora global database.

• Your RDS Proxy must be in the same VPC as the database. The proxy can't be publicly accessible, although the database can be.

• You can't use RDS Proxy with a VPC that has dedicated tenancy.

• If you use RDS Proxy with an RDS DB instance or Aurora DB cluster that has IAM authentication enabled, make sure that all users who connect through a proxy authenticate through user names and passwords. See Setting up AWS Identity and Access Management (IAM) policies (p. 269) for details about IAM support in RDS Proxy.

• You can't use RDS Proxy with custom DNS.

• RDS Proxy is available for the MySQL and PostgreSQL engine families.

• Each proxy can be associated with a single target DB instance or cluster. However, you can associate multiple proxies with the same DB instance or cluster.

The following RDS Proxy prerequisites and limitations apply to MySQL:

• For RDS MySQL, RDS Proxy supports MySQL 5.6 and 5.7. For Aurora MySQL, RDS Proxy supports version 1 (compatible with MySQL 5.6) and version 2 (compatible with MySQL 5.7).

• Currently, all proxies listen on port 3306 for MySQL. The proxies still connect to your database using the port that you specified in the database settings.

• You can't use RDS Proxy with RDS MySQL 8.0.

• You can't use RDS Proxy with self-managed MySQL databases in EC2 instances.

• Proxies don't support MySQL compressed mode. For example, they don't support the compression used by the --compress or -c options of the mysql command.

• Some SQL statements and functions can change the connection state without causing pinning. For the most current pinning behavior, see Avoiding pinning (p. 283).

The following RDS Proxy prerequisites and limitations apply to PostgreSQL:

• For RDS PostgreSQL, RDS Proxy supports version 10.10 and higher minor versions, and version 11.5 and higher minor versions. For Aurora PostgreSQL, RDS Proxy supports version 10.11 and higher minor versions, and 11.6 and higher minor versions.

• Currently, all proxies listen on port 5432 for PostgreSQL.
• Query cancellation isn't supported for PostgreSQL.
• The results of the PostgreSQL function `lastval()` aren't always accurate. As a work-around, use the `INSERT` statement with the `RETURNING` clause.

Identifying DB instances, clusters, and applications to use with RDS Proxy

You can determine which of your DB instances, clusters, and applications might benefit the most from using RDS Proxy. To do so, consider these factors:

• RDS Proxy is highly available and deployed over multiple Availability Zones (AZs). To ensure overall high availability for your database, deploy your Amazon RDS DB instance or Aurora cluster in a Multi-AZ configuration.
• Any DB instance or cluster that encounters “too many connections” errors is a good candidate for associating with a proxy. The proxy enables applications to open many client connections, while the proxy manages a smaller number of long-lived connections to the DB instance or cluster.
• For DB instances or clusters that use smaller AWS instance classes, such as T2 or T3, using a proxy can help avoid out-of-memory conditions. It can also help reduce the CPU overhead for establishing connections. These conditions can occur when dealing with large numbers of connections.
• You can monitor certain Amazon CloudWatch metrics to determine whether a DB instance or cluster is approaching certain types of limit. These limits are for the number of connections and the memory associated with connection management. You can also monitor certain CloudWatch metrics to determine whether a DB instance or cluster is handling many short-lived connections. Opening and closing such connections can impose performance overhead on your database. For information about the metrics to monitor, see Monitoring RDS Proxy using Amazon CloudWatch (p. 285).
• AWS Lambda functions can also be good candidates for using a proxy. These functions make frequent short database connections that benefit from connection pooling offered by RDS Proxy. You can take advantage of any IAM authentication you already have for Lambda functions, instead of managing database credentials in your Lambda application code.
• Applications that use languages and frameworks such as PHP and Ruby on Rails are typically good candidates for using a proxy. Such applications typically open and close large numbers of database connections, and don't have built-in connection pooling mechanisms.
• Applications that keep a large number of connections open for long periods are typically good candidates for using a proxy. Applications in industries such as software as a service (SaaS) or ecommerce often minimize the latency for database requests by leaving connections open. With RDS Proxy, an application can keep more connections open than it can when connecting directly to the DB instance or cluster.
• You might not have adopted IAM authentication and Secrets Manager due to the complexity of setting up such authentication for all DB instances and clusters. If so, you can leave the existing authentication methods in place and delegate the authentication to a proxy. The proxy can enforce the authentication policies for client connections for particular applications. You can take advantage of any IAM authentication you already have for Lambda functions, instead of managing database credentials in your Lambda application code.

Setting up network prerequisites

Using RDS Proxy requires you to have a set of networking resources in place. These include a virtual private cloud (VPC), two or more subnets, an Amazon EC2 instance within the same VPC, and an internet gateway. If you've successfully connected to any RDS DB instances or Aurora DB clusters, you already have the required network resources.

If you're just getting started with RDS or Aurora, you can learn the basics of connecting to a database by following the procedures in Setting up your environment for Amazon Aurora (p. 73). You can also follow the tutorial in Getting started with Amazon Aurora (p. 78).
The following Linux example shows AWS CLI commands that examine the VPCs and subnets owned by your AWS account. In particular, you pass subnet IDs as parameters when you create a proxy using the CLI.

```bash
aws ec2 describe-vpcs
aws ec2 describe-internet-gateways
aws ec2 describe-subnets --query '*[].[VpcId,SubnetId]' --output text | sort
```

The following Linux example shows AWS CLI commands to determine the subnet IDs corresponding to a specific Aurora DB cluster or RDS DB instance. For an Aurora cluster, first you find the ID for one of the associated DB instances. You can extract the subnet IDs used by that DB instance by examining the nested fields within the DBSubnetGroup and Subnets attributes in the describe output for the DB instance. You specify some or all of those subnet IDs when setting up a proxy for that database server.

```bash
$ # Optional first step, only needed if you're starting from an Aurora cluster. Find the ID of any DB instance in the cluster.
$ aws rds describe-db-clusters --db-cluster-id my_cluster_id --query '*[].[DBClusterMembers][0][0][*.DBInstanceIdentifier]' --output text
  my_instance_id
  instance_id_2
  instance_id_3
  ...

$ # From the DB instance, trace through the DBSubnetGroup and Subnets to find the subnet IDs.
$ aws rds describe-db-instances --db-instance-id my_instance_id --query '*[].[DBSubnetGroup][0][0][Subnets][0][*.SubnetIdentifier]' --output text
  subnet_id_1
  subnet_id_2
  subnet_id_3
  ...

As an alternative, you can first find the VPC ID for the DB instance. Then you can examine the VPC to find its subnets. The following Linux example shows how.

```bash
$ # From the DB instance, find the VPC.
$ aws rds describe-db-instances --db-instance-id my_instance_id --query '*[].[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
```

**Setting up database credentials in AWS Secrets Manager**

For each proxy that you create, you first use the Secrets Manager service to store sets of user name and password credentials. You create a separate Secrets Manager secret for each database user account that the proxy connects to on whichever RDS DB instances or Aurora DB clusters that you associate with the proxy. To do this, you can use the setting `Credentials for`
other database. Credentials for RDS database, or Other type of secrets. Fill in the appropriate values for the User name and Password fields, and placeholder values for any other required fields. The proxy ignores other fields such as Host and Port if they're present in the secret. Those details are automatically supplied by the proxy.

You can also choose Other type of secrets. In this case, you create the secret with keys named username and password.

Because the secrets used by your proxy aren’t tied to a specific database server, you can reuse a secret across multiple proxies if you use the same credentials across multiple database servers. For example, you might use the same credentials across a group of development and test servers.

To connect through the proxy as a specific user, make sure that the password associated with a secret matches the database password for that user. If there's a mismatch, you can update the associated secret in Secrets Manager. In this case, you can still connect to other accounts where the secret credentials and the database passwords do match.

When you create a proxy through the AWS CLI or RDS API, you specify the Amazon Resource Names (ARNs) of the corresponding secrets for all the DB user accounts that the proxy can access. In the AWS Management Console, you choose the secrets by their descriptive names.

For instructions about creating secrets in Secrets Manager, see the Creating a secret page in the Secrets Manager documentation. Use one of the following techniques. For instructions about creating secrets in Secrets Manager, see Creating a secret in the AWS Secrets Manager User Guide. Use one of the following techniques:

- Use Secrets Manager in the console.
- To use the CLI to create a Secrets Manager secret for use with RDS Proxy, use a command such as the following.

```bash
aws secretsmanager create-secret
   --name "secret_name"
   --description "secret_description"
   --region region_name
   --secret-string '\{"username":"db_user","password":"db_user_password"\}'
```

For example, the following commands create Secrets Manager secrets for two database users, one named admin and the other named app-user.

```bash
aws secretsmanager create-secret \   --name admin_secret_name --description "db admin user" \   --secret-string '\{"username":"admin","password":"choose_your_own_password"\}'
aws secretsmanager create-secret \   --name proxy_secret_name --description "application user" \   --secret-string '\{"username":"app-user","password":"choose_your_own_password"\}'
```

To see the secrets owned by your AWS account, use a command such as the following.

```bash
aws secretsmanager list-secrets
```

When you create a proxy using the CLI, you pass the Amazon resource names (ARNs) of one or more secrets to the --auth parameter. The following Linux example shows how to prepare a report with only the name and ARN of each secret owned by your AWS account. This example uses the --output table parameter that is available in AWS CLI version 2. If you are using AWS CLI version 1, use --output text instead.
aws secretsmanager list-secrets --query '*[].[Name,ARN]' --output table

To verify that you stored the correct credentials and in the right format in a secret, use a command such as the following. Substitute the short name or the ARN of the secret for `your_secret_name`.

```
aws secretsmanager get-secret-value --secret-id your_secret_name
```

The output should include a line displaying a JSON-encoded value like the following.

```
"SecretString": "{"username":"your_username","password":"your_password"}"
```

### Setting up AWS Identity and Access Management (IAM) policies

After you create the secrets in Secrets Manager, you create an IAM policy that can access those secrets. For general information about using IAM with RDS and Aurora, see Identity and access management in Amazon Aurora (p. 1222).

**Tip**
The following procedure applies if you use the IAM console. If you use the AWS Management Console for RDS, RDS can create the IAM policy for you automatically. In that case, you can skip the following procedure.

**To create an IAM policy that accesses your Secrets Manager secrets for use with your proxy**

1. Sign in to the IAM console. Follow the **Create role** process, as described in **Creating IAM roles**. Include the **Add Role to Database** step.
2. For the new role, perform the **Add inline policy** step. Use the same general procedures as in **Editing IAM policies**. Paste the following JSON into the JSON text box. Substitute your own account ID. Substitute your AWS Region for `us-east-2`. Substitute the Amazon Resource Names (ARNs) for the secrets that you created. For the `kms:Decrypt` action, substitute the ARN of the default AWS KMS customer master key (CMK) or your own AWS KMS CMK, depending on which one you used to encrypt the Secrets Manager secrets.

```json
{  
  "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",  
      "Condition": {  
        "StringEquals": {  
          "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"  
        }  
      }  
    }  
  ]  
}
```
3. Edit the trust policy for this IAM role. Paste the following JSON into the JSON text box.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "rds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

The following commands perform the same operation through the AWS CLI.

```
PREFIX=choose_an_identifier
aws iam create-role --role-name choose_role_name \  
  --assume-role-policy-document '{"Version":"2012-10-17","Statement": [
  {"Effect":"Allow","Principal":{"Service":
  ["rds.amazonaws.com"],"Action":"sts:AssumeRole"}]}'
aws iam put-role-policy --role-name same_role_name_as_previous 
  --policy-name $PREFIX-secret-reader-policy --policy-document "
  same_json_as_in_previous_example"
aws kms create-key --description "$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_ARNA","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",
```
Creating an RDS Proxy

To manage connections for a specified set of DB instances, you can create a proxy. You can associate a proxy with an RDS MySQL DB instance, PostgreSQL DB instance, or an Aurora DB cluster.

AWS Management Console

To create a proxy

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Proxies.
3. Choose Create proxy.
4. Choose all the settings for your proxy.

For Proxy configuration, provide information for the following:

- **Proxy identifier.** Specify a name of your choosing, unique within your AWS account ID and current AWS Region.
- **Engine compatibility.** Choose either MySQL or POSTGRESQL.
- **Require Transport Layer Security.** Choose this setting if you want the proxy to enforce TLS/SSL for all client connections. When you use an encrypted or unencrypted connection to a proxy, the proxy uses the same encryption setting when it makes a connection to the underlying database.
- **Idle client connection timeout.** Choose a time period that a client connection can be idle before the proxy can close it. The default is 1,800 seconds (30 minutes). A client connection is considered idle when the application doesn't submit a new request within the specified time after the previous request completed. The underlying database connection stays open and is returned to the connection pool. Thus, it's available to be reused for new client connections.

Consider lowering the idle client connection timeout if you want the proxy to proactively remove stale connections. If your workload is spiking, consider raising the idle client connection timeout to save the cost of establishing connections.

For Target group configuration, provide information for the following:

- **Database.** Choose one RDS DB instance or Aurora DB cluster to access through this proxy. The list only includes DB instances and clusters with compatible database engines, engine versions, and other settings. If the list is empty, create a new DB instance or cluster that's compatible with RDS Proxy. To do so, follow the procedure in Creating an Amazon Aurora DB cluster (p. 118). Then try creating the proxy again.
• **Connection pool maximum connections.** Specify a value from 1 through 100. This setting represents the percentage of the `max_connections` value that RDS Proxy can use for its connections. If you only intend to use one proxy with this DB instance or cluster, you can set this value to 100. For details about how RDS Proxy uses this setting, see [Controlling connection limits and timeouts](p. 282).

• **Session pinning filters.** (Optional) This is an advanced setting, for troubleshooting performance issues with particular applications. Currently, the only choice is `EXCLUDE_VARIABLE_SETS`. Choose a filter only if both of following are true: Your application isn't reusing connections due to certain kinds of SQL statements, and you can verify that reusing connections with those SQL statements doesn't affect application correctness. For more information, see [Avoiding pinning](p. 283).

• **Connection borrow timeout.** In some cases, you might expect the proxy to sometimes use all available database connections. In such cases, you can specify how long the proxy waits for a database connection to become available before returning a timeout error. You can specify a period up to a maximum of five minutes. This setting only applies when the proxy has the maximum number of connections open and all connections are already in use.

For **Connectivity**, provide information for the following:

• **Secrets Manager ARNs.** Choose at least one Secrets Manager secret that contains DB user credentials for the RDS DB instance or Aurora DB cluster that you intend to access with this proxy.

• **IAM role.** Choose an IAM role that has permission to access the Secrets Manager secrets that you chose earlier. You can also choose for the AWS Management Console to create a new IAM role for you and use that.

• **IAM Authentication.** Choose whether to require or disallow IAM authentication for connections to your proxy. The choice of IAM authentication or native database authentication applies to all DB users that access this proxy.

• **Subnets.** This field is prepopulated with all the subnets associated with your VPC. You can remove any subnets that you don't need for this proxy. You must leave at least two subnets.

Provide additional connectivity configuration:

• **VPC security group.** Choose an existing VPC security group. You can also choose for the AWS Management Console to create a new security group for you and use that.

  **Note**
  
  This security group must allow access to the database the proxy connects to. The same security group is used for ingress from your applications to the proxy, and for egress from the proxy to the database. For example, suppose that you use the same security group for your database and your proxy. In this case, make sure that you specify that resources in that security group can communicate with other resources in the same security group.

(Optional) Provide advanced configuration:

• **Enable enhanced logging.** You can enable this setting to troubleshoot proxy compatibility or performance issues.

  When this setting is enabled, RDS Proxy includes detailed information about SQL statements in its logs. This information helps you to debug issues involving SQL behavior or the performance and scalability of the proxy connections. The debug information includes the text of SQL statements that you submit through the proxy. Thus, only enable this setting when needed for debugging, and only when you have security measures in place to safeguard any sensitive information that appears in the logs.
To minimize overhead associated with your proxy, RDS Proxy automatically turns this setting off 24 hours after you enable it. Enable it temporarily to troubleshoot a specific issue.

5. Choose **Create Proxy**.

**AWS CLI**

To create a proxy, use the AWS CLI command `create-db-proxy`. The **--engine-family** value is case-sensitive.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds create-db-proxy
  --db-proxy-name proxy_name
  --engine-family { MYSQL | POSTGRESQL }
  --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]
```

For Windows:

```bash
aws rds create-db-proxy ^
  --db-proxy-name proxy_name ^
  --engine-family { MYSQL | POSTGRESQL } ^
  --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]
```

**Tip**

If you don't already know the subnet IDs to use for the **--vpc-subnet-ids** parameter, see [Setting up network prerequisites (p. 266)](#) for examples of how to find the subnet IDs that you can use.

To create the required information and associations for the proxy, you also use the `register-db-proxy-targets` command. Specify the target group name `default`. RDS Proxy automatically creates a target group with this name when you create each proxy.

```bash
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), or
  [--db-cluster-endpoint endpoint_name] # rds db cluster endpoint (all instances)
```
RDS API

To create an RDS proxy, call the Amazon RDS API operation `CreateDBProxy`. You pass a parameter with the `AuthConfig` data structure.

RDS Proxy automatically creates a target group named `default` when you create each proxy. You associate an RDS DB instance or Aurora DB cluster with the target group by calling the function `RegisterDBProxyTargets`.

Viewing an RDS Proxy

After you create one or more RDS proxies, you can view them all to examine their configuration details and choose which ones to modify, delete, and so on.

Any database applications that use the proxy require the proxy endpoint to use in the connection string.

AWS Management Console

To view your proxy

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region in which you created the RDS Proxy.
3. In the navigation pane, choose `Proxies`.
4. Choose the name of an RDS proxy to display its details.
5. On the details page, the `Target groups` section shows how the proxy is associated with a specific RDS DB instance or Aurora DB cluster. You can follow the link to the `default` target group page to see more details about the association between the proxy and the database. This page is where you see settings that you specified when creating the proxy, such as maximum connection percentage, connection borrow timeout, engine compatibility, and session pinning filters.

CLI

To view your proxy using the CLI, use the `describe-db-proxies` command. By default, it displays all proxies owned by your AWS account. To see details for a single proxy, specify its name with the `--db-proxy-name` parameter.

```
aws rds describe-db-proxies [--db-proxy-name proxy_name]
```

To view the other information associated with the proxy, use the following commands.

```
aws rds describe-db-proxy-target-groups --db-proxy-name proxy_name
aws rds describe-db-proxy-targets --db-proxy-name proxy_name
```

Use the following sequence of commands to see more detail about the things that are associated with the proxy:

1. To get a list of proxies, run `describe-db-proxies`.
2. To show connection parameters such as the maximum percentage of connections that the proxy can use, run `describe-db-proxy-target-groups --db-proxy-name` and use the name of the proxy as the parameter value.
3. To see the details of the RDS DB instance or Aurora DB cluster associated with the returned target group, run `describe-db-proxy-targets`.

**RDS API**

To view your proxies using the RDS API, use the `DescribeDBProxies` operation. It returns values of the `DBProxy` data type.

To see details of the connection settings for the proxy, use the proxy identifiers from this return value with the `DescribeDBProxyTargetGroups` operation. It returns values of the `DBProxyTargetGroup` data type.

To see the RDS instance or Aurora DB cluster associated with the proxy, use the `DescribeDBProxyTargets` operation. It returns values of the `DBProxyTarget` data type.

**Connecting to a database through RDS Proxy**

You connect to an RDS DB instance or Aurora DB cluster through a proxy in generally the same way as you connect directly to the database. The main difference is that you specify the proxy endpoint instead of the instance or cluster endpoint. For an Aurora DB cluster, all proxy connections have read/write capability and use the writer instance. If you use the reader endpoint for read-only connections, you continue using the reader endpoint the same way.

**Topics**

- Connecting to a proxy using native authentication (p. 275)
- Connecting to a proxy using IAM authentication (p. 276)
- Considerations for connecting to a proxy with PostgreSQL (p. 276)

**Connecting to a proxy using native authentication**

Use the following basic steps to connect to a proxy using native authentication:

1. Find the proxy endpoint. In the AWS Management Console, you can find the endpoint on the details page for the corresponding proxy. With the AWS CLI, you can use the `describe-db-proxies` command. The following example shows how.

```bash
# Add `--output text` to get output as a simple tab-separated list.
# aws rds describe-db-proxies --query '[]
[  
  {  
    "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"  
  }
]
```

275
2. Specify that endpoint as the host parameter in the connection string for your client application. For example, specify the proxy endpoint as the value for the `mysql -h` option or `psql -h` option.

3. Supply the same database user name and password as you usually do.

### Connecting to a proxy using IAM authentication

When you use IAM authentication with RDS Proxy, set up your database users to authenticate with regular user names and passwords. The IAM authentication applies to RDS Proxy retrieving the user name and password credentials from Secrets Manager. The connection from RDS Proxy to the underlying database doesn't go through IAM.

To connect to RDS Proxy using IAM authentication, follow the same general procedure as for connecting to an RDS DB instance or Aurora cluster using IAM authentication. For general information about using IAM with RDS and Aurora, see Security in Amazon Aurora (p. 1205).

The major differences in IAM usage for RDS Proxy include the following:

- You don't configure each individual database user with an authorization plugin. The database users still have regular user names and passwords within the database. You set up Secrets Manager secrets containing these user names and passwords, and authorize RDS Proxy to retrieve the credentials from Secrets Manager.

  **Important**
  
  The IAM authentication applies to the connection between your client program and the proxy. The proxy then authenticates to the database using the user name and password credentials retrieved from Secrets Manager. When you use IAM for the connection to a proxy, make sure that the underlying RDS DB instance or Aurora DB cluster doesn't have IAM enabled.

- Instead of the instance, cluster, or reader endpoint, you specify the proxy endpoint. For details about the proxy endpoint, see Connecting to your DB cluster using IAM authentication (p. 1245).

- In the direct DB IAM auth case, you selectively pick database users and configure them to be identified with a special auth plugin. You can then connect to those users using IAM auth.

  In the proxy use case, you need to provide the proxy with Secrets that contain some user's username and password (native auth). You then connect to the proxy using IAM auth (by generating an auth token with the proxy endpoint, not the database endpoint) and using a username which matches one of the usernames for the secrets you previously provided.

- Make sure that you use Transport Layer Security (TLS) / Secure Sockets Layer (SSL) when connecting to a proxy using IAM authentication.

You can grant a specific user access to the proxy by modifying the IAM policy. An example follows.

```
```

### Considerations for connecting to a proxy with PostgreSQL

For PostgreSQL, when a client starts a connection to a PostgreSQL database, it sends a startup message that includes pairs of parameter name and value strings. For details, see the `StartupMessage` in the PostgreSQL documentation.

When connecting through an RDS proxy, the startup message can include the following currently recognized parameters:

- `user`
• `database`
  • `replication`

The startup message can also include the following additional runtime parameters:

• `application_name`
• `client_encoding`
• `DateStyle`
• `TimeZone`
• `extra_float_digits`

For more information about PostgreSQL messaging, see the Frontend/Backend protocol in the PostgreSQL documentation.

For PostgreSQL, if you use JDBC we recommend the following to avoid pinning:

• Set the JDBC connection parameter `assumeMinServerVersion` to at least 9.0 to avoid pinning. Doing this prevents the JDBC driver from performing an extra round trip during connection startup when it runs `SET extra_float_digits = 3`.

• Set the JDBC connection parameter `ApplicationName` to `any/your-application-name` to avoid pinning. Doing this prevents the JDBC driver from performing an extra round trip during connection startup when it runs `SET application_name = "PostgreSQL JDBC Driver"`. Note the JDBC parameter is `ApplicationName` but the PostgreSQL StartupMessage parameter is `application_name`.

• Set the JDBC connection parameter `preferQueryMode` to `extendedForPrepared` to avoid pinning. The `extendedForPrepared` ensures that the extended mode is used only for prepared statements.

The default for the `preferQueryMode` parameter is `extended`, which uses the extended mode for all queries. The extended mode uses a series of `Prepare`, `Bind`, `Execute`, and `Sync` requests and corresponding responses. This type of series causes connection pinning in an RDS proxy.

For more information, see Avoiding pinning (p. 283). For more information about connecting using JDBC, see Connecting to the database in the PostgreSQL documentation.

Managing an RDS Proxy

Following, you can find an explanation of how to manage RDS proxy operation and configuration. These procedures help your application make the most efficient use of database connections and achieve maximum connection reuse. The more that you can take advantage of connection reuse, the more CPU and memory overhead that you can save. This in turn reduces latency for your application and enables the database to devote more of its resources to processing application requests.

**Topics**

• Modifying an RDS Proxy (p. 278)
• Adding a new database user (p. 282)
• Changing the password for a database user (p. 282)
• Controlling connection limits and timeouts (p. 282)
• Managing and monitoring connection pooling (p. 282)
• Avoiding pinning (p. 283)
• Deleting an RDS Proxy (p. 285)
Modifying an RDS Proxy

You can change certain settings associated with a proxy after you create the proxy. You do so by modifying the proxy itself, its associated target group, or both. Each proxy has an associated target group.

AWS Management Console

To modify the settings for a proxy

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Proxies.
3. In the list of proxies, choose the proxy whose settings you want to modify or go to its details page.
4. For Actions, choose Modify.
5. Enter or choose the properties to modify. You can do the following:
   - Rename the proxy by entering a new identifier.
   - Turn the requirement for Transport layer Security (TLS) on or off.
   - Enter a time period for the idle connection timeout.
   - Add or remove Secrets Manager secrets. These secrets correspond to database user names and passwords.
   - Change the IAM role used to retrieve the secrets from Secrets Manager.
   - Require or disallow IAM authentication for connections to the proxy.
   - Add or remove VPC subnets for the proxy to use.
   - Add or remove VPC security groups for the proxy to use.
   - Enable or disable enhanced logging.
6. Choose Modify.

If you didn't find the settings listed that you want to change, use the following procedure to update the target group for the proxy. The target group associated with a proxy controls the settings related to the physical database connections. Each proxy has one associated target group named default, which is created automatically along with the proxy.

You can only modify the target group from the proxy details page, not from the list on the Proxies page.

To modify the settings for a proxy target group

1. On the Proxies page, go to the details page for a proxy.
2. For Target groups, choose the default link. Currently, all proxies have a single target group named default.
3. On the details page for the default target group, choose Modify.
4. Choose new settings for the properties that you can modify:
   - Choose a different RDS DB instance or Aurora cluster.
   - Adjust what percentage of the maximum available connections the proxy can use.
   - Choose a session pinning filter. Doing this can help reduce performance issues due to insufficient transaction-level reuse for connections. Using this setting requires understanding of application behavior and the circumstances under which RDS Proxy pins a session to a database connection.
   - Adjust the connection borrow timeout interval. This setting applies when the maximum number of connections is already being used for the proxy. The setting determines how long the proxy waits for a connection to become available before returning a timeout error.
You can't change certain properties, such as the target group identifier and the database engine.

5. Choose **Modify target group**.

**AWS CLI**

To modify a proxy using the AWS CLI, use the commands `modify-db-proxy`, `modify-db-proxy-target-group`, `deregister-db-proxy-targets`, and `register-db-proxy-targets`.

With the `modify-db-proxy` command, you can change properties such as the following:

- The set of Secrets Manager secrets used by the proxy.
- Whether TLS is required.
- The idle client timeout.
- Whether to log additional information from SQL statements for debugging.
- The IAM role used to retrieve Secrets Manager secrets.
- The security groups used by the proxy.

The following example shows how to rename an existing proxy.

```bash
aws rds modify-db-proxy --db-proxy-name the-proxy --new-db-proxy-name the_new_name
```

To modify connection-related settings or rename the target group, use the `modify-db-proxy-target-group` command. Currently, all proxies have a single target group named `default`. When working with this target group, you specify the name of the proxy and `default` for the name of the target group.

The following example shows how to first check the `MaxConnectionsPercent` setting for a proxy and then change it, using the target group.

```bash
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
}

With the `deregister-db-proxy-targets` and `register-db-proxy-targets` commands, you change which RDS DB instance or Aurora DB cluster the proxy is associated with through its target group. Currently, each proxy can connect to one RDS DB instance or Aurora DB cluster. The target group tracks the connection details for all the RDS DB instances in a Multi-AZ configuration, or all the DB instances in an Aurora cluster.

The following example starts with a proxy that is associated with an Aurora MySQL cluster named `cluster-56-2020-02-25-1399`. The example shows how to change the proxy so that it can connect to a different cluster named `provisioned-cluster`.

When you work with an RDS DB instance, you specify the `--db-instance-identifier` option. When you work with an Aurora DB cluster, you specify the `--db-cluster-identifier` option instead.

The following example modifies an Aurora MySQL proxy. An Aurora PostgreSQL proxy has 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"
    }
  ]
}
```

280
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

To modify a proxy using the RDS API, you use the operations ModifyDBProxy, ModifyDBProxyTargetGroup, DeregisterDBProxyTargets, and RegisterDBProxyTargets operations.

With ModifyDBProxy, you can change properties such as the following:

- The set of Secrets Manager secrets used by the proxy.
- Whether TLS is required.
- The idle client timeout.
- Whether to log additional information from SQL statements for debugging.
- The IAM role used to retrieve Secrets Manager secrets.
- The security groups used by the proxy.

With ModifyDBProxyTargetGroup, you can modify connection-related settings or rename the target group. Currently, all proxies have a single target group named default. When working with this target group, you specify the name of the proxy and default for the name of the target group.

With DeregisterDBProxyTargets and RegisterDBProxyTargets, you change which RDS DB instance or Aurora DB cluster the proxy is associated with through its target group. Currently, each proxy can connect to one RDS DB instance or Aurora DB cluster. The target group tracks the connection details for all the RDS DB instances in a Multi-AZ configuration, or all the DB instances in an Aurora cluster.
Adding a new database user

In some cases, you might add a new database user to an RDS DB instance or Aurora cluster that's associated with a proxy. If so, add or repurpose a Secrets Manager secret to store the credentials for that user. To do this, choose one of the following options:

- Create a new Secrets Manager secret, using the procedure described in Setting up database credentials in AWS Secrets Manager (p. 267).
- Update the IAM role to give RDS Proxy access to the new Secrets Manager secret. To do so, update the resources section of the IAM role policy.
- If the new user takes the place of an existing one, update the credentials stored in the proxy's Secrets Manager secret for the existing user.

Changing the password for a database user

In some cases, you might change the password for a database user in an RDS DB instance or Aurora cluster that's associated with a proxy. If so, update the corresponding Secrets Manager secret with the new password.

Controlling connection limits and timeouts

RDS Proxy uses the `max_connections` setting for your RDS DB instance or Aurora DB cluster. This setting represents the overall upper limit on the connections that the proxy can open at any one time. In Aurora clusters and RDS Multi-AZ configurations, the `max_connections` value that the proxy uses is the one for the Aurora primary instance or the RDS writer instance.

To set this value for your RDS DB instance or Aurora DB cluster, follow the procedures in Working with DB parameter groups and DB cluster parameter groups (p. 298). These procedures demonstrate how to associate a parameter group with your database and edit the `max_connections` value in the parameter group.

The proxy setting for maximum connections represents a percentage of the `max_connections` value for the database that's associated with the proxy. If you have multiple applications all using the same database, you can effectively divide their connection quotas by using a proxy for each application with a specific percentage of `max_connections`. If you do so, ensure that the percentages add up to 100 or less for all proxies associated with the same database.

RDS Proxy periodically disconnects idle connections and returns them to the connection pool. You can adjust this timeout interval. Doing so helps your applications to deal with stale resources, especially if the application mistakenly leaves a connection open while holding important database resources.

Managing and monitoring connection pooling

As described in Connection pooling (p. 262), connection pooling is a crucial RDS Proxy feature. Following, you can learn how to make the most efficient use of connection pooling and transaction-level connection reuse (multiplexing).

Because the connection pool is managed by RDS Proxy, you can monitor it and adjust connection limits and timeout intervals without changing your application code.

For each proxy, you can specify an upper limit on the number of connections used by the connection pool. You specify the limit as a percentage. This percentage applies to the maximum connections configured in the database. The exact number varies depending on the DB instance size and configuration settings.

For example, suppose that you configured RDS Proxy to use 75 percent of the maximum connections for the database. For MySQL, the maximum value is defined by the `max_connections` configuration parameter. In this case, the other 25 percent of maximum connections remain available to assign to other proxies or for connections that don't go through a proxy. In some cases, the proxy might keep
less than 75 percent of the maximum connections open at a particular time. Those cases might include situations where the database doesn't have many simultaneous connections, or some connections stay idle for long periods.

The overall number of connections available for the connection pool changes as you update the `max_connections` configuration setting that applies to an RDS DB instance or an Aurora cluster.

The proxy doesn't reserve all of these connections in advance. Thus, you can specify a relatively large percentage, and those connections are only opened when the proxy becomes busy enough to need them.

You can choose how long to wait for a connection to become available for use by your application. This setting is represented by the `Connection borrow timeout` option when you create a proxy. This setting specifies how long to wait for a connection to become available in the connection pool before returning a timeout error. It applies when the number of connections is at the maximum, and so no connections are available in the connection pool. It also applies if no writer instance is available because a failover operation is in process. Using this setting, you can set the best wait period for your application without having to change the query timeout in your application code.

### Avoiding pinning

Multiplexing is more efficient when database requests don't rely on state information from previous requests. In that case, RDS Proxy can reuse a connection at the conclusion of each transaction. Examples of such state information include most variables and configuration parameters that you can change through `SET` or `SELECT` statements. SQL transactions on a client connection can multiplex between underlying database connections by default.

Your connections to the proxy can enter a state known as pinning. When a connection is pinned, each later transaction uses the same underlying database connection until the session ends. Other client connections also can't reuse that database connection until the session ends. The session ends when the client connection is dropped.

RDS Proxy automatically pins a client connection to a specific DB connection when it detects a session state change that isn't appropriate for other sessions. Pinning reduces the effectiveness of connection reuse. If all or almost all of your connections experience pinning, consider modifying your application code or workload to reduce the conditions that cause the pinning.

For example, if your application changes a session variable or configuration parameter, later statements can rely on the new variable or parameter to be in effect. Thus, when RDS Proxy processes requests to change session variables or configuration settings, it pins that session to the DB connection. That way, the session state remains in effect for all later transactions in the same session.

This rule doesn't apply to all parameters you can set. RDS Proxy tracks changes to the character set, collation, time zone, autocommit, current database, SQL mode, and `session_track_schema` settings. Thus RDS Proxy doesn't pin the session when you modify these. In this case, RDS Proxy only reuses the connection for other sessions that have the same values for those settings.

Performance tuning for RDS Proxy involves trying to maximize transaction-level connection reuse (multiplexing) by minimizing pinning. You can do so by doing the following:

- Avoid unnecessary database requests that might cause pinning.
- Set variables and configuration settings consistently across all connections. That way, later sessions are more likely to reuse connections that have those particular settings.

However, for PostgreSQL setting a variable leads to session pinning.

- Apply a session pinning filter to the proxy. You can exempt certain kinds of operations from pinning the session if you know that doing so doesn't affect the correct operation of your application.
- See how frequently pinning occurs by monitoring the CloudWatch metric `DatabaseConnectionsCurrentlySessionPinned`. For information about this and other CloudWatch metrics, see Monitoring RDS Proxy using Amazon CloudWatch (p. 285).
• If you use `SET` statements to perform identical initialization for each client connection, you can do so while preserving transaction-level multiplexing. In this case, you move the statements that set up the initial session state into the initialization query used by a proxy. This property is a string containing one or more SQL statements, separated by semicolons.

For example, you can define an initialization query for a proxy that sets certain configuration parameters. Then, RDS Proxy applies those settings whenever it sets up a new connection for that proxy. You can remove the corresponding `SET` statements from your application code, so that they don’t interfere with transaction-level multiplexing.

**Important**

For proxies associated with MySQL databases, don’t set the configuration parameter `sql_auto_is_null` to `true` or a nonzero value in the initialization query. Doing so might cause incorrect application behavior.

The proxy pins the session to the current connection in the following situations where multiplexing might cause unexpected behavior:

• Any statement with a text size greater than 16 KB causes the proxy to pin the session.
• Prepared statements cause the proxy to pin the session. This rule applies whether the prepared statement uses SQL text or the binary protocol.
• Explicit MySQL statements `LOCK TABLE`, `LOCK TABLES`, or `FLUSH TABLES WITH READ LOCK` cause the proxy to pin the session.
• Setting a user variable or a system variable (with some exceptions) causes the proxy to pin the session. If this situation reduces your connection reuse too much, you can choose for `SET` operations not to cause pinning. For information about how to do so by setting the `SessionPinningFilters` property, see Creating an RDS Proxy (p. 271).
• Creating a temporary table causes the proxy to pin the session. That way, the contents of the temporary table are preserved throughout the session regardless of transaction boundaries.
• Calling the MySQL functions `ROW_COUNT`, `FOUND_ROWS`, and `LAST_INSERT_ID` sometimes causes pinning.

The exact circumstances where these functions cause pinning might differ between Aurora MySQL versions that are compatible with MySQL 5.6 and MySQL 5.7.

Calling MySQL stored procedures and stored functions doesn't cause pinning. RDS Proxy doesn't detect any session state changes resulting from such calls. Therefore, make sure that your application doesn't change session state inside stored routines and rely on that session state to persist across transactions. For example, if a stored procedure creates a temporary table that is intended to persist across transactions, that application currently isn't compatible with RDS Proxy.

For PostgreSQL, the following interactions cause pinning:

• Using `SET` commands
• Using the extended query protocol such as by using JDBC default settings
• Creating temporary sequences, tables, or views
• Declaring cursors
• Discarding the session state
• Listening on a notification channel
• Loading a library module such as `auto_explain`
• Manipulating sequences using functions such as `nextval()` and `setval()`
• Interacting with locks using functions such as `pg_advisory_lock()` and `pg_try_advisory_lock()`
Managing connections with RDS Proxy

• Using prepared statements, setting parameters, or resetting a parameter to its default

If you have expert knowledge about your application behavior, you can skip the pinning behavior for certain application statements. To do so, choose the Session pinning filters option when creating the proxy. Currently, you can opt out of session pinning for setting session variables and configuration settings.

For metrics about how often pinning occurs for a proxy, see Monitoring RDS Proxy using Amazon CloudWatch (p. 285).

Deleting an RDS Proxy

You can delete a proxy if you no longer need it. You might delete a proxy because the application that was using it is no longer relevant. Or you might delete a proxy if you take the DB instance or cluster associated with it out of service.

AWS Management Console

To delete a proxy

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Proxies.
3. Choose the proxy to delete from the list.

AWS CLI

To delete a DB proxy, use the AWS CLI command delete-db-proxy. To remove related associations, also use the deregister-db-proxy-targets command.

```bash
aws rds delete-db-proxy --name proxy_name
```

```bash
aws rds deregister-db-proxy-targets
    --db-proxy-name proxy_name
    [--target-group-name target_group_name]       # or
    [--target-ids comma_separated_list]           # or
    [--db-instance-identifiers instance_id]       # or
    [--db-cluster-identifiers cluster_id]
```

RDS API

To delete a DB proxy, call the Amazon RDS API function DeleteDBProxy. To delete related items and associations, you also call the functions DeleteDBProxyTargetGroup and DeregisterDBProxyTargets.

Monitoring RDS Proxy using Amazon CloudWatch

You can monitor RDS Proxy by using Amazon CloudWatch. CloudWatch collects and processes raw data from the proxies into readable, near-real-time metrics. To find these metrics in the CloudWatch console, choose Metrics, then choose RDS, and choose Per-Proxy Metrics. For more information, see Using Amazon CloudWatch metrics in the Amazon CloudWatch User Guide.

Note

RDS publishes these metrics for each underlying Amazon EC2 instance associated with a proxy. A single proxy might be served by more than one EC2 instance. Use CloudWatch statistics to aggregate the values for a proxy across all the associated instances.
Some of these metrics might not be visible until after the first successful connection by a proxy.

All RDS Proxy metrics are in the group `proxy`.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Valid period</th>
<th>CloudWatch dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AvailabilityPercentage</td>
<td>The percentage of time for which the target group was available in the role indicated by the dimension. This metric is reported every minute. The most useful statistic for this metric is <code>Average</code>.</td>
<td>1 minute</td>
<td>ProxyName, TargetGroup, TargetRole</td>
</tr>
<tr>
<td>ClientConnections</td>
<td>The current number of client connections. This metric is reported every minute. The most useful statistic for this metric is <code>Sum</code>.</td>
<td>1 minute</td>
<td>ProxyName</td>
</tr>
<tr>
<td>ClientConnectionsClosed</td>
<td>The number of client connections closed. The most useful statistic for this metric is <code>Sum</code>.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>ClientConnectionsNoTLS</td>
<td>The current number of client connections without Transport Layer Security (TLS). This metric is reported every minute. The most useful statistic for this metric is <code>Sum</code>.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>ClientConnectionsReceived</td>
<td>The number of client connection requests received. The most useful statistic for this metric is <code>Sum</code>.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>ClientConnectionsSetupFailedAuth</td>
<td>The number of client connection attempts that failed due to misconfigured authentication or TLS. The most useful statistic for this metric is <code>Sum</code>.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>ClientConnectionsSetupSucceeded</td>
<td>The number of client connections successfully established with any authentication mechanism with or without TLS.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Valid period</td>
<td>CloudWatch dimensions</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>ClientConnectionsTLS</td>
<td>The current number of client connections with TLS. This metric is reported every minute. The most useful statistic for this metric is Sum.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>DatabaseConnectionRequests</td>
<td>The number of requests to create a database connection. The most useful statistic for this metric is Sum.</td>
<td>1 minute and above</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>DatabaseConnectionRequestsWithTLS</td>
<td>The number of requests to create a database connection with TLS. The most useful statistic for this metric is Sum.</td>
<td>1 minute and above</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>DatabaseConnections</td>
<td>The current number of database connections. This metric is reported every minute. The most useful statistic for this metric is Sum.</td>
<td>1 minute</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>DatabaseConnectionsBorrowLatency</td>
<td>The time in microseconds that it takes for the proxy being monitored to get a database connection. The most useful statistic for this metric is Average.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>DatabaseConnectionsCurrentlyBorrowed</td>
<td>The current number of database connections in the borrow state. This metric is reported every minute. The most useful statistic for this metric is Sum.</td>
<td>1 minute</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Valid period</td>
<td>CloudWatch dimensions</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>DatabaseConnectionsCurrentlyInTransaction</td>
<td>The current number of database connections in a transaction. This metric is reported every minute. The most useful statistic for this metric is Sum.</td>
<td>1 minute</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>DatabaseConnectionsCurrentlySessionPinned</td>
<td>The current number of database connections currently pinned because of operations in client requests that change session state. This metric is reported every minute. The most useful statistic for this metric is Sum.</td>
<td>1 minute</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>DatabaseConnectionsSetupFailed</td>
<td>The number of database connection requests that failed. The most useful statistic for this metric is Sum.</td>
<td>1 minute and above</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>DatabaseConnectionsSetupSucceeded</td>
<td>The number of database connections successfully established with or without TLS. The most useful statistic for this metric is Sum.</td>
<td>1 minute and above</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>DatabaseConnectionsWithTLS</td>
<td>The current number of database connections with TLS. This metric is reported every minute. The most useful statistic for this metric is Sum.</td>
<td>1 minute</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>MaxDatabaseConnectionsAllowed</td>
<td>The maximum number of database connections allowed. This metric is reported every minute. The most useful statistic for this metric is Sum.</td>
<td>1 minute</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
</tbody>
</table>
### Metric Description

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Valid period</th>
<th>CloudWatch dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryDatabaseResponseLatency</td>
<td>The time in microseconds that the database took to respond to the query. The most useful statistic for this metric is Average.</td>
<td>1 minute and above</td>
<td>ProxyName, TargetGroup, Target</td>
</tr>
<tr>
<td>QueryRequests</td>
<td>The number of queries received. A query including multiple statements is counted as one query. The most useful statistic for this metric is Sum.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>QueryRequestsNoTLS</td>
<td>The number of queries received from non-TLS connections. A query including multiple statements is counted as one query. The most useful statistic for this metric is Sum.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>QueryRequestsTLS</td>
<td>The number of queries received from TLS connections. A query including multiple statements is counted as one query. The most useful statistic for this metric is Sum.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
<tr>
<td>QueryResponseLatency</td>
<td>The time in microseconds between getting a query request and the proxy responding to it. The most useful statistic for this metric is Average.</td>
<td>1 minute and above</td>
<td>ProxyName</td>
</tr>
</tbody>
</table>

### Command-line examples for RDS Proxy

To see how combinations of connection commands and SQL statements interact with RDS Proxy, look at the following examples.

**Examples**

- Preserving Connections to a MySQL Database Across a Failover
- Adjusting the max_connections Setting for an Aurora DB Cluster
Example Preserving connections to a MySQL database across a failover

This MySQL example demonstrates how open connections continue working during a failover, for example when you reboot a database or it becomes unavailable due to a problem. This example uses a proxy named `the-proxy` and an Aurora DB cluster with DB instances `instance-8898` and `instance-9814`. When you run the `failover-db-cluster` command from the Linux command line, the writer instance that the proxy is connected to changes to a different DB instance. You can see that the DB instance associated with the proxy changes while the connection remains open.

```
$ 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> select @@aurora_server_id;
+--------------------+
| @@aurora_server_id |
+--------------------+
| instance-9814      |
+--------------------+
1 row in set (0.01 sec)
mysql>

mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com -u admin_user -p
```

# aws rds failover-db-cluster --db-cluster-id 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-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> select @@aurora_server_id;
+--------------------+
| @@aurora_server_id |
+--------------------+
| instance-8898      |
+--------------------+
1 row in set (0.01 sec)
mysql>

mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com -u admin_user -p
```

# aws rds failover-db-cluster --db-cluster-id 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  Adjusting the max_connections setting for an Aurora DB cluster

This example demonstrates how you can adjust the max_connections setting for an Aurora MySQL DB cluster. To do so, you create your own DB cluster parameter group based on the default parameter settings for clusters that are compatible with MySQL 5.6 or 5.7. You specify a value for the max_connections setting, overriding the formula that sets the default value. You associate the DB cluster parameter group with your DB cluster.

```
export REGION=us-east-1
export CLUSTER_PARAM_GROUP=rds-proxy-mysql-56-max-connections-demo
export CLUSTER_NAME=rds-proxy-mysql-56

aws rds create-db-parameter-group --region $REGION \
  --db-parameter-group-family aurora5.6 \
  --db-parameter-group-name $CLUSTER_PARAM_GROUP \
  --description "Aurora MySQL 5.6 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"
```

Troubleshooting for RDS Proxy

Following, you can find troubleshooting ideas for some common RDS Proxy issues and information on CloudWatch logs for RDS Proxy.

Topics
- Common issues and solutions (p. 291)
- Working with CloudWatch logs for RDS Proxy (p. 295)
- Verifying connectivity for a proxy (p. 296)

Common issues and solutions

For possible causes and solutions to some common problems that you might encounter using RDS Proxy, see the following.
You might encounter the following issues while creating a new proxy or connecting to a proxy.

<table>
<thead>
<tr>
<th>Error</th>
<th>Causes or workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>403: The security token included in the request is invalid</td>
<td>Select an existing IAM role instead of choosing to create a new one.</td>
</tr>
</tbody>
</table>

You might encounter the following issues while connecting to a MySQL proxy.

<table>
<thead>
<tr>
<th>Error</th>
<th>Causes or workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR 1040 (HY000): Connections rate limit exceeded</td>
<td>The rate of connection requests from the client to the proxy has exceeded the limit.</td>
</tr>
<tr>
<td>limit_value</td>
<td></td>
</tr>
<tr>
<td>ERROR 1040 (HY000): IAM authentication rate limit exceeded</td>
<td>The number of simultaneous requests with IAM authentication from the client to the proxy has exceeded the limit.</td>
</tr>
<tr>
<td>ERROR 1040 (HY000): Number simultaneous connections exceeded</td>
<td>The number of simultaneous connection requests from the client to the proxy exceeded the limit.</td>
</tr>
<tr>
<td>limit_value</td>
<td></td>
</tr>
<tr>
<td>ERROR 1045 (28000): Access denied for user 'DB_USER'@'%' (using password: YES)</td>
<td>Some possible reasons include the following:</td>
</tr>
<tr>
<td></td>
<td>• The Secrets Manager secret used by the proxy doesn't match the user name and password of an existing database user. Either update the credentials in the Secrets Manager secret, or make sure the database user exists and has the same password as in the secret.</td>
</tr>
<tr>
<td>ERROR 1105 (HY000): Unknown error</td>
<td>An unknown error occurred.</td>
</tr>
<tr>
<td>ERROR 1231 (42000): Variable 'character_set_client' can't be set to the value of value</td>
<td>The value set for the character_set_client parameter is not valid. For example, the value ucs2 is not valid because it can crash the MySQL server.</td>
</tr>
<tr>
<td>ERROR 3159 (HY000): This RDS Proxy requires TLS connections.</td>
<td>You enabled the setting <strong>Require Transport Layer Security</strong> in the proxy but your connection included the parameter <code>ssl-mode=DISABLED</code> in the MySQL client. Do either of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disable the setting <strong>Require Transport Layer Security</strong> for the proxy.</td>
</tr>
<tr>
<td></td>
<td>• Connect to the database using the minimum setting of <code>ssl-mode=REQUIRED</code> in the MySQL client.</td>
</tr>
</tbody>
</table>
You might encounter the following issues while connecting to a PostgreSQL proxy.

<table>
<thead>
<tr>
<th>Error</th>
<th>Causes or workarounds</th>
</tr>
</thead>
</table>
| ERROR 2026 (HY000): SSL connection error: Internal Server Error | The TLS handshake to the proxy failed. Some possible reasons include the following:  
• SSL is required but the server doesn't support it.  
• An internal server error occurred.  
• A bad handshake occurred. |
| ERROR 9501 (HY000): Timed-out waiting to acquire database connection | The proxy timed-out waiting to acquire a database connection. Some possible reasons include the following:  
• The proxy is unable to establish a database connection because the maximum connections have been reached  
• The proxy is unable to establish a database connection because the database is unavailable. |

<table>
<thead>
<tr>
<th>Error</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM authentication is allowed only with SSL connections.</td>
<td>The user tried to connect to the database using IAM authentication with the setting sslmode=disable in the PostgreSQL client.</td>
<td>The user needs to connect to the database using the minimum setting of sslmode=require in the PostgreSQL client. For more information, see the PostgreSQL SSL support documentation.</td>
</tr>
</tbody>
</table>
| This RDS Proxy requires TLS connections. | The user enabled the option **Require Transport Layer Security** but tried to connect with sslmode=disable in the PostgreSQL client. | To fix this error, do one of the following:  
• Disable the proxy's **Require Transport Layer Security** option.  
• Connect to the database using the minimum setting of sslmode=allow in the PostgreSQL client. |
| IAM authentication failed for user **user_name**. Check the IAM token for this user and try again. | This error might be due to the following reasons:  
• The client supplied the incorrect IAM user name.  
• The client supplied an incorrect IAM authorization token for the user.  
• The client is using an IAM policy that does not have the necessary permissions.  
• The client supplied an expired IAM authorization token for the user. | To fix this error, do the following:  
1. Confirm that the provided IAM user exists.  
2. Confirm that the IAM authorization token belongs to the provided IAM user.  
3. Confirm that the IAM policy has adequate permissions for RDS.  
4. Check the validity of the IAM authorization token used. |
<table>
<thead>
<tr>
<th>Error</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>This RDS proxy has no credentials for the role <code>role_name</code>. Check the credentials for this role and try again.</td>
<td>There is no Secrets Manager secret for this role.</td>
<td>Add a Secrets Manager secret for this role.</td>
</tr>
<tr>
<td>RDS supports only IAM or MD5 authentication.</td>
<td>The database client being used to connect to the proxy is using an authentication mechanism not currently supported by the proxy, such as SCRAM-SHA-256.</td>
<td>If you're not using IAM authentication, use the MD5 password authentication only.</td>
</tr>
<tr>
<td>A user name is missing from the connection startup packet. Provide a user name for this connection.</td>
<td>The database client being used to connect to the proxy isn't sending a user name when trying to establish a connection.</td>
<td>Make sure to define a user name when setting up a connection to the proxy using the PostgreSQL client of your choice.</td>
</tr>
<tr>
<td>Feature not supported: RDS Proxy supports only version 3.0 of the PostgreSQL messaging protocol.</td>
<td>The PostgreSQL client used to connect to the proxy uses a protocol older than 3.0.</td>
<td>Use a newer PostgreSQL client that supports the 3.0 messaging protocol. If you're using the PostgreSQL <code>psql</code> CLI, use a version greater than or equal to 7.4.</td>
</tr>
<tr>
<td>Feature not supported: RDS Proxy currently doesn't support streaming replication mode.</td>
<td>The PostgreSQL client used to connect to the proxy is trying to use the streaming replication mode, which isn't currently supported by RDS Proxy.</td>
<td>Turn off the streaming replication mode in the PostgreSQL client being used to connect.</td>
</tr>
<tr>
<td>Feature not supported: RDS Proxy currently doesn't support the option <code>option_name</code>.</td>
<td>Through the startup message, the PostgreSQL client used to connect to the proxy is requesting an option that isn't currently supported by RDS Proxy.</td>
<td>Turn off the option being shown as not supported from the message above in the PostgreSQL client being used to connect.</td>
</tr>
<tr>
<td>The IAM authentication failed because of too many competing requests.</td>
<td>The number of simultaneous requests with IAM authentication from the client to the proxy has exceeded the limit.</td>
<td>Reduce the rate in which connections using IAM authentication from a PostgreSQL client are established.</td>
</tr>
<tr>
<td>The maximum number of client connections to the proxy exceeded <code>number_value</code>.</td>
<td>The number of simultaneous connection requests from the client to the proxy exceeded the limit.</td>
<td>Reduce the number of active connections from PostgreSQL clients to this RDS proxy.</td>
</tr>
<tr>
<td>Rate of connection to proxy exceeded <code>number_value</code>.</td>
<td>The rate of connection requests from the client to the proxy has exceeded the limit.</td>
<td>Reduce the rate in which connections from a PostgreSQL client are established.</td>
</tr>
<tr>
<td>Error</td>
<td>Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>The password that was provided for the role <em>role_name</em> is wrong.</td>
<td>The password for this role doesn't match the Secrets Manager secret.</td>
<td>Check the secret for this role in Secrets Manager to see if the password is the same as what's being used in your PostgreSQL client.</td>
</tr>
<tr>
<td>The IAM authentication failed for the role <em>role_name</em>. Check the IAM token for this role and try again.</td>
<td>There is a problem with the IAM token used for IAM authentication.</td>
<td>Generate a new authentication token and use it in a new connection.</td>
</tr>
<tr>
<td>IAM is allowed only with SSL connections.</td>
<td>A client tried to connect using IAM authentication, but SSL wasn't enabled.</td>
<td>Enable SSL in the PostgreSQL client.</td>
</tr>
<tr>
<td>Unknown error.</td>
<td>An unknown error occurred.</td>
<td>Reach out to AWS Support for us to investigate the issue.</td>
</tr>
</tbody>
</table>
| Timed-out waiting to acquire database connection. | The proxy timed-out waiting to acquire a database connection. Some possible reasons include the following:  
• The proxy can't establish a database connection because the maximum connections have been reached.  
• The proxy can't establish a database connection because the database is unavailable. | Possible solutions are:  
• Check the target of the RDS DB instance or Aurora DB cluster status to see if it's unavailable.  
• Check if there are long-running transactions and/or queries being executed. They can use database connections from the connection pool for a long time. |
| Request returned an error: *database_error*. | The database connection established from the proxy returned an error. | The solution depends on the specific database error. One example is: Request returned an error: database "your-database-name" does not exist. This means the specified database name, or the user name used as a database name (in case a database name hasn't been specified), doesn't exist in the database server. |

**Working with CloudWatch logs for RDS Proxy**

You can find logs of RDS Proxy activity under CloudWatch in the AWS Management Console. Each proxy has an entry in the Log groups page.

**Important**

These logs are intended for human consumption for troubleshooting purposes and not for programmatic access. The format and content of the logs is subject to change.
Verifying connectivity for a proxy

You can use the following commands to verify that all components of the connection mechanism can communicate with the other components.

Examine the proxy itself using the `describe-db-proxies` command. Also examine the associated target group using the `describe-db-proxy-target-groups` command. Check that the details of the targets match the RDS DB instance or Aurora DB cluster that you intend to associate with the proxy. Use commands such as the following.

```
aws rds describe-db-proxies --db-proxy-name $DB_PROXY_NAME
aws rds describe-db-proxy-target-groups --db-proxy-name $DB_PROXY_NAME
```

To confirm that the proxy can connect to the underlying database, examine the targets specified in the target groups using the `describe-db-proxy-targets` command. Use a command such as the following.

```
aws rds describe-db-proxy-targets --db-proxy-name $DB_PROXY_NAME
```

The output of the `describe-db-proxy-targets` command includes a `TargetHealth` field. You can examine the fields `State`, `Reason`, and `Description` inside `TargetHealth` to check if the proxy can communicate with the underlying DB instance.

- A `State` value of `AVAILABLE` indicates that the proxy can connect to the DB instance.
- A `State` value of `UNAVAILABLE` indicates a temporary or permanent connection problem. In this case, examine the `Reason` and `Description` fields. For example, if `Reason` has a value of `PENDING_PROXY_CAPACITY`, try connecting again after the proxy finishes its scaling operation. If `Reason` has a value of `UNREACHABLE`, `CONNECTION_FAILED`, or `AUTH_FAILURE`, use the explanation from the `Description` field to help you diagnose the issue.
- The `State` field might have a value of `REGISTERING` for a brief time before changing to `AVAILABLE` or `UNAVAILABLE`.

If the following Netcat command (`nc`) is successful, you can access the proxy endpoint from the EC2 instance or other system where you're logged in. This command reports failure if you're not in the same VPC as the proxy and the associated database. You might be able to log directly in to the database without being in the same VPC. However, you can't log into the proxy unless you're in the same VPC.

```
nc -zx MySQL_proxy_endpoint 3306
nc -zx PostgreSQL_proxy_endpoint 5432
```

You can use the following commands to make sure that your EC2 instance has the required properties. In particular, the VPC for the EC2 instance must be the same as the VPC for the RDS DB instance or Aurora DB cluster that the proxy connects to.

```
aws ec2 describe-instances --instance-ids your_ec2_instance_id
```

Examine the Secrets Manager secrets used for the proxy.

```
aws secretsmanager list-secrets
aws secretsmanager get-secret-value --secret-id your_secret_id
```

Make sure that the `SecretString` field displayed by `get-secret-value` is encoded as a JSON string that includes `username` and `password` fields. The following example shows the format of the `SecretString` field.
Using RDS Proxy with AWS CloudFormation

You can use RDS Proxy with AWS CloudFormation. Doing so helps you to create groups of related resources, including a proxy that can connect to a newly created Amazon RDS DB instance or Aurora DB cluster. RDS Proxy support in AWS CloudFormation involves two new registry types: `DBProxy` and `DBProxyTargetGroup`.

The following listing shows a sample AWS CloudFormation template for RDS Proxy.

```yaml
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
            InstanceIdentifiers:
                - Fn::ImportValue: DBInstanceName
        DependsOn: DBProxy
```

For more information about the Amazon RDS and Aurora resources that you can create using AWS CloudFormation, see RDS resource type reference.
Working with DB parameter groups and DB cluster parameter groups

You manage your DB engine configuration by associating your DB instances and Aurora DB clusters with parameter groups. Amazon RDS defines parameter groups with default settings that apply to newly created DB instances and Aurora DB clusters.

**Important**
You can define your own parameter groups with customized settings. Then you can modify your DB instances and Aurora clusters to use your own parameter groups.

For information about modifying a DB cluster or DB instance, see Modifying an Amazon Aurora DB cluster (p. 327).

A **DB parameter group** acts as a container for engine configuration values that are applied to one or more DB instances. DB parameter groups apply to DB instances in both Amazon RDS and Aurora. These configuration settings apply to properties that can vary among the DB instances within an Aurora cluster, such as the sizes for memory buffers.

A **DB cluster parameter group** acts as a container for engine configuration values that are applied to every DB instance in an Aurora DB cluster. For example, the Aurora shared storage model requires that every DB instance in an Aurora cluster use the same setting for parameters such as `innodb_file_per_table`. Thus, parameters that affect the physical storage layout are part of the cluster parameter group. The DB cluster parameter group also includes default values for all the instance-level parameters.

If you create a DB instance without specifying a DB parameter group, the DB instance uses a default DB parameter group. Likewise, if you create an Aurora DB cluster without specifying a DB cluster parameter group, the DB cluster uses a default DB cluster parameter group. Each default parameter group contains database engine defaults and Amazon RDS system defaults based on the engine, compute class, and allocated storage of the instance. You can't modify the parameter settings of a default parameter group. Instead, you create your own parameter group where you choose your own parameter settings. Not all DB engine parameters can be changed in a parameter group that you create.

If you want to use your own parameter group, you create a new parameter group and modify the parameters that you want to. You then modify your DB instance or DB cluster to use the new parameter group. If you update parameters within a DB parameter group, the changes apply to all DB instances that are associated with that parameter group. Likewise, if you update parameters within a DB cluster parameter group, the changes apply to all Aurora clusters that are associated with that DB cluster parameter group.

You can copy an existing DB parameter group with the AWS CLI `copy-db-parameter-group` command. You can copy an existing DB cluster parameter group with the AWS CLI `copy-db-cluster-parameter-group` command. Copying a parameter group can be convenient when you want to include most of an existing parameter group's custom parameters and values in a new parameter group.

Here are some important points about working with parameters in a parameter group:

- When you change a dynamic parameter and save the parameter group, the change is applied immediately regardless of the **Apply Immediately** setting. When you change a static parameter and save the DB parameter group, the parameter change takes effect after you manually reboot the DB instance. You can reboot a DB instance using the RDS console or by explicitly calling the `RebootDbInstance` API operation (without failover, if the DB instance is in a Multi-AZ deployment). The requirement to reboot the associated DB instance after a static parameter change helps mitigate the risk of a parameter misconfiguration affecting an API call, such as calling `ModifyDBInstance` to change DB instance class or scale storage.

  If a DB instance isn't using the latest changes to its associated DB parameter group, the AWS Management Console shows the DB parameter group with a status of **pending-reboot**. The **pending-reboot** status is displayed until the DB instance is rebooted.
reboot parameter groups status doesn’t result in an automatic reboot during the next maintenance window. To apply the latest parameter changes to that DB instance, manually reboot the DB instance.

- When you change the DB parameter group associated with a DB instance, you must manually reboot the instance before the DB instance can use the new DB parameter group. For more information about changing the DB parameter group, see Modifying an Amazon Aurora DB cluster (p. 327).

  **Note**
  After you change the DB cluster parameter group associated with a DB cluster, reboot the primary DB instance in the cluster to apply the changes to all of the DB instances in the cluster.

- You can specify the value for a parameter as an integer or as an integer expression built from formulas, variables, functions, and operators. Functions can include a mathematical log expression. For more information, see DB parameter values (p. 318).

- Set any parameters that relate to the character set or collation of your database in your parameter group before creating the DB instance and before you create a database in your DB instance. This ensures that the default database and new databases in your DB instance use the character set and collation values that you specify. If you change character set or collation parameters for your DB instance, the parameter changes are not applied to existing databases.

You can change character set or collation values for an existing database using the `ALTER DATABASE` command, for example:

```sql
ALTER DATABASE database_name CHARACTER SET character_set_name COLLATE collation;
```

- Improperly setting parameters in a parameter group can have unintended adverse effects, including degraded performance and system instability. Always exercise caution when modifying database parameters and back up your data before modifying a parameter group. Try out parameter group setting changes on a test DB instance before applying those parameter group changes to a production DB instance.

- For an Aurora global database, you can specify different configuration settings for the individual Aurora clusters. Make sure that the settings are similar enough to produce consistent behavior if you promote a secondary cluster to be the primary cluster. For example, use the same settings for time zones and character sets across all the clusters of an Aurora global database.

- To determine the supported parameters for your DB engine, you can view the parameters in the DB parameter group and DB cluster parameter group used by the DB cluster. For more information, see Viewing parameter values for a DB parameter group (p. 315) and Viewing parameter values for a DB cluster parameter group (p. 316).

**Topics**

- Amazon Aurora DB cluster and DB instance parameters (p. 300)
- Creating a DB parameter group (p. 301)
- Creating a DB cluster parameter group (p. 302)
- Modifying parameters in a DB parameter group (p. 303)
- Modifying parameters in a DB cluster parameter group (p. 305)
- Resetting parameters in a DB parameter group to their default values (p. 307)
- Resetting parameters in a DB cluster parameter group (p. 309)
- Copying a DB parameter group (p. 310)
- Copying a DB cluster parameter group (p. 312)
- Listing DB parameter groups (p. 313)
- Listing DB cluster parameter groups (p. 314)
- Viewing parameter values for a DB parameter group (p. 315)
Amazon Aurora DB cluster and DB instance parameters

Aurora uses a two-level system of configuration settings, as follows:

- Parameters in a **DB cluster parameter group** apply to every DB instance in a DB cluster. Your data is stored in the Aurora shared storage subsystem. Because of this, all parameters related to physical layout of table data must be the same for all DB instances in an Aurora cluster. Likewise, because Aurora DB instances are connected by replication, all the parameters for replication settings must be identical throughout an Aurora cluster.

- Parameters in a **DB parameter group** apply to a single DB instance in an Aurora DB cluster. These parameters are related to aspects such as memory usage that you can vary across DB instances in the same Aurora cluster. For example, a cluster often contains DB instances with different AWS instance classes.

Every Aurora cluster is associated with a DB cluster parameter group. Each DB instance within the cluster inherits the settings from that DB cluster parameter group, and is associated with a DB parameter group. Aurora assigns default parameter groups when you create a cluster or a new DB instance, based on the specified database engine and version. You can change the parameter groups later to ones that you create, where you can edit the parameter values.

The DB cluster parameter groups also include default values for all the instance-level parameters from the DB parameter group. These defaults are mainly intended for configuring Aurora Serverless clusters, which are only associated with DB cluster parameter groups, not DB parameter groups. You can modify the instance-level parameter settings in the DB cluster parameter group. Then, Aurora applies those settings to each new DB instance that's added to a Serverless cluster. To learn more about configuration settings for Aurora Serverless clusters and which settings you can modify, see [Aurora Serverless v1 and parameter groups](p. 142).

For non-Serverless clusters, any configuration values that you modify in the DB cluster parameter group override default values in the DB parameter group. If you edit the corresponding values in the DB parameter group, those values override the settings from the DB cluster parameter group.

Any DB parameter settings that you modify take precedence over the DB cluster parameter group values, even if you change the configuration parameters back to their default values. You can see which parameters are overridden by using the `describe-db-parameters` AWS CLI command or the `DescribeDBParameters` RDS API. The `Source` field contains the value `user` if you modified that parameter. To reset one or more parameters so that the value from the DB cluster parameter group takes precedence, use the `reset-db-parameter-group` AWS CLI command or the `ResetDBParameterGroup` RDS API operation.

The DB cluster and DB instance parameters available to you in Aurora vary depending on database engine compatibility.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora MySQL</td>
<td>See [Aurora MySQL parameters](p. 848). For Aurora Serverless clusters, see additional details in [Aurora Serverless v1 and parameter groups](p. 142).</td>
</tr>
</tbody>
</table>
Creating a DB parameter group

You can create a new DB parameter group using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To create a DB parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.
3. Choose Create parameter group.
   The Create parameter group window appears.
4. In the Parameter group family list, select a DB parameter group family.
5. In the Type list, select DB Parameter Group.
6. In the Group name box, enter the name of the new DB parameter group.
7. In the Description box, enter a description for the new DB parameter group.
8. Choose Create.

AWS CLI

To create a DB parameter group, use the AWS CLI create-db-parameter-group command. The following example creates a DB parameter group named mydbparametergroup for MySQL version 5.6 with a description of "My new parameter group."

Include the following required parameters:

- --db-parameter-group-name
- --db-parameter-group-family
- --description

To list all of the available parameter group families, use the following command:

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

Note
The output contains duplicates.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-parameter-group \ 
  --db-parameter-group-name mydbparametergroup \ 
```

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora PostgreSQL</td>
<td>See Amazon Aurora PostgreSQL parameters (p. 1137).</td>
</tr>
</tbody>
</table>
Creating a DB cluster parameter group

You can create a new DB cluster parameter group using the AWS Management Console, the AWS CLI, or the RDS API.

**Console**

To create a DB cluster parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.
3. Choose Create parameter group.
4. In the Parameter group family list, select a DB parameter group family
5. In the Type list, select DB Cluster Parameter Group.
6. In the Group name box, enter the name of the new DB cluster parameter group.
7. In the Description box, enter a description for the new DB cluster parameter group.
8. Choose Create.

**AWS CLI**

To create a DB cluster parameter group, use the AWS CLI `create-db-cluster-parameter-group` command. The following example creates a DB cluster parameter group named `mydbclusterparametergroup` for MySQL version 5.6 with a description of "My new cluster parameter group."

Include the following required parameters:
Modifying parameters in a DB parameter group

To list all of the available parameter group families, use the following command:

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

**Note**
The output contains duplicates.

**Example**

For Linux, macOS, or Unix:

```
aws rds create-db-cluster-parameter-group \\n   --db-cluster-parameter-group-name mydbclusterparametergroup \\n   --db-parameter-group-family aurora5.6 \\n   --description "My new cluster parameter group"
```

For Windows:

```
aws rds create-db-cluster-parameter-group ^
   --db-cluster-parameter-group-name mydbclusterparametergroup ^
   --db-parameter-group-family aurora5.6 ^
   --description "My new cluster parameter group"
```

This command produces output similar to the following:

```
DBCLUSTERPARAMETERGROUP mydbclusterparametergroup mysql5.6 My cluster new parameter group
```

**RDS API**

To create a DB cluster parameter group, use the RDS API `CreateDBClusterParameterGroup` action.

Include the following required parameters:

- `DBClusterParameterGroupName`
- `DBParameterGroupFamily`
- `Description`

**Modifying parameters in a DB parameter group**

You can modify parameter values in a customer-created DB parameter group; you can't change the parameter values in a default DB parameter group. Changes to parameters in a customer-created DB parameter group are applied to all DB instances that are associated with the DB parameter group.

Changes to some parameters are applied to the DB instance immediately without a reboot. Changes to other parameters are applied only after the DB instance is rebooted. The RDS console shows the status of the DB parameter group associated with a DB instance on the **Configuration** tab. For example, if the
DB instance isn't using the latest changes to its associated DB parameter group, the RDS console shows the DB parameter group with a status of **pending-reboot**. To apply the latest parameter changes to that DB instance, manually reboot the DB instance.

### Console

**To modify a DB parameter group**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the parameter group that you want to modify.
4. For **Parameter group actions**, choose **Edit**.
5. Change the values of the parameters that you want to modify. You can scroll through the parameters using the arrow keys at the top right of the dialog box.
   
   You can't change values in a default parameter group.
6. Choose **Save changes**.
AWS CLI

To modify a DB parameter group, use the AWS CLI `modify-db-parameter-group` command with the following required parameters:

- `--db-parameter-group-name`
- `--parameters`

The following example modifies the `max_connections` and `max_allowed_packet` values in the DB parameter group named `mydbparametergroup`.

**Example**

For Linux, macOS, or Unix:

```
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"
```

For 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"
```

The command produces output like the following:

```
DBPARAMETERGROUP  mydbparametergroup
```

RDS API

To modify a DB parameter group, use the RDS API `ModifyDBParameterGroup` command with the following required parameters:

- `DBParameterGroupName`
- `Parameters`

Modifying parameters in a DB cluster parameter group

You can modify parameter values in a customer-created DB cluster parameter group. You can't change the parameter values in a default DB cluster parameter group. Changes to parameters in a customer-created DB cluster parameter group are applied to all DB clusters that are associated with the DB cluster parameter group.

Console

To modify a DB cluster parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the parameter group that you want to modify.
4. For **Parameter group actions**, choose **Edit**.
5. Change the values of the parameters you want to modify. You can scroll through the parameters using the arrow keys at the top right of the dialog box.
   
   You can't change values in a default parameter group.
6. Choose **Save changes**.
7. Reboot the primary DB instance in the cluster to apply the changes to all of the DB instances in the cluster.

**AWS CLI**

To modify a DB cluster parameter group, use the AWS CLI `modify-db-cluster-parameter-group` command with the following required parameters:

- `--db-cluster-parameter-group-name`
- `--parameters`

The following example modifies the `server Audit Logging` and `server Audit Logs Upload` values in the DB cluster parameter group named `mydbclusterparametergroup`.

**Example**

For Linux, macOS, or Unix:

```bash
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"
```

For Windows:

```bash
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"
```

The command produces output like the following:

```
DBCLUSTERPARAMETERGROUP  mydbclusterparametergroup
```

**RDS API**

To modify a DB cluster parameter group, use the RDS API `ModifyDBClusterParameterGroup` command with the following required parameters:

- `DBClusterParameterGroupName`
- `Parameters`
Resetting parameters in a DB parameter group to their default values

You can reset parameter values in a customer-created DB parameter group to their default values. Changes to parameters in a customer-created DB parameter group are applied to all DB instances that are associated with the DB parameter group.

When you use the console, you can reset specific parameters to their default values, but you can’t easily reset all of the parameters in the DB parameter group at once. When you use the AWS CLI or RDS API, you can reset specific parameters to their default values, and you can reset all of the parameters in the DB parameter group at once.

Changes to some parameters are applied to the DB instance immediately without a reboot. Changes to other parameters are applied only after the DB instance is rebooted. The RDS console shows the status of the DB parameter group associated with a DB instance on the Configuration tab. For example, if the DB instance isn’t using the latest changes to its associated DB parameter group, the RDS console shows the DB parameter group with a status of pending-reboot. To apply the latest parameter changes to that DB instance, manually reboot the DB instance.
Note
In a default DB parameter group, parameters are always set to their default values.

Console

To reset parameters in a DB parameter group to their default values

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.
3. In the list, choose the parameter group.
4. For Parameter group actions, choose Edit.
5. Choose the parameters that you want to reset to their default values. You can scroll through the parameters using the arrow keys at the top right of the dialog box.
   You can't reset values in a default parameter group.
6. Choose Reset and then confirm by choosing Reset parameters.

AWS CLI

To reset some or all of the parameters in a DB parameter group, use the AWS CLI `reset-db-parameter-group` command with the following required option: `--db-parameter-group-name`.

To reset all of the parameters in the DB parameter group, specify the `--reset-all-parameters` option. To reset specific parameters, specify the `--parameters` option.

The following example resets all of the parameters in the DB parameter group named `mydbparametergroup` to their default values.

Example

For Linux, macOS, or Unix:

```
aws rds reset-db-parameter-group \
   --db-parameter-group-name mydbparametergroup \
   --reset-all-parameters
```

For Windows:

```
aws rds reset-db-parameter-group ^
   --db-parameter-group-name mydbparametergroup ^
   --reset-all-parameters
```

The following example resets the `max_connections` and `max_allowed_packet` options to their default values in the DB parameter group named `mydbparametergroup`.

Example

For Linux, macOS, or Unix:

```
aws rds reset-db-parameter-group \
   --db-parameter-group-name mydbparametergroup \
   --parameters "ParameterName=max_connections,ApplyMethod=immediate" \
   "ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

For Windows:
Resetting parameters in a DB cluster parameter group

You can reset parameters to their default values in a customer-created DB cluster parameter group. Changes to parameters in a customer-created DB cluster parameter group are applied to all DB clusters that are associated with the DB cluster parameter group.

**Note**
In a default DB cluster parameter group, parameters are always set to their default values.

**Console**

**To reset parameters in a DB cluster parameter group to their default values**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose Parameter groups.
3. In the list, choose the parameter group.
4. For Parameter group actions, choose Edit.
5. Choose the parameters that you want to reset to their default values. You can scroll through the parameters using the arrow keys at the top right of the dialog box.

You can't reset values in a default parameter group.

6. Choose Reset and then confirm by choosing Reset parameters.
7. Reboot the primary DB instance in the DB cluster to apply the changes to all of the DB instances in the DB cluster.

**AWS CLI**

To reset parameters in a DB cluster parameter group to their default values, use the AWS CLI `reset-db-cluster-parameter-group` command with the following required option: `--db-cluster-parameter-group-name`.

To reset all of the parameters in the DB cluster parameter group, specify the `--reset-all-parameters` option. To reset specific parameters, specify the `--parameters` option.
The following example resets all of the parameters in the DB parameter group named `mydbparametergroup` to their default values.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds reset-db-cluster-parameter-group \
  --db-cluster-parameter-group-name mydbparametergroup \
  --reset-all-parameters
```

For Windows:

```bash
aws rds reset-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name mydbparametergroup ^
  --reset-all-parameters
```

The following example resets the `server_audit_logging` and `server_audit_logs_upload` to their default values in the DB cluster parameter group named `mydbclusterparametergroup`.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds reset-db-cluster-parameter-group \
  --db-cluster-parameter-group-name mydbclusterparametergroup \
  --parameters "ParameterName=serverAuditLogging,ApplyMethod=immediate" \
  "ParameterName=serverAuditLogsUpload,ApplyMethod=immediate"
```

For Windows:

```bash
aws rds reset-db-cluster-parameter-parameter-group ^
  --db-cluster-parameter-group-name mydbclusterparametergroup ^
  --parameters "ParameterName=serverAuditLogging,ParameterValue=1,ApplyMethod=immediate" ^
  "ParameterName=serverAuditLogsUpload,ParameterValue=1,ApplyMethod=immediate"
```

The command produces output like the following:

```
DBClusterParameterGroupName  mydbclusterparametergroup
```

**RDS API**

To reset parameters in a DB cluster parameter group to their default values, use the RDS API `ResetDBClusterParameterGroup` command with the following required parameter: `DBClusterParameterGroupName`.

To reset all of the parameters in the DB cluster parameter group, set the `ResetAllParameters` parameter to `true`. To reset specific parameters, specify the `Parameters` parameter.

**Copying a DB parameter group**

You can copy custom DB parameter groups that you create. Copying a parameter group is a convenient solution when you have already created a DB parameter group and you want to include most of the
custom parameters and values from that group in a new DB parameter group. You can copy a DB 
parameter group by using the AWS Management Console, the AWS CLI copy-db-parameter-group 
command, or the RDS API CopyDBParameterGroup operation.

After you copy a DB parameter group, wait at least 5 minutes before creating your first DB instance that 
uses that DB parameter group as the default parameter group. Doing this allows Amazon RDS to fully 
complete the copy action before the parameter group is used. This is especially important for parameters 
that are critical when creating the default database for a DB instance. An example is the character set 
for the default database defined by the character_set_database parameter. Use the Parameter 
Groups option of the Amazon RDS console or the describe-db-parameters command to verify that your 
DB parameter group is created.

Note
You can't copy a default parameter group. However, you can create a new parameter group that 
is based on a default parameter group. 
Currently, you can't copy a parameter group to a different AWS Region.

Console

To copy a DB parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at https:// 
console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.
3. In the list, choose the custom parameter group that you want to copy.
4. For Parameter group actions, choose Copy.
5. In New DB parameter group identifier, enter a name for the new parameter group.
6. In Description, enter a description for the new parameter group.
7. Choose Copy.

AWS CLI

To copy a DB parameter group, use the AWS CLI copy-db-parameter-group command with the 
following required options:

• --source-db-parameter-group-identifier
• --target-db-parameter-group-identifier
• --target-db-parameter-group-description

The following example creates a new DB parameter group named mygroup2 that is a copy of the DB 
parameter group mygroup1.

Example

For Linux, macOS, or Unix:

```bash
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"
```

For Windows:

```bash
aws rds copy-db-parameter-group ^
```
Copying a DB parameter group

You can copy custom DB cluster parameter groups that you create. Copying a parameter group is a convenient solution when you have already created a DB cluster parameter group and you want to include most of the custom parameters and values from that group in a new DB cluster parameter group. You can copy a DB cluster parameter group by using the AWS CLI `copy-db-cluster-parameter-group` command or the RDS API `CopyDBClusterParameterGroup` operation.

After you copy a DB cluster parameter group, wait at least 5 minutes before creating your first DB cluster that uses that DB cluster parameter group as the default parameter group. Doing this allows Amazon RDS to fully complete the copy action before the parameter group is used as the default for a new DB cluster. You can use the `Parameter Groups` option of the Amazon RDS console or the `describe-db-cluster-parameters` command to verify that your DB cluster parameter group is created.

Note
You can't copy a default parameter group. However, you can create a new parameter group that is based on a default parameter group.

Console

To copy a DB cluster parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.
3. In the list, choose the custom parameter group that you want to copy.
4. For Parameter group actions, choose Copy.
5. In New DB parameter group identifier, enter a name for the new parameter group.
6. In Description, enter a description for the new parameter group.
7. Choose Copy.

AWS CLI

To copy a DB cluster parameter group, use the AWS CLI `copy-db-cluster-parameter-group` command with the following required parameters:

- `--source-db-cluster-parameter-group-identifier`
- `--target-db-cluster-parameter-group-identifier`
- `--target-db-cluster-parameter-group-description`
The following example creates a new DB cluster parameter group named `mygroup2` that is a copy of the DB cluster parameter group `mygroup1`.

**Example**

For Linux, macOS, or Unix:

```
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"
```

For 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**

To copy a DB cluster parameter group, use the RDS API `CopyDBClusterParameterGroup` operation with the following required parameters:

- SourceDBClusterParameterGroupIdentifier
- TargetDBClusterParameterGroupIdentifier
- TargetDBClusterParameterGroupDescription

**Listing DB parameter groups**

You can list the DB parameter groups you've created for your AWS account.

**Note**

Default parameter groups are automatically created from a default parameter template when you create a DB instance for a particular DB engine and version. These default parameter groups contain preferred parameter settings and can't be modified. When you create a custom parameter group, you can modify parameter settings.

**Console**

To list all DB parameter groups for an AWS account

1. Sign in to the AWS Management Console and open the Amazon RDS console at `https://console.aws.amazon.com/rds/`.
2. In the navigation pane, choose Parameter groups.

   The DB parameter groups appear in a list.

**AWS CLI**

To list all DB parameter groups for an AWS account, use the AWS CLI `describe-db-parameter-groups` command.

**Example**

The following example lists all available DB parameter groups for an AWS account.
Listing DB cluster parameter groups

You can list the DB cluster parameter groups you've created for your AWS account.

**Note**

Default parameter groups are automatically created from a default parameter template when you create a DB cluster for a particular DB engine and version. These default parameter groups contain preferred parameter settings and can't be modified. When you create a custom parameter group, you can modify parameter settings.

**Console**

**To list all DB cluster parameter groups for an AWS account**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/
2. In the navigation pane, choose **Parameter groups**.

   The DB cluster parameter groups appear in the list with **DB cluster parameter group** for Type.

**AWS CLI**

**To list all DB cluster parameter groups for an AWS account**, use the AWS CLI `describe-db-cluster-parameter-groups` command.
Example

The following example lists all available DB cluster parameter groups for an AWS account.

```
aws rds describe-db-cluster-parameter-groups
```

The command returns a response like the following:

```
DBCLUSTERPARAMETERGROUPS        arn:aws:rds:us-west-2:1234567890:cluster-pg:default.aurora5.6 default.aurora5.6 aura5.6 Default cluster parameter group for aurora5.6
```

The following example describes the `mydbclusterparametergroup` parameter group.

For Linux, macOS, or Unix:

```
aws rds describe-db-cluster-parameter-groups --db-cluster-parameter-group-name mydbclusterparametergroup
```

For Windows:

```
aws rds describe-db-cluster-parameter-groups ^
   --db-cluster-parameter-group-name mydbclusterparametergroup
```

The command returns a response like the following:

```
```

RDS API

To list all DB cluster parameter groups for an AWS account, use the RDS API `DescribeDBClusterParameterGroups` action.

Viewing parameter values for a DB parameter group

You can get a list of all parameters in a DB parameter group and their values.

Console

To view the parameter values for a DB parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.

   The DB parameter groups appear in a list.
3. Choose the name of the parameter group to see its list of parameters.

**AWS CLI**

To view the parameter values for a DB parameter group, use the AWS CLI `describe-db-parameters` command with the following required parameter.

- `--db-parameter-group-name`

**Example**

The following example lists the parameters and parameter values for a DB parameter group named `mydbparametergroup`.

```bash
aws rds describe-db-parameters --db-parameter-group-name mydbparametergroup
```

The command returns a response like the following:

<table>
<thead>
<tr>
<th>DBPARAMETER</th>
<th>Parameter Name</th>
<th>Parameter Value</th>
<th>Source</th>
<th>Data Type</th>
<th>Apply Type</th>
<th>Is Modifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBPARAMETER</td>
<td>allow-suspicious-udfs</td>
<td></td>
<td>engine-default</td>
<td>boolean</td>
<td>static</td>
<td>false</td>
</tr>
<tr>
<td>DBPARAMETER</td>
<td>auto_increment_increment</td>
<td></td>
<td>engine-default</td>
<td>integer</td>
<td>dynamic</td>
<td>true</td>
</tr>
<tr>
<td>DBPARAMETER</td>
<td>auto_increment_offset</td>
<td></td>
<td>engine-default</td>
<td>integer</td>
<td>dynamic</td>
<td>true</td>
</tr>
<tr>
<td>DBPARAMETER</td>
<td>binlog_cache_size</td>
<td>32768</td>
<td>system</td>
<td>integer</td>
<td>dynamic</td>
<td>true</td>
</tr>
<tr>
<td>DBPARAMETER</td>
<td>socket</td>
<td>/tmp/mysql.sock</td>
<td>system</td>
<td>string</td>
<td>static</td>
<td>false</td>
</tr>
</tbody>
</table>

**RDS API**

To view the parameter values for a DB parameter group, use the RDS API `DescribeDBParameters` command with the following required parameter.

- `DBParameterGroupName`

**Viewing parameter values for a DB cluster parameter group**

You can get a list of all parameters in a DB cluster parameter group and their values.

**Console**

**To view the parameter values for a DB cluster parameter group**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.
3. The DB cluster parameter groups appear in the list with DB cluster parameter group for Type.
4. Choose the name of the DB cluster parameter group to see its list of parameters.
AWS CLI

To view the parameter values for a DB cluster parameter group, use the AWS CLI `describe-db-cluster-parameters` command with the following required parameter.

- `--db-cluster-parameter-group-name`

Example

The following example lists the parameters and parameter values for a DB cluster parameter group named `mydbclusterparametergroup`, in JSON format.

The command returns a response like the following:

```
aws rds describe-db-cluster-parameters --db-cluster-parameter-group-name mydbclusterparametergroup
```

```
{
   "Parameters": [
   {
      "ApplyMethod": "pending-reboot",
      "Description": "Controls whether user-defined functions that have only an xxx symbol for the main function can be loaded",
      "DataType": "boolean",
      "AllowedValues": "0,1",
      "SupportedEngineModes": [
         "provisioned"
      ],
      "Source": "engine-default",
      "IsModifiable": false,
      "ParameterName": "allow-suspicious-udfs",
      "ApplyType": "static"
   },
   {
      "ApplyMethod": "pending-reboot",
      "Description": "Enables new features in the Aurora engine.",
      "DataType": "boolean",
      "IsModifiable": true,
      "AllowedValues": "0,1",
      "SupportedEngineModes": [
         "provisioned"
      ],
      "Source": "engine-default",
      "ParameterValue": "0",
      "ParameterName": "aurora_lab_mode",
      "ApplyType": "static"
   }
   ...
}
```

The following example lists the parameters and parameter values for a DB cluster parameter group named `mydbclusterparametergroup`, in plain text format.

```
aws rds describe-db-cluster-parameters --db-cluster-parameter-group-name mydbclusterparametergroup --output text
```

The command returns a response like the following:
Comparing parameter groups

You can use the AWS Management Console to view the differences between two parameter groups for the same DB engine and version.

To compare two parameter groups

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Parameter groups.
3. In the list, choose the two parameter groups that you want to compare.
4. For Parameter group actions, choose Compare.

Note
If the items you selected aren't equivalent, you can't choose Compare. For example, you can't compare a MySQL 5.6 and a MySQL 5.7 parameter group. You can't compare a DB parameter group and an Aurora DB cluster parameter group.

DB parameter values

You can specify the value for a DB parameter as any of the following:

- An integer constant
- A DB parameter formula
- A DB parameter function
- A character string constant
- A log expression (the log function represents log base 2), such as
  
  value={log(DBInstanceClassMemory/8187281418)*1000}

DB parameter formulas

A DB parameter formula is an expression that resolves to an integer value or a Boolean value, and is enclosed in braces: {}. You can specify formulas for either a DB parameter value or as an argument to a DB parameter function.

Syntax
DB parameter formula variables

Each formula variable returns integer or a Boolean value. The names of the variables are case-sensitive.

AllocatedStorage

Returns the size, in bytes, of the data volume.

DBInstanceClassMemory

Returns the number of bytes of memory allocated to the DB instance class associated with the current DB instance, less the memory used by the Amazon RDS processes that manage the instance.

EndPointPort

Returns the number of the port used when connecting to the DB instance.

DB parameter formula operators

DB parameter formulas support two operators: division and multiplication.

Division Operator: /

Divides the dividend by the divisor, returning an integer quotient. Decimals in the quotient are truncated, not rounded.

Syntax

\[
\text{dividend} / \text{divisor}
\]

The dividend and divisor arguments must be integer expressions.

Multiplication Operator: *

Multiplies the expressions, returning the product of the expressions. Decimals in the expressions are truncated, not rounded.

Syntax

\[
\text{expression} * \text{expression}
\]

Both expressions must be integers.

DB parameter functions

The parameter arguments can be specified as either integers or formulas. Each function must have at least one argument. Multiple arguments can be specified as a comma-separated list. The list can't have any empty members, such as \text{argument1}, argument3. Function names are case-insensitive.

IF()

Returns an argument.
Syntax

IF(argument1, argument2, argument3)

Returns the second argument if the first argument evaluates to true. Returns the third argument otherwise.

GREATEST()

Returns the largest value from a list of integers or parameter formulas.

Syntax

GREATEST(argument1, argument2,...argumentn)

Returns an integer.

LEAST()

Returns the smallest value from a list of integers or parameter formulas.

Syntax

LEAST(argument1, argument2,...argumentn)

Returns an integer.

SUM()

Adds the values of the specified integers or parameter formulas.

Syntax

SUM(argument1, argument2,...argumentn)

Returns an integer.

**DB parameter value examples**

These examples show using formulas and functions in the values for DB parameters.

**Warning**

Improperly setting parameters in a DB parameter group can have unintended adverse effects, including degraded performance and system instability. Always exercise caution when modifying database parameters and back up your data before modifying your DB parameter group. Try out parameter group changes on a test DB instances, created using point-in-time-restores, before applying those parameter group changes to your production DB instances.

You can specify the `LEAST()` function in an Aurora MySQL `table_definition_cache` parameter value to set the number of table definitions that can be stored in the definition cache to the lesser of `DBInstanceClassMemory/393040` or `20000`.

`LEAST({DBInstanceClassMemory/393040}, 20000)`
Migrating data to an Amazon Aurora DB cluster

You have several options for migrating data from your existing database to an Amazon Aurora DB cluster, depending on database engine compatibility. Your migration options also depend on the database that you are migrating from and the size of the data that you are migrating.

Migrating data to an Amazon Aurora MySQL DB cluster

You can migrate data from one of the following sources to an Amazon Aurora MySQL DB cluster.

- An Amazon RDS MySQL DB instance
- A MySQL database external to Amazon RDS
- A database that is not MySQL-compatible

For more information, see Migrating data to an Amazon Aurora MySQL DB cluster (p. 644).

Migrating data to an Amazon Aurora PostgreSQL DB cluster

You can migrate data from one of the following sources to an Amazon Aurora PostgreSQL DB cluster.

- An Amazon RDS PostgreSQL DB instance
- A database that is not PostgreSQL-compatible

For more information, see Migrating data to Amazon Aurora with PostgreSQL compatibility (p. 1005).
Managing an Amazon Aurora DB cluster

This section shows how to manage and maintain your Aurora DB cluster. Aurora involves clusters of database servers that are connected in a replication topology. Thus, managing Aurora often involves deploying changes to multiple servers and making sure that all Aurora Replicas are keeping up with the master server. Because Aurora transparently scales the underlying storage as your data grows, managing Aurora requires relatively little management of disk storage. Likewise, because Aurora automatically performs continuous backups, an Aurora cluster does not require extensive planning or downtime for performing backups.

Topics
- Stopping and starting an Amazon Aurora DB cluster (p. 323)
- Modifying an Amazon Aurora DB cluster (p. 327)
- Adding Aurora replicas to a DB cluster (p. 345)
- Managing performance and scaling for Aurora DB clusters (p. 349)
- Cloning an Aurora DB cluster volume (p. 355)
- Integrating Aurora with other AWS services (p. 371)
- Maintaining an Amazon Aurora DB cluster (p. 388)
- Rebooting a DB instance in a DB cluster (p. 396)
- Deleting an Aurora DB cluster or a DB instance (p. 398)
- Tagging Amazon RDS resources (p. 401)
- Working with Amazon Resource Names (ARNs) in Amazon RDS (p. 406)
- Amazon Aurora updates (p. 413)
Stopping and starting an Amazon Aurora DB cluster

Stopping and starting Amazon Aurora clusters helps you manage costs for development and test environments. You can temporarily stop all the DB instances in your cluster, instead of setting up and tearing down all the DB instances each time that you use the cluster.

Topics

- Overview of stopping and starting an Aurora DB cluster (p. 323)
- Limitations for stopping and starting Aurora DB clusters (p. 323)
- Stopping an Aurora DB cluster (p. 324)
- Possible operations while an Aurora DB cluster is stopped (p. 325)
- Starting an Aurora DB cluster (p. 325)

Overview of stopping and starting an Aurora DB cluster

During periods where you don't need an Aurora cluster, you can stop all instances in that cluster at once. You can start the cluster again anytime you need to use it. Starting and stopping simplifies the setup and teardown processes for clusters used for development, testing, or similar activities that don't require continuous availability. You can perform all the AWS Management Console procedures involved with only a single action, regardless of how many instances are in the cluster.

While your DB cluster is stopped, you are charged only for cluster storage, manual snapshots, and automated backup storage within your specified retention window. You aren't charged for any DB instance hours. Aurora automatically starts your DB cluster after seven days so that it doesn't fall behind any required maintenance updates.

To minimize charges for a lightly loaded Aurora cluster, you can stop the cluster instead of deleting all of its Aurora Replicas. For clusters with more than one or two instances, frequently deleting and recreating the DB instances is only practical using the AWS CLI or Amazon RDS API. Such a sequence of operations can also be difficult to perform in the right order, for example to delete all Aurora Replicas before deleting the primary instance to avoid activating the failover mechanism.

Don't use starting and stopping if you need to keep your DB cluster running but it has more capacity than you need. If your cluster is too costly or not very busy, delete one or more DB instances or change all your DB instances to a small instance class. You can't stop an individual Aurora DB instance.

Limitations for stopping and starting Aurora DB clusters

Some Aurora clusters can't be stopped and started:

- You can't stop and start a cluster that's part of an Aurora global database (p. 206).
- For a cluster that uses the Aurora parallel query (p. 697) feature, the minimum Aurora MySQL versions are 1.23.0 and 2.09.0.
- You can't stop and start an Aurora Serverless cluster (p. 134).
- You can't stop and start an Aurora multi-master cluster (p. 766).
If an existing cluster can't be stopped and started, the Stop action isn't available from the Actions menu on the Databases page or the details page.

Stopping an Aurora DB cluster

To use an Aurora DB cluster or perform administration, you always begin with a running Aurora DB cluster, then stop the cluster, and then start the cluster again. While your cluster is stopped, you are charged for cluster storage, manual snapshots, and automated backup storage within your specified retention window, but not for DB instance hours.

The stop operation stops the Aurora Replica instances first, then the primary instance, to avoid activating the failover mechanism.

You can't stop a DB cluster that acts as the replication target for data from another DB cluster, or acts as the replication master and transmits data to another cluster.

You can't stop certain special kinds of clusters. Currently, you can't stop a cluster that's part of an Aurora global database, or a multi-master cluster.

Console

To stop an Aurora cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases, and then choose a cluster. You can perform the stop operation from this page, or navigate to the details page for the DB cluster that you want to stop.
   - If an existing cluster can't be stopped and started, the Stop action isn't available from the Actions menu on the Databases page or the details page. For the kinds of clusters that you can't start and stop, see Limitations for stopping and starting Aurora DB clusters (p. 323).
3. For Actions, choose Stop.

AWS CLI

To stop a DB instance by using the AWS CLI, call the stop-db-cluster command with the following parameters:

- --db-cluster-identifier – the name of the Aurora cluster.

Example

```
aws rds stop-db-cluster --db-cluster-identifier mydbcluster
```

RDS API

To stop a DB instance by using the Amazon RDS API, call the StopDBCluster operation with the following parameter:

- DBClusterIdentifier – the name of the Aurora cluster.
Possible operations while an Aurora DB cluster is stopped

While an Aurora cluster is stopped, you can do a point-in-time restore to any point within your specified automated backup retention window. For details about doing a point-in-time restore, see Restoring data (p. 415).

You can't modify the configuration of an Aurora DB cluster, or any of its DB instances, while the cluster is stopped. You also can't add or remove DB instances from the cluster, or delete the cluster if it still has any associated DB instances. You must start the cluster before performing any such administrative actions.

Stopping a DB cluster removes pending actions, except for the DB cluster parameter group or for the DB parameter groups of the DB cluster instances.

Aurora applies any scheduled maintenance to your stopped cluster after it's started again. Remember that after seven days, Aurora automatically starts any stopped clusters so that they don't fall too far behind in their maintenance status.

Aurora also doesn't perform any automated backups, because the underlying data can't change while the cluster is stopped. Aurora doesn't extend the backup retention period while the cluster is stopped.

Starting an Aurora DB cluster

You always start an Aurora DB cluster beginning with an Aurora cluster that is already in the stopped state. When you start the cluster, all its DB instances become available again. The cluster keeps its configuration settings such as endpoints, parameter groups, and VPC security groups.

Console

To start an Aurora cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases, and then choose a cluster. You can perform the start operation from this page, or navigate to the details page for the DB cluster that you want to start.
3. For Actions, choose Start.

AWS CLI

To start a DB cluster by using the AWS CLI, call the start-db-cluster command with the following parameters:

* `--db-cluster-identifier` – the name of the Aurora cluster. This name is either a specific cluster identifier you chose when creating the cluster, or the DB instance identifier you chose with -cluster appended to the end.

Example

```bash
aws rds start-db-cluster --db-cluster-identifier mydbcluster
```
RDS API

To start an Aurora DB cluster by using the Amazon RDS API, call the `StartDBCluster` operation with the following parameter:

- `DBCluster` – the name of the Aurora cluster. This name is either a specific cluster identifier you chose when creating the cluster, or the DB instance identifier you chose with `-cluster` appended to the end.
Modifying an Amazon Aurora DB cluster

You can change the settings of a DB cluster to accomplish tasks such as changing its backup retention period or its database port. You can also modify DB instances in a DB cluster to accomplish tasks such as changing its DB instance class or enabling Performance Insights for it. This topic guides you through modifying an Aurora DB cluster and its DB instances, and describes the settings for each.

We recommend that you test any changes on a test DB cluster or DB instance before modifying a production DB cluster or DB instance, so that you fully understand the impact of each change. This is especially important when upgrading database versions.

Modifying the DB cluster by using the console, CLI, and API

You can modify a DB cluster using the AWS Management Console, the AWS CLI, or the RDS API.

Note
For Aurora, when you modify a DB cluster, only changes to the DB cluster identifier, IAM DB authentication, and New master password settings are affected by the Apply Immediately setting. All other modifications are applied immediately, regardless of the value of the Apply Immediately setting.

Console

To modify a DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases, and then select the DB cluster that you want to modify.
4. Change any of the settings that you want. For information about each setting, see Settings for Amazon Aurora (p. 330).

Note
In the AWS Management Console, some instance level changes only apply to the current DB instance, while others apply to the entire DB cluster. For information about whether a setting applies to the DB instance or the DB cluster, see the scope for the setting in Settings for Amazon Aurora (p. 330). To change a setting that modifies the entire DB cluster at the instance level in the AWS Management Console, follow the instructions in Modify a DB instance in a DB cluster (p. 328).

5. When all the changes are as you want them, choose Continue and check the summary of modifications.
6. To apply the changes immediately, select Apply immediately.
7. On the confirmation page, review your changes. If they are correct, choose Modify cluster to save your changes.

Alternatively, choose Back to edit your changes, or choose Cancel to cancel your changes.

AWS CLI

To modify a DB cluster using the AWS CLI, call the modify-db-cluster command. Specify the DB cluster identifier, and the values for the settings that you want to modify. For information about each setting, see Settings for Amazon Aurora (p. 330).
Note
Some settings only apply to DB instances. To change those settings, follow the instructions in Modify a DB instance in a DB cluster (p. 328).

Example

The following command modifies mydbcluster by setting the backup retention period to 1 week (7 days).

For Linux, macOS, or Unix:

```
aws rds modify-db-cluster \
  --db-cluster-identifier mydbcluster \
  --backup-retention-period 7
```

For Windows:

```
aws rds modify-db-cluster ^
  --db-cluster-identifier mydbcluster ^
  --backup-retention-period 7
```

RDS API

To modify a DB cluster using the Amazon RDS API, call the ModifyDBCluster operation. Specify the DB cluster identifier, and the values for the settings that you want to modify. For information about each parameter, see Settings for Amazon Aurora (p. 330).

Note
Some settings only apply to DB instances. To change those settings, follow the instructions in Modify a DB instance in a DB cluster (p. 328).

Modify a DB instance in a DB cluster

You can modify a DB instance in a DB cluster using the AWS Management Console, the AWS CLI, or the RDS API.

When you modify a DB instance, you can apply the changes immediately. To apply changes immediately, when you select the Apply Immediately option in the AWS Management Console, you use the --apply-immediately parameter when calling the AWS CLI, or you set the ApplyImmediately parameter to true when using the Amazon RDS API.

If you don't choose to apply changes immediately, the changes are put into the pending modifications queue. During the next maintenance window, any pending changes in the queue are applied. If you choose to apply changes immediately, your new changes and any changes in the pending modifications queue are applied.

Important
If any of the pending modifications require downtime, choosing apply immediately can cause unexpected downtime for the DB instance. There is no downtime for the other DB instances in the DB cluster.

Console

To modify a DB instance in a DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**, and then select the DB instance that you want to modify.

3. For **Actions**, choose **Modify**. The **Modify DB Instance** page appears.

4. Change any of the settings that you want. For information about each setting, see **Settings for Amazon Aurora** (p. 330).

   **Note**
   Some settings apply to the entire DB cluster and must be changed at the cluster level. To change those settings, follow the instructions in **Modifying the DB cluster by using the console, CLI, and API** (p. 327).

   In the AWS Management Console, some instance level changes only apply to the current DB instance, while others apply to the entire DB cluster. For information about whether a setting applies to the DB instance or the DB cluster, see the **Settings for Amazon Aurora** (p. 330).

5. When all the changes are as you want them, choose **Continue** and check the summary of modifications.

6. To apply the changes immediately, select **Apply immediately**.

7. On the confirmation page, review your changes. If they are correct, choose **Modify DB Instance** to save your changes.

   Alternatively, choose **Back** to edit your changes, or choose **Cancel** to cancel your changes.

### AWS CLI

To modify a DB instance in a DB cluster by using the AWS CLI, call the `modify-db-instance` command. Specify the DB instance identifier, and the values for the settings that you want to modify. For information about each parameter, see **Settings for Amazon Aurora** (p. 330).

**Note**
Some settings apply to the entire DB cluster. To change those settings, follow the instructions in **Modifying the DB cluster by using the console, CLI, and API** (p. 327).

**Example**

The following code modifies `mydbinstance` by setting the DB instance class to `db.r4.xlarge`. The changes are applied during the next maintenance window by using `--no-apply-immediately`. Use `--apply-immediately` to apply the changes immediately.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-instance \
   --db-instance-identifier mydbinstance \
   --db-instance-class db.r4.xlarge \
   --no-apply-immediately
```

For Windows:

```bash
aws rds modify-db-instance ^
   --db-instance-identifier mydbinstance ^
   --db-instance-class db.r4.xlarge ^
   --no-apply-immediately
```

### RDS API

To modify a MySQL instance by using the Amazon RDS API, call the `ModifyDBInstance` operation. Specify the DB instance identifier, and the values for the settings that you want to modify. For information about each parameter, see **Settings for Amazon Aurora** (p. 330).
**Note**

Some settings apply to the entire DB cluster. To change those settings, follow the instructions in Modifying the DB cluster by using the console, CLI, and API (p. 327).

### Settings for Amazon Aurora

The following table contains details about which settings you can modify, the methods for modifying the setting, and the scope of the setting. The scope determines whether the setting applies to the entire DB cluster or if it can be set only for specific DB instances.

<table>
<thead>
<tr>
<th>Setting and description</th>
<th>Method</th>
<th>Scope</th>
<th>Downtime notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto minor version upgrade</strong></td>
<td>Note This setting is enabled by default. For each new cluster, choose the appropriate value for this setting based on its importance, expected lifetime, and the amount of verification testing that you do after each upgrade.</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change. Outages do occur during future maintenance windows when Aurora applies automatic upgrades.</td>
</tr>
<tr>
<td>Whether you want the DB instance to receive preferred minor engine version upgrades automatically when they become available. Upgrades are installed only during your scheduled maintenance window.</td>
<td>For more information about engine updates, see Database engine updates for Amazon Aurora PostgreSQL (p. 1147) and Database engine updates for Amazon Aurora MySQL (p. 874). For more information about the Auto minor version upgrade setting for Aurora MySQL, see Enabling automatic upgrades between minor Aurora MySQL versions (p. 878).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting and description</td>
<td>Method</td>
<td>Scope</td>
<td>Downtime notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Backup retention period</strong></td>
<td>Using the AWS Management Console, <strong>Modifying the DB cluster by using the console, CLI, and API (p. 327).</strong> Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--backup-retention-period</code> option. Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>BackupRetentionPeriod</code> parameter.</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td><strong>Backup window (Start time)</strong></td>
<td>Using the AWS Management Console, <strong>Modifying the DB cluster by using the console, CLI, and API (p. 327).</strong> Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--preferred-backup-window</code> option. Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>PreferredBackupWindow</code> parameter.</td>
<td>The entire DB.</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td>Setting and description</td>
<td>Method</td>
<td>Scope</td>
<td>Downtime notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>Using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the <code>--ca-certificate-identifier</code> option. Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>CACertificateIdentifier</code> parameter.</td>
<td>Only the specified DB instance</td>
<td>An outage occurs during this change. The DB instance is rebooted.</td>
</tr>
<tr>
<td>Copy tags to snapshots</td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327). Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--copy-tags-to-snapshot</code> or <code>--no-copy-tags-to-snapshot</code> option. Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>CopyTagsToSnapshot</code> parameter.</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td>Data API</td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327). Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--enable-http-endpoint</code> option. Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>EnableHttpEndpoint</code> parameter.</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change.</td>
</tr>
</tbody>
</table>
### Available settings

<table>
<thead>
<tr>
<th>Setting and description</th>
<th>Method</th>
<th>Scope</th>
<th>Downtime notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database authentication</strong></td>
<td>The database authentication option you want to use.</td>
<td>Choose <strong>Password authentication</strong> to authenticate database users with database passwords only.</td>
<td>Choose <strong>Password and IAM DB authentication</strong> to authenticate database users with database passwords and user credentials through IAM users and roles. For more information, see IAM database authentication (p. 1238).</td>
</tr>
</tbody>
</table>

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

### Database port

The port that you want to use to access the DB cluster.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.

#### Using the AWS Management Console,
**Modifying the DB cluster by using the console, CLI, and API (p. 327).**

Using the AWS CLI, run `modify-db-cluster` and set the `--no-enable-iam-database-authentication` option.

Using the RDS API, call `ModifyDBCluster` and set the `EnableIAMDatabaseAuthentication` parameter.

#### Using the AWS CLI, run `modify-db-cluster` and set the `--port` option.

Using the RDS API, call `ModifyDBCluster` and set the `Port` parameter.
### Setting and description

<table>
<thead>
<tr>
<th>Setting and description</th>
<th>Method</th>
<th>Scope</th>
<th>Downtime notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DB cluster identifier</strong>&lt;br&gt;The DB cluster identifier. This value is stored as a lowercase string.&lt;br&gt;When you change the DB cluster identifier, the DB cluster endpoint changes, and the endpoints of the DB instances in the DB cluster change.</td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327).&lt;br&gt;Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--new-db-cluster-identifier</code> option.&lt;br&gt;Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>NewDBClusterIdentifier</code> parameter.</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td><strong>DB cluster parameter group</strong>&lt;br&gt;The DB cluster parameter group that you want associated with the DB cluster.&lt;br&gt;For more information, see Working with DB parameter groups and DB cluster parameter groups (p. 298).</td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327).&lt;br&gt;Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--db-cluster-parameter-group-name</code> option.&lt;br&gt;Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>DBClusterParameterGroupName</code> parameter.</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change. When you change the parameter group, changes to some parameters are applied to the DB instances in the DB cluster immediately without a reboot. Changes to other parameters are applied only after the DB instances in the DB cluster are rebooted.</td>
</tr>
<tr>
<td><strong>DB engine version</strong>&lt;br&gt;The version of the DB engine that you want to use. Before you upgrade your production DB cluster, we recommend that you test the upgrade process on a test DB cluster to verify its duration and to validate your applications.</td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327).&lt;br&gt;Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--engine-version</code> option.&lt;br&gt;Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>EngineVersion</code> parameter.</td>
<td>The entire DB cluster</td>
<td>An outage occurs during this change.</td>
</tr>
<tr>
<td>Setting and description</td>
<td>Method</td>
<td>Scope</td>
<td>Downtime notes</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>DB instance class</strong></td>
<td>Using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the <code>--db-instance-class</code> option. Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>DBInstanceClass</code> parameter.</td>
<td>Only the specified DB instance</td>
<td>An outage occurs during this change.</td>
</tr>
<tr>
<td>The DB instance class that you want to use. For more information, see DB instance classes (p. 46).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DB instance identifier</strong></td>
<td>Using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the <code>--new-db-instance-identifier</code> option. Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>NewDBInstanceIdentifier</code> parameter.</td>
<td>Only the specified DB instance</td>
<td>An outage occurs during this change. The DB instance is rebooted.</td>
</tr>
<tr>
<td>The DB instance identifier. This value is stored as a lowercase string.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DB parameter group</strong></td>
<td>Using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the <code>--db-parameter-group-name</code> option. Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>DBParameterGroupName</code> parameter.</td>
<td>Only the specified DB instance</td>
<td>An outage doesn't occur during this change. However, you must manually reboot the DB instance before the new DB parameter group is used by the DB instance. For more information, see Working with DB parameter groups and DB cluster parameter groups (p. 298) and Rebooting a DB instance in a DB cluster (p. 396).</td>
</tr>
<tr>
<td>The DB parameter group that you want associated with the DB instance. For more information, see Working with DB parameter groups and DB cluster parameter groups (p. 298).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Available settings

<table>
<thead>
<tr>
<th>Setting and description</th>
<th>Method</th>
<th>Scope</th>
<th>Downtime notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deletion protection</strong></td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327). Using the AWS CLI, run <code>modify-db-cluster</code> and set the `--deletion-protection</td>
<td>--no-deletion-protection<code>option. Using the RDS API, call</code>ModifyDBCluster<code>and set the</code>DeletionProtection` parameter.</td>
<td>The entire DB cluster</td>
</tr>
<tr>
<td><strong>Enhanced monitoring</strong></td>
<td>Using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the <code>--monitoring-role-arn</code> and <code>--monitoring-interval</code> options. Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>MonitoringRoleArn</code> and <code>MonitoringInterval</code> parameters.</td>
<td>Only the specified DB instance</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td>Setting and description</td>
<td>Method</td>
<td>Scope</td>
<td>Downtime notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Log exports</strong>&lt;br&gt;Select the log types to publish to Amazon CloudWatch Logs.&lt;br&gt;For more information, see MySQL database log files (p. 622).</td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327).&lt;br&gt;Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--cloudwatch-logs-export-configuration</code> option.&lt;br&gt;Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>CloudwatchLogsExportConfiguration</code> parameter.</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change.</td>
</tr>
</tbody>
</table>
## Available settings

<table>
<thead>
<tr>
<th>Setting and description</th>
<th>Method</th>
<th>Scope</th>
<th>Downtime notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maintenance window</strong></td>
<td>To change the maintenance window for the DB cluster using the AWS Management Console, <strong>Modifying the DB cluster by using the console, CLI, and API (p. 327)</strong>.</td>
<td>The entire DB cluster or a single DB instance</td>
<td>If there are one or more pending actions that cause an outage, and the maintenance window is changed to include the current time, then those pending actions are applied immediately, and an outage occurs.</td>
</tr>
<tr>
<td></td>
<td>To change the maintenance window for a DB instance using the AWS Management Console, <strong>Modify a DB instance in a DB cluster (p. 328)</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To change the maintenance window for the DB cluster using the AWS CLI, run <strong>modify-db-cluster</strong> and set the <strong>--preferred-maintenance-window</strong> option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To change the maintenance window for a DB instance using the AWS CLI, run <strong>modify-db-instance</strong> and set the <strong>--preferred-maintenance-window</strong> option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To change the maintenance window for the DB cluster using the RDS API, call <strong>ModifyDBCluster</strong> and set the <strong>PreferredMaintenanceWindow</strong> parameter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To change the maintenance window for a DB instance using the RDS API, call <strong>ModifyDBInstance</strong> and set the <strong>PreferredMaintenanceWindow</strong> parameter.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The time range during which system maintenance occurs. System maintenance includes upgrades, if applicable. The maintenance window is a start time in Universal Coordinated Time (UTC), and a duration in hours.

If you set the window to the current time, there must be at least 30 minutes between the current time and end of the window to ensure any pending changes are applied.

You can set the maintenance window independently for the DB cluster and for each DB instance in the DB cluster. When the scope of a modification is the entire DB cluster, the modification is performed during the DB cluster maintenance window. When the scope of a modification is the a DB instance, the modification is performed during maintenance window of that DB instance.

The maintenance window and the backup window for the DB cluster can't overlap.

For more information, see **The Amazon RDS maintenance window (p. 391)**.
<table>
<thead>
<tr>
<th>Setting and description</th>
<th>Method</th>
<th>Scope</th>
<th>Downtime notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New master password</strong></td>
<td>The password for your master user. The password must contain from 8 to 41 alphanumeric characters.</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td></td>
<td>Using the AWS Management Console, *<a href="#">Modifying the DB cluster by using the console, CLI, and API (p. 327).*</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--master-user-password</code> option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>MasterUserPassword</code> parameter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Performance Insights</strong></td>
<td>Whether to enable Performance Insights, a tool that monitors your DB instance load so that you can analyze and troubleshoot your database performance. For more information, see *<a href="#">Using Amazon RDS Performance Insights (p. 514).*</a></td>
<td>Only the specified DB instance</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td></td>
<td>Using the AWS Management Console, *<a href="#">Modify a DB instance in a DB cluster (p. 328).*</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using the AWS CLI, run <code>modify-db-instance</code> and set the `--enable-performance-insights</td>
<td>--no-enable-performance-insights` option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>EnablePerformanceInsights</code> parameter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting and description</td>
<td>Method</td>
<td>Scope</td>
<td>Downtime notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Performance Insights AWS KMS key identifier</strong></td>
<td>Using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the <code>--performance-insights-kms-key-id</code> option. Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>PerformanceInsightsKMSKeyId</code> parameter.</td>
<td>Only the specified DB instance</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td><strong>Performance Insights retention period</strong></td>
<td>Using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the <code>--performance-insights-retention-period</code> option. Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>PerformanceInsightsRetentionPeriod</code> parameter.</td>
<td>Only the specified DB instance</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td><strong>Promotion tier</strong></td>
<td>Using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the <code>--promotion-tier</code> option. Using the RDS API, call <code>ModifyDBInstance</code> and set the <code>PromotionTier</code> parameter.</td>
<td>Only the specified DB instance</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td>Setting and description</td>
<td>Method</td>
<td>Scope</td>
<td>Downtime notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Public access</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Publicly accessible</strong></td>
<td>using the AWS Management Console, Modify a DB instance in a DB cluster (p. 328). Using the AWS CLI, run <code>modify-db-instance</code> and set the `--publicly-accessible</td>
<td>--no-publicly-accessible<code>option. Using the RDS API, call</code>ModifyDBInstance<code>and set the</code>PubliclyAccessible` parameter.</td>
<td>only the specified DB instance</td>
</tr>
<tr>
<td><strong>Not publicly accessible</strong></td>
<td>to make the DB instance accessible only from inside the VPC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information, see Hiding a DB instance in a VPC from the internet (p. 1293). To connect to a DB instance from outside of its Amazon VPC, the DB instance must be publicly accessible, access must be granted using the inbound rules of the DB instance's security group, and other requirements must be met. For more information, see Can't connect to Amazon RDS DB instance (p. 1306). If your DB instance isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 1221).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting and description</td>
<td>Method</td>
<td>Scope</td>
<td>Downtime notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Scaling configuration</strong></td>
<td>The scaling properties of the DB cluster. You can only modify scaling properties for DB clusters in serverless DB engine mode. This setting is available only for Aurora MySQL. For information about Aurora Serverless, see Using Amazon Aurora Serverless v1 (p. 134).</td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327). Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--scaling-configuration</code> option. Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>ScalingConfiguration</code> parameter.</td>
<td>The entire DB cluster An outage doesn't occur during this change.</td>
</tr>
<tr>
<td><strong>Security group</strong></td>
<td>The security group you want associated with the DB cluster. For more information, see Controlling access with security groups (p. 1274).</td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327). Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--vpc-security-group-ids</code> option. Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>VpcSecurityGroupIds</code> parameter.</td>
<td>The entire DB cluster An outage doesn't occur during this change.</td>
</tr>
</tbody>
</table>
## Setting and description

<table>
<thead>
<tr>
<th>Setting and description</th>
<th>Method</th>
<th>Scope</th>
<th>Downtime notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target Backtrack window</strong></td>
<td>Using the AWS Management Console, Modifying the DB cluster by using the console, CLI, and API (p. 327).</td>
<td>The entire DB cluster</td>
<td>An outage doesn't occur during this change.</td>
</tr>
<tr>
<td></td>
<td>Using the AWS CLI, run <code>modify-db-cluster</code> and set the <code>--backtrack-window</code> option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using the RDS API, call <code>ModifyDBCluster</code> and set the <code>BacktrackWindow</code> parameter.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Settings that do not apply to Amazon Aurora

The following settings in the AWS CLI command `modify-db-instance` and the RDS API operation `ModifyDBInstance` do not apply to Amazon Aurora.

**Note**
The AWS Management Console doesn't allow you to modify these settings for Aurora.

<table>
<thead>
<tr>
<th>AWS CLI setting</th>
<th>RDS API setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--allocated-storage</code></td>
<td><code>AllocatedStorage</code></td>
</tr>
<tr>
<td>`--allow-major-version-upgrade</td>
<td>--no-allow-major-version-upgrade`</td>
</tr>
<tr>
<td>`--copy-tags-to-snapshot</td>
<td>--no-copy-tags-to-snapshot`</td>
</tr>
<tr>
<td><code>--domain</code></td>
<td><code>Domain</code></td>
</tr>
<tr>
<td><code>--db-security-groups</code></td>
<td><code>DBSecurityGroups</code></td>
</tr>
<tr>
<td><code>--db-subnet-group-name</code></td>
<td><code>DBSubnetGroupName</code></td>
</tr>
<tr>
<td><code>--domain-iam-role-name</code></td>
<td><code>DomainIAMRoleName</code></td>
</tr>
<tr>
<td>`--multi-az</td>
<td>--no-multi-az`</td>
</tr>
<tr>
<td><code>--iops</code></td>
<td><code>Iops</code></td>
</tr>
<tr>
<td><code>--license-model</code></td>
<td><code>LicenseModel</code></td>
</tr>
<tr>
<td><code>--option-group-name</code></td>
<td><code>OptionGroupName</code></td>
</tr>
<tr>
<td><code>--processor-features</code></td>
<td><code>ProcessorFeatures</code></td>
</tr>
<tr>
<td>AWS CLI setting</td>
<td>RDS API setting</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>--storage-type</td>
<td>StorageType</td>
</tr>
<tr>
<td>--tde-credential-arn</td>
<td>TdeCredentialArn</td>
</tr>
<tr>
<td>--tde-credential-password</td>
<td>TdeCredentialPassword</td>
</tr>
<tr>
<td>--use-default-processor-features</td>
<td>--no-use-default-processor-features</td>
</tr>
</tbody>
</table>
Adding Aurora replicas to a DB cluster

An Aurora DB cluster with single-master replication has one primary DB instance and up to 15 Aurora Replicas. The primary DB instance supports read and write operations, and performs all data modifications to the cluster volume. Aurora Replicas connect to the same storage volume as the primary DB instance, but support read operations only. You use Aurora Replicas to offload read workloads from the primary DB instance. For more information, see Aurora Replicas (p. 57).

Amazon Aurora also supports replication with an external database, such as an RDS DB instance. The RDS DB instance must be in the same AWS Region as Amazon Aurora. For more information, see Replication with Amazon Aurora (p. 57).

Amazon Aurora Replicas have the following limitations:

- You can't create an Aurora Replica for an Aurora Serverless v1 DB cluster. Aurora Serverless v1 has a single DB instance that scales up and down automatically to support all database read and write operations.
- You can't create Aurora Replicas for an Aurora multi-master cluster. By design, an Aurora multi-master cluster has read-write DB instances only.
- Aurora PostgreSQL–based DB clusters can have only one Aurora Replica. If you try to create an Aurora Replica for an Aurora PostgreSQL DB cluster that already has an Aurora Replica, Aurora rejects your request. For more information, see Replication with Amazon Aurora PostgreSQL (p. 1034).
- Aurora PostgreSQL–based DB clusters can't have Aurora Replicas in different AWS Regions. In other words, Aurora PostgreSQL doesn't support cross-region Aurora Replicas. To scale reads for an Aurora PostgreSQL–based DB cluster beyond a single Region, use Aurora global database. Aurora global database supports a primary Aurora DB cluster in one AWS Region with up to five secondary read-only Aurora DB clusters in five different Regions. For more information see Using Amazon Aurora global databases (p. 206).

We recommend that you distribute the primary instance and Aurora Replicas of your Aurora DB cluster over multiple Availability Zones to improve the availability of your DB cluster. For more information, see Region availability (p. 6).

To remove an Aurora Replica from an Aurora DB cluster, delete the Aurora Replica by following the instructions in Deleting an Aurora DB cluster or a DB instance (p. 398).

You can add Aurora Replicas to a DB cluster using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To add an Aurora replica to a DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases, and then select the DB cluster where you want to add the new DB instance.
3. Make sure that both the cluster and the primary instance are in the Available state. If the DB cluster or the primary instance are in a transitional state such as Creating, you can't add a replica.

   If the cluster doesn't have a primary instance, create one using the create-db-instance AWS CLI command. This situation can arise if you used the CLI to restore a DB cluster snapshot and then view the cluster in the AWS Management Console.

4. For Actions, choose Add reader.
The Add reader page appears.

5. On the Add reader page, specify options for your Aurora Replica. The following table shows settings for an Aurora Replica.

<table>
<thead>
<tr>
<th>For this option</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability zone</td>
<td>Determine if you want to specify a particular Availability Zone. The list includes only those Availability Zones that are mapped by the DB subnet group you specified earlier. For more information about Availability Zones, see Regions and Availability Zones (p. 5).</td>
</tr>
<tr>
<td>Publicly accessible</td>
<td>Select Yes to give the Aurora Replica a public IP address; otherwise, select No. For more information about hiding Aurora Replicas from public access, see Hiding a DB instance in a VPC from the internet (p. 1293).</td>
</tr>
<tr>
<td>Encryption</td>
<td>Select Enable encryption to enable encryption at rest for this Aurora Replica. For more information, see Encrypting Amazon Aurora resources (p. 1208).</td>
</tr>
<tr>
<td>DB instance class</td>
<td>Select a DB instance class that defines the processing and memory requirements for the Aurora Replica. For more information about DB instance class options, see DB instance classes (p. 46).</td>
</tr>
<tr>
<td>Aurora replica source</td>
<td>Select the identifier of the primary instance to create an Aurora Replica for.</td>
</tr>
<tr>
<td>DB instance identifier</td>
<td>Type a name for the instance that is unique for your account in the AWS Region you selected. You might choose to add some intelligence to the name such as including the AWS Region and DB engine you selected, for example aurora-read-instance1.</td>
</tr>
<tr>
<td>Priority</td>
<td>Choose a failover priority for the instance. If you don't select a value, the default is tier-1. This priority determines the order in which Aurora Replicas are promoted when recovering from a primary instance failure. For more information, see Fault tolerance for an Aurora DB cluster (p. 56).</td>
</tr>
<tr>
<td>Database port</td>
<td>The port for an Aurora Replica is the same as the port for the DB cluster.</td>
</tr>
<tr>
<td>DB parameter group</td>
<td>Select a parameter group. Aurora has a default parameter group you can use, or you can create your own parameter group. For more information about parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).</td>
</tr>
<tr>
<td>Enhanced monitoring</td>
<td>Choose Enable enhanced monitoring to enable gathering metrics in real time for the operating system that your DB cluster runs on. For more information, see Enhanced Monitoring (p. 504).</td>
</tr>
<tr>
<td>Monitoring Role</td>
<td>Only available if Enhanced Monitoring is set to Enable enhanced monitoring. Choose the IAM role that</td>
</tr>
</tbody>
</table>
Adding Aurora replicas

<table>
<thead>
<tr>
<th>For this option</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>For this option</td>
<td>you created to permit Amazon RDS to communicate with Amazon CloudWatch Logs for you, or choose Default to have RDS create a role for you named rds-monitoring-role. For more information, see Enhanced Monitoring (p. 504).</td>
</tr>
<tr>
<td>Granularity</td>
<td>Only available if Enhanced Monitoring is set to Enable enhanced monitoring. Set the interval, in seconds, between when metrics are collected for your DB cluster.</td>
</tr>
<tr>
<td>Auto minor version upgrade</td>
<td>Select Enable auto minor version upgrade if you want to enable your Aurora DB cluster to receive minor DB Engine version upgrades automatically when they become available.</td>
</tr>
<tr>
<td></td>
<td>The Auto minor version upgrade setting applies to both Aurora PostgreSQL and Aurora MySQL DB clusters. For Aurora MySQL 1.x and 2.x clusters, this setting upgrades the clusters to a maximum version of 1.22.2 and 2.07.2.</td>
</tr>
<tr>
<td></td>
<td>For more information about engine updates for Aurora PostgreSQL, see Database engine updates for Amazon Aurora PostgreSQL (p. 1147).</td>
</tr>
<tr>
<td></td>
<td>For more information about engine updates for Aurora MySQL, see Database engine updates for Amazon Aurora MySQL (p. 874).</td>
</tr>
</tbody>
</table>

6. Choose Add reader to create the Aurora Replica.

AWS CLI

To create an Aurora Replica in your DB cluster, run the create-db-instance AWS CLI command. Include the name of the DB cluster as the --db-cluster-identifier option. You can optionally specify an Availability Zone for the Aurora Replica using the --availability-zone parameter, as shown in the following examples.

For example, the following command creates a new MySQL 5.7–compatible Aurora Replica named sample-instance-us-west-2a.

For Linux, macOS, or Unix:

```bash
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.r4.large --availability-zone us-west-2a
```

For Windows:

```bash
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.r4.large --availability-zone us-west-2a
```

The following command creates a new MySQL 5.6–compatible Aurora Replica named sample-instance-us-west-2a.
For Linux, macOS, or Unix:

```bash
aws rds create-db-instance --db-instance-identifier sample-instance-us-west-2a --db-cluster-identifier sample-cluster --engine aurora --db-instance-class db.r4.large
  --availability-zone us-west-2a
```

For Windows:

```bash
aws rds create-db-instance --db-instance-identifier sample-instance-us-west-2a
  --db-cluster-identifier sample-cluster --engine aurora --db-instance-class db.r4.large
  --availability-zone us-west-2a
```

The following command creates a new PostgreSQL-compatible Aurora Replica named `sample-instance-us-west-2a`.

For Linux, macOS, or Unix:

```bash
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.r4.large
  --availability-zone us-west-2a
```

For Windows:

```bash
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.r4.large
  --availability-zone us-west-2a
```

**RDS API**

To create an Aurora Replica in your DB cluster, call the `CreateDBInstance` operation. Include the name of the DB cluster as the `DBClusterIdentifier` parameter. You can optionally specify an `AvailabilityZone` for the Aurora Replica using the `AvailabilityZone` parameter.
Managing performance and scaling for Aurora DB clusters

You can use the following options to manage performance and scaling for Aurora DB clusters and DB instances:

Topics

- Storage scaling (p. 349)
- Instance scaling (p. 353)
- Read scaling (p. 353)
- Managing connections (p. 353)
- Managing query execution plans (p. 354)

Storage scaling

Aurora storage automatically scales with the data in your cluster volume. As your data grows, your cluster volume storage expands up to a maximum of 128 tebibytes (TiB). To learn what kinds of data are included in the cluster volume, see Amazon Aurora storage and reliability (p. 51).

The size of your cluster volume is evaluated on an hourly basis to determine your storage costs. For pricing information, see the Aurora pricing page.

Even though an Aurora cluster volume can scale up in size to many tebibytes, you are only charged for the space that you use in the volume. The mechanism for determining billed storage space depends on the version of your Aurora cluster.

- When Aurora data is removed from the cluster volume, the overall billed space decreases by a comparable amount. This dynamic resizing behavior happens when underlying database files are deleted or reorganized to require less space. Thus, you can reduce storage charges by deleting tables, indexes, databases, and so on that you no longer need. Dynamic resizing applies to certain Aurora versions. The following are the minimum Aurora versions where the cluster volume dynamically resizes as you delete data:
  - Aurora MySQL 2.09 (compatible with MySQL 5.7)
  - Aurora MySQL 1.23 (compatible with MySQL 5.6)
  - Aurora PostgreSQL 3.3.0 (compatible with PostgreSQL 11.8)
  - Aurora PostgreSQL 2.6.0 (compatible with PostgreSQL 10.13)
- In Aurora versions lower than those in the preceding list, the cluster volume can reuse space that was freed up when you deleted data, but the volume itself never decreases in size.
- This feature is being deployed in phases to the AWS Regions where Aurora is available. Depending on the Region where your cluster is, this feature might not be available yet.

Dynamic resizing applies to operations that physically remove or resize data files within the cluster volume. Thus, it applies to SQL statements such as DROP TABLE, DROP DATABASE, and TRUNCATE TABLE. It doesn't apply to deleting rows using the DELETE statement. If you delete a large number of rows from a table, you can run the Aurora MySQL OPTIMIZE TABLE statement or the Aurora PostgreSQL VACUUM statement afterward to reorganize the table and dynamically resize the cluster volume.

Note
For Aurora MySQL, the innodb_file_per_table affects how table storage is organized. When tables are part of the system tablespace, dropping the table doesn't reduce the size of the
system tablespace. Thus, make sure to use the setting `innodb_file_per_table=1` for Aurora MySQL clusters to take full advantage of dynamic resizing.

These Aurora versions also have a higher storage limit for the cluster volume than lower versions do. Thus, you can consider upgrading to one of these versions if you are close to exceeding the original 64 TiB volume size.

You can check how much storage space a cluster is using by monitoring the `VolumeBytesUsed` metric in CloudWatch.

- In the AWS Management Console, you can see this figure in a chart by viewing the Monitoring tab on the details page for the cluster.
- With the AWS CLI, you can run a command similar to the following Linux example. Substitute your own values for the start and end times and the name of the cluster.

```bash
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"
```

That command produces output similar to the following.

```json
{
  "Label": "VolumeBytesUsed",
  "Datapoints": [
    {
      "Timestamp": "2020-08-04T21:25:00+00:00",
      "Average": 182871982080.0,
      "Minimum": 182871982080.0,
      "Maximum": 182871982080.0,
      "Unit": "Bytes"
    }
  ]
}
```

The following examples show how you might track storage usage for an Aurora cluster over time using AWS CLI commands on a Linux system. The `--start-time` and `--end-time` parameters define the overall time interval as one day. The `--period` parameter requests the measurements at one hour intervals. It doesn't make sense to choose a `--period` value that's small, because the metrics are collected at intervals, not continuously. Also, Aurora storage operations sometimes continue for some time in the background after the relevant SQL statement finishes.

The first example returns output in the default JSON format. The data points are returned in arbitrary order, not sorted by timestamp. You might import this JSON data into a charting tool to do sorting and visualization.

```bash
# 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”: 18287522752.0,
"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 ...

This example returns the same data as the previous one. The --output parameter represents the data in compact plain text format. The aws cloudwatch command pipes its output to the sort command. The -k parameter of the sort command sorts the output by the third field, which is the timestamp in Universal Coordinated Time (UTC) format.

$ 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 18287522752.0 2020-08-04T17:41:00+00:00 Bytes
DATAPOINTS 18287522752.0 2020-08-04T18:41:00+00:00 Bytes
DATAPOINTS 18287522752.0 2020-08-04T19:41:00+00:00 Bytes
DATAPOINTS 18287522752.0 2020-08-04T20:41:00+00:00 Bytes
DATAPOINTS 18287522752.0 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

The sorted output shows how much storage was used at the start and end of the monitoring period. You can also find the points during that period when Aurora allocated more storage for the cluster. The following example uses Linux commands to reformat the starting and ending VolumeBytesUsed values as gigabytes (GB) and as gibibytes (GiB). Gigabytes represent units measured in powers of 10 and are commonly used in discussions of storage for rotational hard drives. Gibibytes represent units measured...
in powers of 2. Aurora storage measurements and limits are typically stated in the power-of-2 units, such as gibibytes and tebibytes.

```bash
$ 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
```

The `VolumeBytesUsed` metric tells you how much storage in the cluster is incurring charges. Thus, it's best to minimize this number when practical. However, this metric doesn't include some storage that Aurora uses internally in the cluster and doesn't charge for. If your cluster is approaching the storage limit and might run out of space, it's more helpful to monitor the `AuroraVolumeBytesLeftTotal` metric and try to maximize that number. The following example runs a similar calculation as the previous one, but for `AuroraVolumeBytesLeftTotal` instead of `VolumeBytesUsed`. You can see that the free size for this cluster reflects the original 64 TiB limit, because the cluster is running Aurora MySQL version 1.22.

```bash
$ awk 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 907791344384.0 2020-08-05T12:52:00+00:00 Count
DATAPOINTS 907791344384.0 2020-08-05T13:52:00+00:00 Count
$ TiB=($(1024*1024*1024*1024))
$ TB=($(1000*1000*1000*1000))
$ echo "$(90779067915264 / $TB) TB remaining for this cluster"
69 TB remaining for this cluster
$ echo "$(90779067915264 / $TiB) TiB remaining for this cluster"
63 TiB remaining for this cluster
```

For a cluster running Aurora MySQL version 1.23 or 2.09 and higher, or Aurora PostgreSQL 3.3.0 or 2.6.0 and higher, the free size reported by `VolumeBytesUsed` increases when data is added and decreases when data is removed. The following example shows how. This report shows the maximum and minimum storage size for a cluster at 15-minute intervals as tables with temporary data are created and dropped. The report lists the maximum value before the minimum value. Thus, to understand how storage usage changed within the 15-minute interval, interpret the numbers from right to left.

```bash
$ awk 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 2020-08-05T20:19:00+00:00 Bytes
DATAPOINTS 14545305600.0 14545305600.0 2020-08-05T21:19:00+00:00 Bytes
DATAPOINTS 14545305600.0 14545305600.0 2020-08-05T22:19:00+00:00 Bytes
DATAPOINTS 14545305600.0 14545305600.0 2020-08-05T23:19:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-06T00:19:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-06T01:19:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-06T02:19:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-06T03:19:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-06T04:19:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-06T05:19:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-06T06:19:00+00:00 Bytes
```

352
The following example shows how with a cluster running Aurora MySQL version 1.23 or 2.09 and higher, or Aurora PostgreSQL 3.3.0 or 2.6.0 and higher, the free size reported by AuroraVolumeBytesLeftTotal reflects the higher 128 TiB size limit.

```
$ 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
```

```
<table>
<thead>
<tr>
<th>DATAPOINTS</th>
<th>140515818864640.0 2020-08-05T20:56:00+00:00</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATAPOINTS</td>
<td>140515818864640.0 2020-08-05T21:26:00+00:00</td>
<td>Count</td>
</tr>
<tr>
<td>DATAPOINTS</td>
<td>140515818864640.0 2020-08-05T21:56:00+00:00</td>
<td>Count</td>
</tr>
<tr>
<td>DATAPOINTS</td>
<td>140514866757632.0 2020-08-05T22:26:00+00:00</td>
<td>Count</td>
</tr>
<tr>
<td>DATAPOINTS</td>
<td>140511020580864.0 2020-08-05T22:56:00+00:00</td>
<td>Count</td>
</tr>
<tr>
<td>DATAPOINTS</td>
<td>140503168843776.0 2020-08-05T23:26:00+00:00</td>
<td>Count</td>
</tr>
<tr>
<td>DATAPOINTS</td>
<td>140503168843776.0 2020-08-05T23:56:00+00:00</td>
<td>Count</td>
</tr>
<tr>
<td>DATAPOINTS</td>
<td>140515818864640.0 2020-08-06T00:26:00+00:00</td>
<td>Count</td>
</tr>
</tbody>
</table>
```

```
$ 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
```

### Instance scaling

You can scale your Aurora DB cluster as needed by modifying the DB instance class for each DB instance in the DB cluster. Aurora supports several DB instance classes optimized for Aurora, depending on database engine compatibility.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instance scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Aurora MySQL</td>
<td>See Scaling Aurora MySQL DB instances (p. 675)</td>
</tr>
<tr>
<td>Amazon Aurora PostgreSQL</td>
<td>See Scaling Aurora PostgreSQL DB instances (p. 1028)</td>
</tr>
</tbody>
</table>

### Read scaling

You can achieve read scaling for your Aurora DB cluster by creating up to 15 Aurora Replicas in a DB cluster that uses single-master replication. Each Aurora Replica returns the same data from the cluster volume with minimal replica lag—usually considerably less than 100 milliseconds after the primary instance has written an update. As your read traffic increases, you can create additional Aurora Replicas and connect to them directly to distribute the read load for your DB cluster. Aurora Replicas don't have to be of the same DB instance class as the primary instance.

For information about adding Aurora Replicas to a DB cluster, see Adding Aurora replicas to a DB cluster (p. 345).

### Managing connections

The maximum number of connections allowed to an Aurora DB instance is determined by the max_connections parameter in the instance-level parameter group for the DB instance. The default value of that parameter varies depending on the DB instance class used for the DB instance and database engine compatibility.
Managing query execution plans

If you use query plan management for Aurora PostgreSQL, you gain control over which plans the optimizer runs. For more information, see Managing query execution plans for Aurora PostgreSQL (p. 1049).

<table>
<thead>
<tr>
<th>Database engine</th>
<th>max_connections default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Aurora MySQL</td>
<td>See Maximum connections to an Aurora MySQL DB instance (p. 675)</td>
</tr>
<tr>
<td>Amazon Aurora PostgreSQL</td>
<td>See Maximum connections to an Aurora PostgreSQL DB instance (p. 1028)</td>
</tr>
</tbody>
</table>
Cloning an Aurora DB cluster volume

Using the Aurora cloning feature, you can quickly and cost-effectively create a new cluster containing a duplicate of an Aurora cluster volume and all its data. We refer to the new cluster and its associated cluster volume as a clone. Creating a clone is faster and more space-efficient than physically copying the data using a different technique such as restoring a snapshot.

Tip
If you aren’t familiar with the Aurora cluster volume and what kinds of data it holds, you can learn more about it by reading Overview of Aurora storage (p. 51).

Topics
• Overview of Aurora cloning (p. 355)
• Limitations of Aurora cloning (p. 356)
• Copy-on-write protocol for Aurora cloning (p. 356)
• Deleting a source cluster volume (p. 358)
• Creating an Aurora clone through the AWS Management Console (p. 358)
• Creating an Aurora clone through the AWS CLI (p. 358)
• Cross-account cloning (p. 359)

Overview of Aurora cloning

Aurora cloning uses a copy-on-write protocol. With this mechanism, a clone requires only minimal additional space when first created. In the beginning, Aurora maintains a single copy of the data, which is used by both the original and new DB clusters. Aurora allocates new storage only when data changes, either on the source cluster or the cloned cluster. You can make multiple clones from the same DB cluster. You can also create additional clones from other clones. For more information on how the copy-on-write protocol works in the context of Aurora storage, see Copy-on-write protocol for Aurora cloning (p. 356).

You can use cloning in a variety of use cases, especially where you don’t want to have an impact on your production environment. Some examples are the following:

• Experiment with and assess the impact of changes, such as schema changes or parameter group changes.
• Perform workload-intensive operations, such as exporting data or running analytical queries.
• Create a copy of a production DB cluster in a nonproduction environment for development or testing.

Many of those use cases involve short-lived clones. In these cases, you run tests or query-intensive jobs without causing overhead on the original cluster. Then you delete the clone when that work is finished. If either the original cluster or the cloned cluster have a high volume of write operations, the underlying storage diverges over time, reducing the efficiency advantage of cloning. You can create a new clone if you need to perform similar work on the data later.

Tip
The cloned cluster starts with either one or zero associated DB instances. Creating a clone using the AWS Management Console produces a cluster with a single DB instance. Creating a clone using the AWS CLI or the RDS API produces an empty cluster with no associated DB instances. You can configure the DB instances of the clone differently than the original cluster to match the requirements of the workload for the clone. For example, the cloned cluster might not have the same high availability requirements as the original. In that case, you might use multiple DB instances for the original cluster but only a single DB instance for the clone.
Limitations of Aurora cloning

There are some limitations involved with Aurora cloning, described following:

- Cloning isn't currently supported for Aurora Serverless v1 DB clusters.
- You cannot create clones across AWS Regions. Each clone must be created in the same Region as the source cluster.
- Currently, you are limited to 15 clones based on a copy, including clones based on other clones. After that, only copies can be created. However, each copy can also have up to 15 clones.
- Currently, you cannot clone from a cluster without the parallel query feature, to a cluster where parallel query is enabled. To bring data into a cluster that uses parallel query, create a snapshot of the original cluster and restore it to a cluster where the parallel query option is enabled.
- You can’t create clones from clusters that have no DB instances. Cloning works only for clusters that have at least one database instance.
- You can provide a different virtual private cloud (VPC) for your clone. However, the subnets in those VPCs must map to the same set of Availability Zones.

Copy-on-write protocol for Aurora cloning

The following scenarios illustrate how the copy-on-write protocol works.

Topics
- Before cloning (p. 356)
- After cloning (p. 356)
- When a change occurs on the source cluster volume (p. 357)
- When a change occurs on the clone (p. 357)

Before cloning

Data in a source cluster volume is stored in pages. In the following diagram, the source cluster volume has four pages.

![Diagram showing source database and pages 1 to 4]

After cloning

As shown in the following diagram, there are no changes in the source data after cloning. Both the source cluster volume and the clone point to the same four pages. None of the pages has been physically copied, so no additional storage is required.
When a change occurs on the source cluster volume

In the following example, the source cluster volume makes a change to the data in Page 1. Instead of writing to the original Page 1, additional storage is used to create a new page, called Page 1'. The source cluster volume now points to the new Page 1', and also to Page 2, Page 3, and Page 4. The clone continues to point to Page 1 through Page 4.

When a change occurs on the clone

In the following diagram, the clone cluster volume has also made a change, this time in Page 4. Instead of writing to the original Page 4, additional storage is used to create a new page, called Page 4'. The source cluster volume continues to point to Page 1', and also Page 2 through Page 4, but the clone now points to Page 1 through Page 3, and also Page 4'.
As shown in the second scenario, after cloning there is no additional storage required at the point of clone creation. However, as changes occur in the source cluster volume and the clone, only the changed pages are created, as shown in the third and fourth scenarios. As more changes occur over time in both the source cluster volume and the clone, you need incrementally more storage to capture and store the changes.

Deleting a source cluster volume

When you delete a source cluster volume that has one or more clones associated with it, the clones are not affected. The clones continue to point to the pages that were previously owned by the source cluster volume.

Creating an Aurora clone through the AWS Management Console

The following procedure describes how to clone an Aurora DB cluster using the AWS Management Console.

These instructions apply for DB clusters owned by the same AWS account that is creating the clone. If the DB cluster is owned by a different AWS account, see Cross-account cloning (p. 359) instead.

To create a clone of a DB cluster owned by your AWS account using the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases. Choose the DB cluster that you want to create a clone of.
3. For Actions, choose Create clone.
4. On the Create clone page, type a name for the primary instance of the clone DB cluster as the DB instance identifier.
   If you want to, set any other settings for the clone DB cluster. For information about the different DB cluster settings, see New console (p. 119).
5. Choose Create clone to launch the clone DB cluster.

Creating an Aurora clone through the AWS CLI

The following procedure describes how to create an Aurora clone using the AWS CLI.

To create a clone using the AWS CLI

- Call the `restore-db-cluster-to-point-in-time` AWS CLI command and supply the following values:
  - `--source-db-cluster-identifier` – the name of the source DB cluster to create a clone of.
  - `--db-cluster-identifier` – the name of the clone DB cluster.
  - `--restore-type copy-on-write` – values that indicate to create a clone DB cluster.
  - `--use-latest-restorable-time` – specifies that the latest restorable backup time is used.

The following example creates a clone of the DB cluster named `sample-source-cluster`. The name of the clone DB cluster is `sample-cluster-clone`.

For Linux, macOS, or Unix:
Cross-account cloning

With Amazon Aurora, you can share an Aurora DB cluster with another AWS account or AWS organization. By sharing this way, you can clone the DB cluster and access the clone from the other account or organization.

For example, if you use separate accounts for production and testing, you can create a clone of production data in your test account. You can use this clone to experiment with different parameters and run expensive online analytical processing (OLAP) queries, all without having an impact on the production environment. You can give outside companies access to your database, for example for
an external vendor to train a machine learning model. Cross-account cloning is much faster in such situations than creating and restoring a database snapshot.

To authorize sharing, you use AWS Resource Access Manager (AWS RAM). For more information about controlling access through AWS RAM, see the AWS RAM User Guide.

Creating a cross-account clone requires actions from the AWS account that owns the original cluster, and the AWS account that creates the clone. First, the owner modifies the cluster to allow one or more other accounts to clone it. If any of the accounts are in a different AWS organization, AWS generates a sharing invitation and the other account must accept the invitation before proceeding. Then each authorized account can clone the cluster. Throughout this process, the cluster is identified by its unique Amazon Resource Name (ARN).

You're only charged for additional storage space if you make data changes. If the source cluster is deleted, storage costs are distributed equally among remaining cloned clusters.

**Topics**
- Limitations of cross-account cloning (p. 360)
- Allowing other AWS accounts to clone your cluster (p. 360)
- Cloning a cluster owned by another AWS account (p. 363)

**Limitations of cross-account cloning**

Aurora cross-account cloning has the following limitations:

- You can't clone an Aurora Serverless cluster across AWS accounts.
- Viewing and accepting sharing invitations requires using the AWS CLI the Amazon RDS API, or the AWS RAM console. Currently, you can't perform this procedure using the Amazon RDS console.
- When you make a cross-account cluster, you can't make additional clones of that new cluster or share the cloned cluster with other AWS accounts.
- The maximum number of cross-account clones that you can have for any Aurora cluster is 15.
- Your cluster must be in `ACTIVE` state at the time that you share it with other AWS accounts.
- While an Aurora cluster is shared with other AWS accounts, you can't rename the cluster.
- You can't create a cross-account clone of a cluster that is encrypted with the default RDS key.
- When an encrypted cluster is shared with you, you must encrypt the cloned cluster. The key you use can be different from the encryption key for the original cluster. The cluster owner must also grant you permission to access the AWS Key Management Service (AWS KMS) customer master key (CMK) for the original cluster.

**Allowing other AWS accounts to clone your cluster**

To allow other AWS accounts to clone a cluster that you own, use AWS RAM to set the sharing permission. Doing so also sends an invitation to each of the other accounts that's in a different AWS organization.

For the procedures to share resources owned by you in the AWS RAM console, see Sharing resources owned by you in the AWS RAM User Guide.

**Topics**
- Granting permission to other AWS accounts to clone your cluster (p. 361)
- Checking if a cluster you own is shared with other AWS accounts (p. 362)
Granting permission to other AWS accounts to clone your cluster

If the cluster that you're sharing is encrypted, you also share the customer master key (CMK) for the cluster. You can allow AWS Identity and Access Management (IAM) users or roles in one AWS account to use a CMK in a different account. To do this, you first add the external account (root user) to the CMK's key policy through AWS KMS. You don't add the individual IAM users or roles to the key policy, only the external account that owns them. You can only share a CMK that you create, not the default RDS service key. For information about access control for CMKs, see Authentication and access control for AWS KMS.

Console

To grant permission to clone your cluster using the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the DB cluster that you want to share to see its Details page, and choose the Connectivity & security tab.
4. In the Share DB cluster with other AWS accounts section, enter the numeric account ID for the AWS account that you want to allow to clone this cluster. For account IDs in the same organization, you can begin typing in the box and then choose from the menu.
   
   Important
   In some cases, you might want an account that is not in the same AWS organization as your account to clone a cluster. In these cases, for security reasons the AWS Management Console doesn't report who owns that account ID or whether the account exists.
   Be careful entering account numbers that are not in the same AWS organization as your AWS account. Immediately verify that you shared with the intended account.
5. On the confirmation page, verify that the account ID that you specified is correct. Enter share in the confirmation box to confirm.

On the Details page, an entry appears showing the specified AWS account ID under Accounts that this DB cluster is shared with. The Status column initially shows a status of Pending.
6. Contact the owner of the other AWS account, or sign in to that account if you own both of them. Instruct the owner of the other account to accept the sharing invitation and clone the DB cluster, as described following.

AWS CLI

To grant permission to clone your cluster using the AWS CLI

1. Gather the information for the required parameters. You need the ARN for your cluster and the numeric ID for the other AWS account.
2. Run the RAM CLI command create-resource-share.

   For Linux, macOS, or Unix:
   
   ```bash
   aws ram create-resource-share --name descriptive_name \  
   --region region \  
   --resource-arns cluster_arn \  
   --principals other_account_ids
   ```
   
   For Windows:
   
   ```bash
   ```

361
aws ram create-resource-share --name descriptive_name ^
  --region region ^
  --resource-arns cluster_arn ^
  --principals other_account_ids

To include multiple account IDs for the --principals parameter, separate IDs from each other with spaces. To specify whether the permitted account IDs can be outside your AWS organization, include the --allow-external-principals or --no-allow-external-principals parameter for create-resource-share.

RAM API

To grant permission to clone your cluster using the RAM API

1. Gather the information for the required parameters. You need the ARN for your cluster and the numeric ID for the other AWS account.
2. Call the RAM API operation CreateResourceShare, and specify the following values:
   - Specify the account IDs of one or more AWS accounts as the principals parameter.
   - Specify the ARNs of one or more Aurora DB clusters as the resourceArns parameter.
   - Specify whether the permitted account IDs can be outside your AWS organization or not by including a Boolean value for the allowExternalPrincipals parameter.

Recreating a cluster that uses default RDS key

To recreate an encrypted cluster that uses the default RDS key

If the encrypted cluster that you intend to share uses the default RDS key, you must recreate it using a customer master key (CMK) and share the new cluster instead. You do so by creating a manual snapshot of your DB cluster and restoring it to a new cluster. Use the following steps.

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Snapshots from the navigation pane.
3. Choose your snapshot.
4. For Actions, choose Copy Snapshot, and then choose Enable encryption.
5. For Master key, choose the new encryption key that you want to use.
6. Restore the copied snapshot. To do so, follow the procedure in Restoring from a DB cluster snapshot (p. 420). The new DB instance uses your new encryption key.
7. (Optional) Delete the old DB cluster if you no longer need it. To do so, follow the procedure in Deleting a DB cluster snapshot (p. 457). Before you do, confirm that your new cluster has all necessary data and that your application can access it successfully.

Checking if a cluster you own is shared with other AWS accounts

You can check if other users have permission to share a cluster. Doing so can help you understand whether the cluster is approaching the limit for the maximum number of cross-account clones.

For the procedures to share resources using the AWS RAM console, see Sharing resources owned by you in the AWS RAM User Guide.
AWS CLI

To find out if a cluster you own is shared with other AWS accounts using the AWS CLI

- Call the RAM CLI command `list-principals`, using your account ID as the resource owner and the ARN of your cluster as the resource ARN. You can see all shares with the following command. The results indicate which AWS accounts are allowed to clone the cluster.

```
aws ram list-principals \
  --resource-arns your_cluster_arn \
  --principals your_aws_id
```

RAM API

To find out if a cluster you own is shared with other AWS accounts using the RAM API

- Call the RAM API operation `ListPrincipals`. Use your account ID as the resource owner and the ARN of your cluster as the resource ARN.

Cloning a cluster owned by another AWS account

To clone a cluster that's owned by another AWS account, use AWS RAM to get permission to make the clone. After you have the required permission, you use the standard procedure for cloning an Aurora cluster.

You can also check whether a cluster that you own is a clone of a cluster owned by a different AWS account.

For the procedures to work with resources owned by others in the AWS RAM console, see Accessing resources shared with you in the AWS RAM User Guide.

Topics

- Viewing invitations to clone clusters owned by other AWS accounts (p. 363)
- Accepting invitations to share clusters owned by other AWS accounts (p. 364)
- Cloning an Aurora cluster owned by another AWS account (p. 365)
- Checking if a DB cluster is a cross-account clone (p. 368)

Viewing invitations to clone clusters owned by other AWS accounts

To work with invitations to clone clusters owned by AWS accounts in other AWS organizations, use the AWS CLI, the AWS RAM console, or the AWS RAM API. Currently, you can't perform this procedure using the Amazon RDS console.

For the procedures to work with invitations in the AWS RAM console, see Accessing resources shared with you in the AWS RAM User Guide.

AWS CLI

To see invitations to clone clusters owned by other AWS accounts using the AWS CLI

1. Run the RAM CLI command `get-resource-share-invitations`. 

aws ram get-resource-share-invitations --region region_name

The results from the preceding command show all invitations to clone clusters, including any that you already accepted or rejected.

2. (Optional) Filter the list so you see only the invitations that require action from you. To do so, add the parameter --query 'resourceShareInvitations[?status==`PENDING`]'.

**RAM API**

To see invitations to clone clusters owned by other AWS accounts using the RAM API

1. Call the RAM API operation GetResourceShareInvitations. This operation returns all such invitations, including any that you already accepted or rejected.
2. (Optional) Find only the invitations that require action from you by checking the resourceShareAssociations return field for a status value of PENDING.

**Accepting invitations to share clusters owned by other AWS accounts**

You can accept invitations to share clusters owned by other AWS accounts that are in different AWS organizations. To work with these invitations, use the AWS CLI, the RAM and RDS APIs, or the RAM console. Currently, you can't perform this procedure using the RDS console.

For the procedures to work with invitations in the AWS RAM console, see Accessing resources shared with you in the AWS RAM User Guide.

**Console**

To accept an invitation to share a cluster from another AWS account using the AWS CLI

1. Find the invitation ARN by running the RAM CLI command get-resource-share-invitations, as shown preceding.
2. Accept the invitation by calling the RAM CLI command accept-resource-share-invitation, as shown following.

   For Linux, macOS, or Unix:

   ```
   aws ram accept-resource-share-invitation \
   --resource-share-invitation-arn invitation_arn \ 
   --region region
   ```

   For Windows:

   ```
   aws ram accept-resource-share-invitation ^ 
   --resource-share-invitation-arn invitation_arn ^ 
   --region region
   ```

**RAM and RDS API**

To accept invitations to share somebody's cluster using the RAM and RDS APIs

1. Find the invitation ARN by calling the RAM API operation GetResourceShareInvitations, as shown preceding.
2. Pass that ARN as the resourceShareInvitationArn parameter to the RDS API operation AcceptResourceShareInvitation.

Cloning an Aurora cluster owned by another AWS account

After you accept the invitation from the AWS account that owns the DB cluster, as shown preceding, you can clone the cluster.

Console

To clone an Aurora cluster owned by another AWS account using the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
   - At the top of the database list, you should see one or more items with a Role value of Shared from account #account_id#. For security reasons, you can only see limited information about the original clusters. The properties that you can see are the ones such as database engine and version that must be the same in your cloned cluster.
3. Choose the cluster that you intend to clone.
4. For Actions, choose Create clone.
5. Follow the procedure in Creating an Aurora clone through the AWS Management Console (p. 358) to finish setting up the cloned cluster.
6. As needed, enable encryption for the cloned cluster. If the cluster that you are cloning is encrypted, you must enable encryption for the cloned cluster. The AWS account that shared the cluster with you must also share the AWS KMS customer master key (CMK) that was used to encrypt the cluster. You can use the same CMK to encrypt the clone, or your own CMK. You can't create a cross-account clone for a cluster that is encrypted with the default RDS CMK.

   The account owning the encryption key must grant permission to use the key to the destination account by using a key policy. This process is similar to how encrypted snapshots are shared, by using a key policy that grants permission to the destination account to use the key.

AWS CLI

To clone an Aurora cluster owned by another AWS account using the AWS CLI

1. Accept the invitation from the AWS account that owns the DB cluster, as shown preceding.
2. Clone the cluster by specifying the full ARN of the source cluster in the source-db-cluster-identifier parameter of the RDS CLI command restore-db-cluster-to-point-in-time, as shown following.

   If the ARN passed as the source-db-cluster-identifier hasn't been shared, the same error is returned as if the specified cluster doesn't exist.

   For Linux, macOS, or Unix:

   ```bash
   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. If the cluster that you are cloning is encrypted, encrypt your cloned cluster by including a `kms-key-id` parameter. This `kms-key-id` value can be the same one used to encrypt the original DB cluster, or your own customer master key (CMK). Your account must have permission to use that encryption key.

For 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. If the cluster that you are cloning is encrypted, encrypt your cloned cluster by including a `kms-key-id` parameter. This `kms-key-id` value can be the same one used to encrypt the original DB cluster, or your own customer master key (CMK). Your account must have permission to use that encryption key.

For Linux, macOS, or Unix:

```
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
```

For 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
```

The account owning the encryption key must grant permission to use the key to the destination account by using a key policy. This process is similar to how encrypted snapshots are shared, by using a key policy that grants permission to the destination account to use the key. An example of a key policy follows.

```
{
  "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": "*"
    }
  ]
}
```
Note
The `restore-db-cluster-to-point-in-time` AWS CLI command only restores the DB cluster, not the DB instances for that DB cluster. You must invoke the `create-db-instance` command to create DB instances for the restored DB cluster, specifying the identifier of the restored DB cluster in `--db-cluster-identifier`. You can create DB instances only after the `restore-db-cluster-to-point-in-time` command has completed and the DB cluster is available.

RDS API

To clone an Aurora cluster owned by another AWS account using the RDS API

1. Accept the invitation from the AWS account that owns the DB cluster, as shown preceding.
2. Clone the cluster by specifying the full ARN of the source cluster in the `SourceDBClusterIdentifier` parameter of the RDS API operation `RestoreDBClusterToPointInTime`.

   If the ARN passed as the `SourceDBClusterIdentifier` hasn't been shared, then the same error is returned as if the specified cluster doesn't exist.

3. If the cluster that you are cloning is encrypted, include a `KmsKeyId` parameter to encrypt your cloned cluster. This `kms-key-id` value can be the same one used to encrypt the original DB cluster, or your own customer master key (CMK). Your account must have permission to use that encryption key.

   When cloning a volume, the destination account must have permission to use the encryption key used to encrypt the source cluster. Aurora encrypts the new cloned cluster with the encryption key specified in `KmsKeyId`.

   The account owning the encryption key must grant permission to use the key to the destination account by using a key policy. This process is similar to how encrypted snapshots are shared, by using a key policy that grants permission to the destination account to use the key. An example of a key policy follows.

   ```json
   {
   "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:ListGrants",
   "kms:RevokeGrant"
   ],
   "Resource": "*",
   "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
   }
   ]
   }
   ```
Cross-account cloning

The RestoreDBClusterToPointInTime RDS API operation only restores the DB cluster, not the DB instances for that DB cluster. You must invoke the CreateDBInstance RDS API operation to create DB instances for the restored DB cluster, specifying the identifier of the restored DB cluster in `DBClusterIdentifier`. You can create DB instances only after the RestoreDBClusterToPointInTime operation has completed and the DB cluster is available.

Checking if a DB cluster is a cross-account clone

The `DBClusters` object identifies whether each cluster is a cross-account clone. You can see the clusters that you have permission to clone by using the `include-shared` option when you run the RDS CLI command `describe-db-clusters`. However, you can't see most of the configuration details for such clusters.

**AWS CLI**

**To check if a DB cluster is a cross-account clone using the AWS CLI**

- Call the RDS CLI command `describe-db-clusters`.

The following example shows how actual or potential cross-account clone DB clusters appear in `describe-db-clusters` output. For existing clusters owned by your AWS account, the `CrossAccountClone` field indicates whether the cluster is a clone of a DB cluster that is owned by another AWS account.

In some cases, an entry might have a different AWS account number than yours in the `DBClusterArn` field. In this case, that entry represents a cluster that is owned by a different AWS account and that you can clone. Such entries have few fields other than `DBClusterArn`. When
creating the cloned cluster, specify the same StorageEncrypted, Engine, and EngineVersion values as in the original cluster.

```bash
$ aws rds describe-db-clusters --include-shared --region us-east-1
{
    "DBClusters": [
    {
        "Engine": "aurora",
        "EngineVersion": "5.6.10a",
        "CrossAccountClone": false,
        ...
    },
    {
        "EarliestRestorableTime": "2019-04-09T16:01:07.398Z",
        "Engine": "aurora",
        "EngineVersion": "5.6.10a",
        "CrossAccountClone": true,
        ...
    },
    {
        "StorageEncrypted": false,
        "Engine": "aurora",
        "EngineVersion": "5.6.10a",
    }
    ]
}
```

**RDS API**

**To check if a DB cluster is a cross-account clone using the RDS API**

- Call the RDS API operation `DescribeDBClusters`.

For existing clusters owned by your AWS account, the `CrossAccountClone` field indicates whether the cluster is a clone of a DB cluster owned by another AWS account. Entries with a different AWS account number in the `DBClusterArn` field represent clusters that you can clone and that are owned by other AWS accounts. These entries have few fields other than `DBClusterArn`. When creating the cloned cluster, specify the same `StorageEncrypted`, `Engine`, and `EngineVersion` values as in the original cluster.

The following example shows a return value that demonstrates both actual and potential cloned clusters.

```json
{
    "DBClusters": [
    {
        "Engine": "aurora",
        "EngineVersion": "5.6.10a",
        "CrossAccountClone": false,
        ...
    },
    {
        "EarliestRestorableTime": "2019-04-09T16:01:07.398Z",
        "Engine": "aurora",
        "EngineVersion": "5.6.10a",
        "CrossAccountClone": true,
        ...
    },
    {
        "StorageEncrypted": false,
        "Engine": "aurora",
        "EngineVersion": "5.6.10a",
    }
    ]
}
```
... },
  { "StorageEncrypted": false,
    "Engine": "aurora",
    "EngineVersion": "5.6.10a"
  }
}
}
Integrating Aurora with other AWS services

Integrate Amazon Aurora with other AWS services so that you can extend your Aurora DB cluster to use additional capabilities in the AWS Cloud.

Topics
- Integrating AWS services with Amazon Aurora MySQL (p. 371)
- Integrating AWS services with Amazon Aurora PostgreSQL (p. 371)
- Using Amazon Aurora Auto Scaling with Aurora replicas (p. 372)
- Using machine learning (ML) capabilities with Amazon Aurora (p. 387)

Integrating AWS services with Amazon Aurora MySQL

Amazon Aurora MySQL integrates with other AWS services so that you can extend your Aurora MySQL DB cluster to use additional capabilities in the AWS Cloud. Your Aurora MySQL DB cluster can use AWS services to do the following:

- Synchronously or asynchronously invoke an AWS Lambda function using the native functions `lambda_sync` or `lambda_async`. Or, asynchronously invoke an AWS Lambda function using the `mysql.lambda_async` procedure.
- Load data from text or XML files stored in an Amazon S3 bucket into your DB cluster using the `LOAD DATA FROM S3` or `LOAD XML FROM S3` command.
- Save data to text files stored in an Amazon S3 bucket from your DB cluster using the `SELECT INTO OUTFILE S3` command.
- Automatically add or remove Aurora Replicas with Application Auto Scaling. For more information, see Using Amazon Aurora Auto Scaling with Aurora replicas (p. 372).

For more information about integrating Aurora MySQL with other AWS services, see Integrating Amazon Aurora MySQL with other AWS services (p. 792).

Integrating AWS services with Amazon Aurora PostgreSQL

Amazon Aurora PostgreSQL integrates with other AWS services so that you can extend your Aurora PostgreSQL DB cluster to use additional capabilities in the AWS Cloud. Your Aurora PostgreSQL DB cluster can use AWS services to do the following:

- Quickly collect, view, and assess performance on your relational database workloads with Performance Insights.
- Automatically add or remove Aurora Replicas with Aurora Auto Scaling. For more information, see Using Amazon Aurora Auto Scaling with Aurora replicas (p. 372).

For more information about integrating Aurora PostgreSQL with other AWS services, see Integrating Amazon Aurora PostgreSQL with other AWS services (p. 1040).
Using Amazon Aurora Auto Scaling with Aurora replicas

To meet your connectivity and workload requirements, Aurora Auto Scaling dynamically adjusts the number of Aurora Replicas provisioned for an Aurora DB cluster using single-master replication. Aurora Auto Scaling is available for both Aurora MySQL and Aurora PostgreSQL. Aurora Auto Scaling enables your Aurora DB cluster to handle sudden increases in connectivity or workload. When the connectivity or workload decreases, Aurora Auto Scaling removes unnecessary Aurora Replicas so that you don’t pay for unused provisioned DB instances.

You define and apply a scaling policy to an Aurora DB cluster. The scaling policy defines the minimum and maximum number of Aurora Replicas that Aurora Auto Scaling can manage. Based on the policy, Aurora Auto Scaling adjusts the number of Aurora Replicas up or down in response to actual workloads, determined by using Amazon CloudWatch metrics and target values.

You can use the AWS Management Console to apply a scaling policy based on a predefined metric. Alternatively, you can use either the AWS CLI or Aurora Auto Scaling API to apply a scaling policy based on a predefined or custom metric.

Topics
- Before you begin (p. 372)
- Aurora Auto Scaling policies (p. 373)
- Adding a scaling policy (p. 374)
- Editing a scaling policy (p. 383)
- Deleting a scaling policy (p. 385)
- DB instance IDs and tagging (p. 386)

Before you begin

Before you can use Aurora Auto Scaling with an Aurora DB cluster, you must first create an Aurora DB cluster with a primary instance and at least one Aurora Replica. Although Aurora Auto Scaling manages Aurora Replicas, the Aurora DB cluster must start with at least one Aurora Replica. For more information about creating an Aurora DB cluster, see Creating an Amazon Aurora DB cluster (p. 118).

Aurora Auto Scaling only scales a DB cluster if all Aurora Replicas in a DB cluster are in the available state. If any of the Aurora Replicas are in a state other than available, Aurora Auto Scaling waits until the whole DB cluster becomes available for scaling.

When Aurora Auto Scaling adds a new Aurora Replica, the new Aurora Replica is the same DB instance class as the one used by the primary instance. For more information about DB instance classes, see DB instance classes (p. 46). Also, the promotion tier for new Aurora Replicas is set to the last priority, which is 15 by default. This means that during a failover, a replica with a better priority, such as one created manually, would be promoted first. For more information, see Fault tolerance for an Aurora DB cluster (p. 56).

Aurora Auto Scaling only removes Aurora Replicas that it created.

To benefit from Aurora Auto Scaling, your applications must support connections to new Aurora Replicas. To do so, we recommend using the Aurora reader endpoint. For Aurora MySQL you can use a driver such as the MariaDB Connector/J utility. For more information, see Connecting to an Amazon Aurora DB cluster (p. 253).
Aurora Auto Scaling policies

Aurora Auto Scaling uses a scaling policy to adjust the number of Aurora Replicas in an Aurora DB cluster. Aurora Auto Scaling has the following components:

- A service-linked role
- A target metric
- Minimum and maximum capacity
- A cooldown period

Service linked role

Aurora Auto Scaling uses the AWSServiceRoleForApplicationAutoScaling_RDSCluster service-linked role. For more information, see Service-linked roles for Application Auto Scaling in the Application Auto Scaling User Guide.

Target metric

In this type of policy, a predefined or custom metric and a target value for the metric is specified in a target-tracking scaling policy configuration. Aurora Auto Scaling creates and manages CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and target value. The scaling policy adds or removes Aurora Replicas as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target-tracking scaling policy also adjusts to fluctuations in the metric due to a changing workload. Such a policy also minimizes rapid fluctuations in the number of available Aurora Replicas for your DB cluster.

For example, take a scaling policy that uses the predefined average CPU utilization metric. Such a policy can keep CPU utilization at, or close to, a specified percentage of utilization, such as 40 percent.

Note
For each Aurora DB cluster, you can create only one Auto Scaling policy for each target metric.

Minimum and maximum capacity

You can specify the maximum number of Aurora Replicas to be managed by Application Auto Scaling. This value must be set to 0–15, and must be equal to or greater than the value specified for the minimum number of Aurora Replicas.

You can also specify the minimum number of Aurora Replicas to be managed by Application Auto Scaling. This value must be set to 0–15, and must be equal to or less than the value specified for the maximum number of Aurora Replicas.

Note
The minimum and maximum capacity are set for an Aurora DB cluster. The specified values apply to all of the policies associated with that Aurora DB cluster.

Cooldown period

You can tune the responsiveness of a target-tracking scaling policy by adding cooldown periods that affect scaling your Aurora DB cluster in and out. A cooldown period blocks subsequent scale-in or scale-out requests until the period expires. These blocks slow the deletions of Aurora Replicas in your Aurora DB cluster for scale-in requests, and the creation of Aurora Replicas for scale-out requests.

You can specify the following cooldown periods:

- A scale-in activity reduces the number of Aurora Replicas in your Aurora DB cluster. A scale-in cooldown period specifies the amount of time, in seconds, after a scale-in activity completes before another scale-in activity can start.
A scale-out activity increases the number of Aurora Replicas in your Aurora DB cluster. A scale-out cooldown period specifies the amount of time, in seconds, after a scale-out activity completes before another scale-out activity can start.

When a scale-in or a scale-out cooldown period is not specified, the default for each is 300 seconds.

Enable or disable scale-in activities

You can enable or disable scale-in activities for a policy. Enabling scale-in activities allows the scaling policy to delete Aurora Replicas. When scale-in activities are enabled, the scale-in cooldown period in the scaling policy applies to scale-in activities. Disabling scale-in activities prevents the scaling policy from deleting Aurora Replicas.

Note
Scale-out activities are always enabled so that the scaling policy can create Aurora Replicas as needed.

Adding a scaling policy

You can add a scaling policy using the AWS Management Console, the AWS CLI, or the Application Auto Scaling API.

Note
For an example that adds a scaling policy using AWS CloudFormation, see Declaring a scaling policy for an Aurora DB cluster in the AWS CloudFormation User Guide.

Topics
- Adding a scaling policy using the AWS Management Console (p. 374)
- Adding a scaling policy using the AWS CLI or the Application Auto Scaling API (p. 377)

Adding a scaling policy using the AWS Management Console

You can add a scaling policy to an Aurora DB cluster by using the AWS Management Console.

To add an auto scaling policy to an Aurora DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the Aurora DB cluster that you want to add a policy for.
4. Choose the Logs & events tab.
5. In the Auto scaling policies section, choose Add.

The Add Auto Scaling policy dialog box appears.
6. For Policy Name, type the policy name.
7. For the target metric, choose one of the following:
   - Average CPU utilization of Aurora Replicas to create a policy based on the average CPU utilization.
   - Average connections of Aurora Replicas to create a policy based on the average number of connections to Aurora Replicas.
8. For the target value, type one of the following:
• If you chose **Average CPU utilization of Aurora Replicas** in the previous step, type the percentage of CPU utilization that you want to maintain on Aurora Replicas.

• If you chose **Average connections of Aurora Replicas** in the previous step, type the number of connections that you want to maintain.

Aurora Replicas are added or removed to keep the metric close to the specified value.

9. (Optional) Open **Additional Configuration** to create a scale-in or scale-out cooldown period.

10. For **Minimum capacity**, type the minimum number of Aurora Replicas that the Aurora Auto Scaling policy is required to maintain.

11. For **Maximum capacity**, type the maximum number of Aurora Replicas the Aurora Auto Scaling policy is required to maintain.

12. Choose **Add policy**.

The following dialog box creates an Auto Scaling policy based an average CPU utilization of 40 percent. The policy specifies a minimum of 5 Aurora Replicas and a maximum of 15 Aurora Replicas.
The following dialog box creates an auto scaling policy based an average number of connections of 100. The policy specifies a minimum of two Aurora Replicas and a maximum of eight Aurora Replicas.
Adding a scaling policy using the AWS CLI or the Application Auto Scaling API

You can apply a scaling policy based on either a predefined or custom metric. To do so, you can use the AWS CLI or the Application Auto Scaling API. The first step is to register your Aurora DB cluster with Application Auto Scaling.

Registering an Aurora DB cluster

Before you can use Aurora Auto Scaling with an Aurora DB cluster, you register your Aurora DB cluster with Application Auto Scaling. You do so to define the scaling dimension and limits to be applied to that cluster. Application Auto Scaling dynamically scales the Aurora DB cluster along the
rds:cluster:ReadReplicaCount scalable dimension, which represents the number of Aurora Replicas.

To register your Aurora DB cluster, you can use either the AWS CLI or the Application Auto Scaling API.

**AWS CLI**

To register your Aurora DB cluster, use the `register-scalable-target` AWS CLI command with the following parameters:

- `--service-namespace` – Set this value to `rds`.
- `--resource-id` – The resource identifier for the Aurora DB cluster. For this parameter, the resource type is `cluster` and the unique identifier is the name of the Aurora DB cluster, for example `cluster:myscalablecluster`.
- `--scalable-dimension` – Set this value to `rds:cluster:ReadReplicaCount`.
- `--min-capacity` – The minimum number of reader DB instances to be managed by Application Auto Scaling. For information about the relationship between `--min-capacity`, `--max-capacity`, and the number of DB instances in your cluster, see Minimum and maximum capacity (p. 373).
- `--max-capacity` – The maximum number of reader DB instances to be managed by Application Auto Scaling. For information about the relationship between `--min-capacity`, `--max-capacity`, and the number of DB instances in your cluster, see Minimum and maximum capacity (p. 373).

**Example**

In the following example, you register an Aurora DB cluster named `myscalablecluster`. The registration indicates that the DB cluster should be dynamically scaled to have from one to eight Aurora Replicas.

For Linux, macOS, or Unix:

```bash
aws application-autoscaling register-scalable-target \
  --service-namespace rds \
  --resource-id cluster:myscalablecluster \
  --scalable-dimension rds:cluster:ReadReplicaCount \
  --min-capacity 1 \
  --max-capacity 8
```

For Windows:

```bash
aws application-autoscaling register-scalable-target ^
  --service-namespace rds ^
  --resource-id cluster:myscalablecluster ^
  --scalable-dimension rds:cluster:ReadReplicaCount ^
  --min-capacity 1 ^
  --max-capacity 8 ^
```

**RDS API**

To register your Aurora DB cluster with Application Auto Scaling, use the `RegisterScalableTarget` Application Auto Scaling API operation with the following parameters:

- `ServiceNamespace` – Set this value to `rds`.
- `ResourceId` – The resource identifier for the Aurora DB cluster. For this parameter, the resource type is `cluster` and the unique identifier is the name of the Aurora DB cluster, for example `cluster:myscalablecluster`. 
• **ScalableDimension** – Set this value to rds:cluster:ReadReplicaCount.
• **MinCapacity** – The minimum number of reader DB instances to be managed by Application Auto Scaling. For information about the relationship between MinCapacity, MaxCapacity, and the number of DB instances in your cluster, see Minimum and maximum capacity (p. 373).
• **MaxCapacity** – The maximum number of reader DB instances to be managed by Application Auto Scaling. For information about the relationship between MinCapacity, MaxCapacity, and the number of DB instances in your cluster, see Minimum and maximum capacity (p. 373).

**Example**

In the following example, you register an Aurora DB cluster named myscalablecluster with the Application Auto Scaling API. This registration indicates that the DB cluster should be dynamically scaled to have from one to eight Aurora Replicas.

```json
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
}
```

**Defining a scaling policy for an Aurora DB cluster**

A target-tracking scaling policy configuration is represented by a JSON block that the metrics and target values are defined in. You can save a scaling policy configuration as a JSON block in a text file. You use that text file when invoking the AWS CLI or the Application Auto Scaling API. For more information about policy configuration syntax, see TargetTrackingScalingPolicyConfiguration in the Application Auto Scaling API Reference.

The following options are available for defining a target-tracking scaling policy configuration.

**Topics**
- Using a predefined metric (p. 379)
- Using a custom metric (p. 380)
- Using cooldown periods (p. 380)
- Disabling scale-in activity (p. 381)

**Using a predefined metric**

By using predefined metrics, you can quickly define a target-tracking scaling policy for an Aurora DB cluster that works well with both target tracking and dynamic scaling in Aurora Auto Scaling.

Currently, Aurora supports the following predefined metrics in Aurora Auto Scaling:

- **RDSReaderAverageCPUUtilization** – The average value of the CPUUtilization metric in CloudWatch across all Aurora Replicas in the Aurora DB cluster.
• **RDSReaderAverageDatabaseConnections** – The average value of the DatabaseConnections metric in CloudWatch across all Aurora Replicas in the Aurora DB cluster.

For more information about the CPUUtilization and DatabaseConnections metrics, see Amazon Aurora metrics (p. 489).

To use a predefined metric in your scaling policy, you create a target tracking configuration for your scaling policy. This configuration must include a PredefinedMetricSpecification for the predefined metric and a TargetValue for the target value of that metric.

**Example**

The following example describes a typical policy configuration for target-tracking scaling for an Aurora DB cluster. In this configuration, the RDSReaderAverageCPUUtilization predefined metric is used to adjust the Aurora DB cluster based on an average CPU utilization of 40 percent across all Aurora Replicas.

```
{
   "TargetValue": 40.0,
   "PredefinedMetricSpecification":
   {
      "PredefinedMetricType": "RDSReaderAverageCPUUtilization"
   }
}
```

**Using a custom metric**

By using custom metrics, you can define a target-tracking scaling policy that meets your custom requirements. You can define a custom metric based on any Aurora metric that changes in proportion to scaling.

Not all Aurora metrics work for target tracking. The metric must be a valid utilization metric and describe how busy an instance is. The value of the metric must increase or decrease in proportion to the number of Aurora Replicas in the Aurora DB cluster. This proportional increase or decrease is necessary to use the metric data to proportionally scale out or in the number of Aurora Replicas.

**Example**

The following example describes a target-tracking configuration for a scaling policy. In this configuration, a custom metric adjusts an Aurora DB cluster based on an average CPU utilization of 50 percent across all Aurora Replicas in an Aurora DB cluster named 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"
   }
}
```

**Using cooldown periods**

You can specify a value, in seconds, for ScaleOutCooldown to add a cooldown period for scaling out your Aurora DB cluster. Similarly, you can add a value, in seconds, for ScaleInCooldown to add a
cooldown period for scaling in your Aurora DB cluster. For more information about ScaleInCooldown and ScaleOutCooldown, see TargetTrackingScalingPolicyConfiguration in the Application Auto Scaling API Reference.

Example

The following example describes a target-tracking configuration for a scaling policy. In this configuration, the RDSReaderAverageCPUUtilization predefined metric is used to adjust an Aurora DB cluster based on an average CPU utilization of 40 percent across all Aurora Replicas in that Aurora DB cluster. The configuration provides a scale-in cooldown period of 10 minutes and a scale-out cooldown period of 5 minutes.

```json
{
  "TargetValue": 40.0,
  "PredefinedMetricSpecification":
  {
    "PredefinedMetricType": "RDSReaderAverageCPUUtilization",
  },
  "ScaleInCooldown": 600,
  "ScaleOutCooldown": 300
}
```

Disabling scale-in activity

You can prevent the target-tracking scaling policy configuration from scaling in your Aurora DB cluster by disabling scale-in activity. Disabling scale-in activity prevents the scaling policy from deleting Aurora Replicas, while still allowing the scaling policy to create them as needed.

You can specify a Boolean value for DisableScaleIn to enable or disable scale in activity for your Aurora DB cluster. For more information about DisableScaleIn, see TargetTrackingScalingPolicyConfiguration in the Application Auto Scaling API Reference.

Example

The following example describes a target-tracking configuration for a scaling policy. In this configuration, the RDSReaderAverageCPUUtilization predefined metric adjusts an Aurora DB cluster based on an average CPU utilization of 40 percent across all Aurora Replicas in that Aurora DB cluster. The configuration disables scale-in activity for the scaling policy.

```json
{
  "TargetValue": 40.0,
  "PredefinedMetricSpecification":
  {
    "PredefinedMetricType": "RDSReaderAverageCPUUtilization",
  },
  "DisableScaleIn": true
}
```

Applying a scaling policy to an Aurora DB cluster

After registering your Aurora DB cluster with Application Auto Scaling and defining a scaling policy, you apply the scaling policy to the registered Aurora DB cluster. To apply a scaling policy to an Aurora DB cluster, you can use the AWS CLI or the Application Auto Scaling API.

AWS CLI

To apply a scaling policy to your Aurora DB cluster, use the `put-scaling-policy` AWS CLI command with the following parameters:

- `--policy-name` - The name of the scaling policy.
- `--policy-type` - Set this value to TargetTrackingScaling.
Using Auto Scaling with Aurora replicas

- --resource-id – The resource identifier for the Aurora DB cluster. For this parameter, the resource type is cluster and the unique identifier is the name of the Aurora DB cluster, for example cluster:my scalable cluster.
- --service-namespace – Set this value to rds.
- --scalable-dimension – Set this value to rds:cluster:Read Replica Count.
- --target-tracking-scaling-policy-configuration – The target-tracking scaling policy configuration to use for the Aurora DB cluster.

Example

In the following example, you apply a target-tracking scaling policy named my scalable policy to an Aurora DB cluster named my scalable cluster with Application Auto Scaling. To do so, you use a policy configuration saved in a file named config.json.

For Linux, macOS, or Unix:

```bash
aws application-autoscaling put-scaling-policy
  --policy-name my scalable policy
  --policy-type TargetTrackingScaling
  --resource-id cluster:my scalable cluster
  --service-namespace rds
  --scalable-dimension rds:cluster:Read Replica Count
  --target-tracking-scaling-policy-configuration file://config.json
```

For Windows:

```bash
aws application-autoscaling put-scaling-policy
  --policy-name my scalable policy
  --policy-type TargetTrackingScaling
  --resource-id cluster:my scalable cluster
  --service-namespace rds
  --scalable-dimension rds:cluster:Read Replica Count
  --target-tracking-scaling-policy-configuration file://config.json
```

RDS API

To apply a scaling policy to your Aurora DB cluster with the Application Auto Scaling API, use the `PutScalingPolicy` Application Auto Scaling API operation with the following parameters:

- PolicyName – The name of the scaling policy.
- ServiceNamespace – Set this value to rds.
- ResourceID – The resource identifier for the Aurora DB cluster. For this parameter, the resource type is cluster and the unique identifier is the name of the Aurora DB cluster, for example cluster:my scalable cluster.
- ScalableDimension – Set this value to rds:cluster:Read Replica Count.
- PolicyType – Set this value to TargetTrackingScaling.
- TargetTrackingScalingPolicyConfiguration – The target-tracking scaling policy configuration to use for the Aurora DB cluster.

Example

In the following example, you apply a target-tracking scaling policy named my scalable policy to an Aurora DB cluster named my scalable cluster with Application Auto Scaling. You use a policy configuration based on the RDS Reader Average CPU Utilization predefined metric.
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"
    }
  }
}

**Editing a scaling policy**

You can edit a scaling policy using the AWS Management Console, the AWS CLI, or the Application Auto Scaling API.

**Editing a scaling policy using the AWS Management Console**

You can edit a scaling policy by using the AWS Management Console.

**To edit an auto scaling policy for an Aurora DB cluster**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Databases**.
3. Choose the Aurora DB cluster whose auto scaling policy you want to edit.
4. Choose the **Logs & events** tab.
5. In the **Auto scaling policies** section, choose the auto scaling policy, and then choose **Edit**.
6. Make changes to the policy.
7. Choose **Save**.

The following is a sample **Edit Auto Scaling policy** dialog box.
Editing a scaling policy using the AWS CLI or the Application Auto Scaling API

You can use the AWS CLI or the Application Auto Scaling API to edit a scaling policy in the same way that you apply a scaling policy:
• When using the AWS CLI, specify the name of the policy you want to edit in the --policy-name parameter. Specify new values for the parameters you want to change.
• When using the Application Auto Scaling API, specify the name of the policy you want to edit in the PolicyName parameter. Specify new values for the parameters you want to change.

For more information, see Applying a scaling policy to an Aurora DB cluster (p. 381).

Deleting a scaling policy

You can delete a scaling policy using the AWS Management Console, the AWS CLI, or the Application Auto Scaling API.

Deleting a scaling policy using the AWS Management Console

You can delete a scaling policy by using the AWS Management Console.

To delete an auto scaling policy for an Aurora DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the Aurora DB cluster whose auto scaling policy you want to delete.
4. Choose the Logs & events tab.
5. In the Auto scaling policies section, choose the auto scaling policy, and then choose Delete.

Deleting a scaling policy using the AWS CLI or the Application Auto Scaling API

You can use the AWS CLI or the Application Auto Scaling API to delete a scaling policy from an Aurora DB cluster.

AWS CLI

To delete a scaling policy from your Aurora DB cluster, use the delete-scaling-policy AWS CLI command with the following parameters:

• --policy-name – The name of the scaling policy.
• --resource-id – The resource identifier for the Aurora DB cluster. For this parameter, the resource type is cluster and the unique identifier is the name of the Aurora DB cluster, for example cluster:myscalablecluster.
• --service-namespace – Set this value to rds.
• --scalable-dimension – Set this value to rds:cluster:Read Replica Count.

Example

In the following example, you delete a target-tracking scaling policy named myscalablepolicy from an Aurora DB cluster named myscalablecluster.

For Linux, macOS, or Unix:

```
aws application-autoscaling delete-scaling-policy \
   --policy-name myscalablepolicy \
   --resource-id cluster:myescalablecluster \
   --service-namespace rds \
```
For Windows:

```bash
aws application-autoscaling delete-scaling-policy
  --policy-name myscalablepolicy
  --resource-id cluster:myscalablecluster
  --service-namespace rds
  --scalable-dimension rds:cluster:ReadReplicaCount
```

### RDS API

To delete a scaling policy from your Aurora DB cluster, use the `DeleteScalingPolicy` the Application Auto Scaling API operation with the following parameters:

- **PolicyName** – The name of the scaling policy.
- **ServiceNamespace** – Set this value to `rds`.
- **ResourceId** – The resource identifier for the Aurora DB cluster. For this parameter, the resource type is `cluster` and the unique identifier is the name of the Aurora DB cluster, for example `cluster:myscalablecluster`.
- **ScalableDimension** – Set this value to `rds:cluster:ReadReplicaCount`.

#### Example

In the following example, you delete a target-tracking scaling policy named `myscalablepolicy` from an Aurora DB cluster named `myscalablecluster` with the Application Auto Scaling API.

```json
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 and tagging

When a replica is added by Aurora Auto Scaling, its DB instance ID is prefixed by `application-autoscaling-`, for example, `application-autoscaling-61aabbcc-4e2f-4c65-b620-ab7421abc123`.

The following tag is automatically added to the DB instance. You can view it on the Tags tab of the DB instance detail page.
Using machine learning (ML) capabilities with Amazon Aurora

Following, you can find a description of how to use machine learning (ML) capabilities in your Aurora database applications. This feature simplifies developing database applications that use the Amazon SageMaker and Amazon Comprehend services to perform predictions. In ML terminology, these predictions are known as **inferences**.

This feature is suitable for many kinds of quick predictions. Examples include low-latency, real-time use cases such as fraud detection, ad targeting, and product recommendations. The queries pass customer profile, shopping history, and product catalog data to an SageMaker model. Then your application gets product recommendations returned as query results.

To use this feature, it helps for your organization to already have the appropriate ML models, notebooks, and so on available in the Amazon machine learning services. You can divide the database knowledge and ML knowledge among the members of your team. The database developers can focus on the SQL and database side of your application. The Aurora Machine Learning feature enables the application to use ML processing through the familiar database interface of stored function calls.

Topics

- Using machine learning (ML) with Aurora MySQL (p. 827)
- Using machine learning (ML) with Aurora PostgreSQL (p. 1079)
Maintaining an Amazon Aurora DB cluster

Periodically, Amazon RDS performs maintenance on Amazon RDS resources. Maintenance most often involves updates to the DB cluster's underlying hardware, underlying operating system (OS), or database engine version. Updates to the operating system most often occur for security issues and should be done as soon as possible.

Some maintenance items require that Amazon RDS take your DB cluster offline for a short time. Maintenance items that require a resource to be offline include required operating system or database patching. Required patching is automatically scheduled only for patches that are related to security and instance reliability. Such patching occurs infrequently (typically once every few months) and seldom requires more than a fraction of your maintenance window.

You can view whether a maintenance update is available for your DB cluster by using the RDS console, the AWS CLI, or the Amazon RDS API. If an update is available, it is indicated in the Maintenance column for the DB cluster on the Amazon RDS console, as shown following.

If no maintenance update is available for a DB cluster, the column value is none for it.

If a maintenance update is available for a DB cluster, the following column values are possible:

- **required** – The maintenance action will be applied to the resource and can't be deferred indefinitely.
- **available** – The maintenance action is available, but it will not be applied to the resource automatically. You can apply it manually.
- **next window** – The maintenance action will be applied to the resource during the next maintenance window.
- **In progress** – The maintenance action is in the process of being applied to the resource.

If an update is available, you can take one of the actions:

- If the maintenance value is next window, defer the maintenance items by choosing Defer upgrade from Actions. You can't defer a maintenance action if it has already started.
- Apply the maintenance items immediately.
- Schedule the maintenance items to start during your next maintenance window.
- Take no action.
Note
Certain OS updates are marked as required. If you defer a required update, you get a notice from Amazon RDS indicating when the update will be performed. Other updates are marked as available, and these you can defer indefinitely.

To take an action, choose the DB cluster to show its details, then choose Maintenance & backups. The pending maintenance items appear.

The maintenance window determines when pending operations start, but doesn't limit the total run time of these operations. Maintenance operations aren't guaranteed to finish before the maintenance window ends, and can continue beyond the specified end time. For more information, see The Amazon RDS maintenance window (p. 391).

For information about updates to Amazon Aurora engines and instructions for upgrading and patching them, see Database engine updates for Amazon Aurora MySQL (p. 874) and Database engine updates for Amazon Aurora PostgreSQL (p. 1147).
Applying updates for a DB cluster

With Amazon RDS, you can choose when to apply maintenance operations. You can decide when Amazon RDS applies updates by using the RDS console, AWS Command Line Interface (AWS CLI), or RDS API.

**Console**

**To manage an update for a DB cluster**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. Choose the DB cluster that has a required update.
4. For **Actions**, choose one of the following:
   - **Upgrade now**
   - **Upgrade at next window**
   
   **Note**
   If you choose **Upgrade at next window** and later want to delay the update, you can choose **Defer upgrade**. You can't defer a maintenance action if it has already started. To cancel a maintenance action, modify the DB instance and disable **Auto minor version upgrade**.

**AWS CLI**

To apply a pending update to a DB cluster, use the `apply-pending-maintenance-action` AWS CLI command.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds apply-pending-maintenance-action
  --apply-action system-update
  --opt-in-type immediate
```

For Windows:

```bash
aws rds apply-pending-maintenance-action ^
  --apply-action system-update ^
  --opt-in-type immediate
```

**Note**

To defer a maintenance action, specify `undo-opt-in` for `--opt-in-type`. You can't specify `undo-opt-in` for `--opt-in-type` if the maintenance action has already started. To cancel a maintenance action, run the `modify-db-instance` AWS CLI command and specify `--no-auto-minor-version-upgrade`.

To return a list of resources that have at least one pending update, use the `describe-pending-maintenance-actions` AWS CLI command.
Example

For Linux, macOS, or Unix:

```bash
aws rds describe-pending-maintenance-actions
```

For Windows:

```bash
aws rds describe-pending-maintenance-actions
```

You can also return a list of resources for a DB cluster by specifying the `--filters` parameter of the `describe-pending-maintenance-actions` AWS CLI command. The format for the `--filters` command is `Name=filter-name,Value=resource-id,...`

The following are the accepted values for the `Name` parameter of a filter:

- `db-instance-id` – Accepts a list of DB instance identifiers or Amazon Resource Names (ARNs). The returned list only includes pending maintenance actions for the DB instances identified by these identifiers or ARNs.
- `db-cluster-id` – Accepts a list of DB cluster identifiers or ARNs for Amazon Aurora. The returned list only includes pending maintenance actions for the DB clusters identified by these identifiers or ARNs.

For example, the following example returns the pending maintenance actions for the `sample-cluster1` and `sample-cluster2` DB clusters.

Example

For Linux, macOS, or Unix:

```bash
aws rds describe-pending-maintenance-actions
   --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

For Windows:

```bash
aws rds describe-pending-maintenance-actions
   --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

RDS API

To apply an update to a DB cluster, call the Amazon RDS API `ApplyPendingMaintenanceAction` operation.

To return a list of resources that have at least one pending update, call the Amazon RDS API `DescribePendingMaintenanceActions` operation.

The Amazon RDS maintenance window

Every DB cluster has a weekly maintenance window during which any system changes are applied. You can think of the maintenance window as an opportunity to control when modifications and software patching occur, in the event either are requested or required. If a maintenance event is scheduled for a...
The maintenance window
given week, it is initiated during the 30-minute maintenance window you identify. Most maintenance events also complete during the 30-minute maintenance window, although larger maintenance events may take more than 30 minutes to complete.

The 30-minute maintenance window is selected at random from an 8-hour block of time per region. If you don’t specify a preferred maintenance window when you create the DB cluster, then Amazon RDS assigns a 30-minute maintenance window on a randomly selected day of the week.

RDS will consume some of the resources on your DB cluster while maintenance is being applied. You might observe a minimal effect on performance. For a DB instance, on rare occasions, a Multi-AZ failover might be required for a maintenance update to complete.

Following, you can find the time blocks for each region from which default maintenance windows are assigned.

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Time Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (Ohio)</td>
<td>us-east-2</td>
<td>03:00–10:00 UTC</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>03:00–10:00 UTC</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>us-west-1</td>
<td>06:00–11:00 UTC</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>06:00–11:00 UTC</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>ap-east-1</td>
<td>06:00–11:00 UTC</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1</td>
<td>17:30–01:30 UTC</td>
</tr>
<tr>
<td>Asia Pacific (Osaka-Local)</td>
<td>ap-northeast-3</td>
<td>22:00–23:59 UTC</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>13:00–20:00 UTC</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>14:00–20:00 UTC</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>12:00–20:00 UTC</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>12:00–20:00 UTC</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>03:00–11:00 UTC</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>cn-north-1</td>
<td>06:00–11:00 UTC</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>cn-northwest-1</td>
<td>06:00–11:00 UTC</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>23:00–07:00 UTC</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>eu-west-1</td>
<td>22:00–06:00 UTC</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>22:00–06:00 UTC</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>eu-west-3</td>
<td>23:59–07:29 UTC</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>eu-north-1</td>
<td>23:00–07:00 UTC</td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td>me-south-1</td>
<td>06:00–14:00 UTC</td>
</tr>
<tr>
<td>South America (Sao Paulo)</td>
<td>sa-east-1</td>
<td>00:00–08:00 UTC</td>
</tr>
</tbody>
</table>
Adjusting the maintenance window for a DB cluster

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Time Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>us-gov-west-1</td>
<td>06:00–14:00 UTC</td>
</tr>
</tbody>
</table>

Adjusting the preferred DB cluster maintenance window

The Aurora DB cluster maintenance window should fall at the time of lowest usage and thus might need modification from time to time. Your DB cluster is unavailable during this time only if the updates that are being applied require an outage. The outage is for the minimum amount of time required to make the necessary updates.

**Console**

**To adjust the preferred DB cluster maintenance window**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the DB cluster for which you want to change the maintenance window.
4. Choose Modify.
5. In the Maintenance section, update the maintenance window.
6. Choose Continue.
   On the confirmation page, review your changes.
7. To apply the changes to the maintenance window immediately, choose Immediately in the Schedule of modifications section.
8. Choose Modify cluster to save your changes.
   Alternatively, choose Back to edit your changes, or choose Cancel to cancel your changes.

**AWS CLI**

To adjust the preferred DB cluster maintenance window, use the AWS CLI `modify-db-cluster` command with the following parameters:

- `--db-cluster-identifier`
- `--preferred-maintenance-window`

**Example**

The following code example sets the maintenance window to Tuesdays from 4:00–4:30 AM UTC.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster \  
  --db-cluster-identifier my-cluster  \  
  --preferred-maintenance-window Tue:04:00–Tue:04:30
```

For Windows:
Amazon Aurora User Guide for Aurora
Automatic minor version upgrades for Aurora DB clusters

aws rds modify-db-cluster
   --db-cluster-identifier my-cluster
   --preferred-maintenance-window Tue:04:00-Tue:04:30

RDS API

To adjust the preferred DB cluster maintenance window, use the Amazon RDS ModifyDBCluster API operation with the following parameters:

- **DBClusterIdentifier** = *my-cluster*
- **PreferredMaintenanceWindow** = *Tue:04:00-Tue:04:30*

Example

The following code example sets the maintenance window to Tuesdays from 4:00–4:30 AM UTC.

https://rds.us-west-2.amazonaws.com/
?Action=ModifyDBCluster
&DBClusterIdentifier=my-cluster
&PreferredMaintenanceWindow=Tue:04:00-Tue:04:30
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&Version=2014-10-31
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140725/us-east-1/rds/aws4_request
&X-Amz-Date=20161017T161457Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=d6d1c65c2e94f5800ab411a3f7336625820b103713b6c063430900514e21d784

Automatic minor version upgrades for Aurora DB clusters

The **Auto minor version upgrade** setting specifies whether Aurora automatically applies upgrades to your cluster. These upgrades include patch levels containing bug fixes, and new minor versions containing additional features. They don't include any incompatible changes.

**Note**

This setting is enabled by default. For each new cluster, choose the appropriate value for this setting based on its importance, expected lifetime, and the amount of verification testing that you do after each upgrade.

For instructions about turning this setting on or off, see **Settings for Amazon Aurora** (p. 330). In particular, make sure to apply the same setting to all DB instances in the cluster. If any DB instance in your cluster has this setting turned off, the cluster isn't automatically upgraded.

For more information about engine updates for Aurora PostgreSQL, see **Database engine updates for Amazon Aurora PostgreSQL** (p. 1147).

For more information about the **Auto minor version upgrade** setting for Aurora MySQL, see **Enabling automatic upgrades between minor Aurora MySQL versions** (p. 878). For general information about engine updates for Aurora MySQL, see **Database engine updates for Amazon Aurora MySQL** (p. 874).
Choosing the frequency of Aurora MySQL maintenance updates

You can control whether Aurora MySQL upgrades happen frequently or rarely for each DB cluster. The best choice depends on your usage of Aurora MySQL and the priorities for your applications that run on Aurora. For information about the Aurora MySQL long-term stability (LTS) releases that require less frequent upgrades, see Aurora MySQL long-term support (LTS) releases (p. 876).

You might choose to upgrade an Aurora MySQL cluster rarely if some or all of the following conditions apply:

- Your testing cycle for your application takes a long time for each update to the Aurora MySQL database engine.
- You have many DB clusters or many applications all running on the same Aurora MySQL version. You prefer to upgrade all of your DB clusters and associated applications at the same time.
- You use both Aurora MySQL and Amazon RDS MySQL, and you prefer to keep the Aurora MySQL clusters and RDS MySQL DB instances compatible with the same level of MySQL.
- Your Aurora MySQL application is in production or is otherwise business-critical. You can’t afford downtime for upgrades outside of rare occurrences for critical patches.
- Your Aurora MySQL application isn't limited by performance issues or feature gaps that are addressed in subsequent Aurora MySQL versions.

If the preceding factors apply to your situation, you can limit the number of forced upgrades for an Aurora MySQL DB cluster. You do so by choosing a specific Aurora MySQL version known as the “Long-Term Support” (LTS) version when you create or upgrade that DB cluster. Doing so minimizes the number of upgrade cycles, testing cycles, and upgrade-related outages for that DB cluster.

You might choose to upgrade an Aurora MySQL cluster frequently if some or all of the following conditions apply:

- The testing cycle for your application is straightforward and brief.
- Your application is still in the development stage.
- Your database environment uses a variety of Aurora MySQL versions, or Aurora MySQL and Amazon RDS MySQL versions. Each Aurora MySQL cluster has its own upgrade cycle.
- You are waiting for specific performance or feature improvements before you increase your usage of Aurora MySQL.

If the preceding factors apply to your situation, you can enable Aurora to apply important upgrades more frequently by upgrading an Aurora MySQL DB cluster to a more recent Aurora MySQL version than the LTS version. Doing so makes the latest performance enhancements, bug fixes, and features available to you more quickly.
Rebooting a DB instance in a DB cluster

You might need to reboot your DB instance, usually for maintenance reasons. For example, if you make certain modifications, or if you change the DB parameter group associated with the DB instance or its DB cluster, you must reboot the instance for the changes to take effect.

**Note**
If a DB instance isn't using the latest changes to its associated DB parameter group, the AWS Management Console shows the DB parameter group with a status of **pending-reboot**. The **pending-reboot** parameter groups status doesn't result in an automatic reboot during the next maintenance window. To apply the latest parameter changes to that DB instance, manually reboot the DB instance. For more information about parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

Rebooting a DB instance restarts the database engine service. Rebooting a DB instance results in a momentary outage, during which the DB instance status is set to **rebooting**.

You can't reboot your DB instance if it is not in the available state. Your database can be unavailable for several reasons, such as an in-progress backup, a previously requested modification, or a maintenance-window action.

**Important**
When you reboot the primary instance of an Amazon Aurora DB cluster, RDS also automatically restarts all of the Aurora Replicas in that DB cluster. When you reboot the primary instance of an Aurora DB cluster, no failover occurs. When you reboot an Aurora Replica, no failover occurs. To fail over an Aurora DB cluster, call the AWS CLI command **failover-db-cluster**, or the API operation **FailoverDBCluster**.

The time required to reboot your DB instance depends on the crash recovery process, database activity at the time of reboot, and the behavior of your specific DB engine. To improve the reboot time, we recommend that you reduce database activity as much as possible during the reboot process. Reducing database activity reduces rollback activity for in-transit transactions.

For a DB instance with read replicas, you can reboot the source DB instance and its read replicas independently. After a reboot completes, replication resumes automatically.

**Console**

**To reboot a DB instance**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to reboot.
3. For **Actions**, choose **Reboot**.

   The **Reboot DB Instance** page appears.
4. Choose **Reboot** to reboot your DB instance.

   Alternatively, choose **Cancel**.

**AWS CLI**

To reboot a DB instance by using the AWS CLI, call the **reboot-db-instance** command.

**Example Simple reboot**

For Linux, macOS, or Unix:
Rebooting a DB instance

To reboot a DB instance by using the Amazon RDS API, call the RebootDBInstance action.

```
aws rds reboot-db-instance
   --db-instance-identifier mydbinstance
```

For Windows:

```
aws rds reboot-db-instance ^
   --db-instance-identifier mydbinstance
```
Deleting an Aurora DB cluster or a DB instance

You can delete individual DB instances in an Aurora DB cluster, the cluster itself, or both. To delete a DB instance, you specify the name of the instance. Depending on the method you use to delete a cluster, you either specify the name of the cluster or Aurora deletes the cluster automatically as part of deleting the final DB instance.

- If the cluster has more than one instance, deleting one of the instances just reduces the computation capacity of the cluster. If you delete the primary instance from a cluster that has more than one instance, Aurora promotes one of the reader instances to take its place. Thus, usually you delete any reader instances from the cluster first.
- When you use the AWS Management Console, deleting the final DB instance in a DB cluster also deletes the DB cluster and the data in the cluster volume.
- When you use the AWS CLI or the RDS API, you can delete all the DB instances in the cluster without deleting the cluster itself. Your data remains in the cluster volume. Later, you can create one or more new DB instances to start using the cluster again.

**Note**

When the status for a DB instance is deleting, its CA certificate value doesn't appear in the RDS console or in output for AWS CLI commands or RDS API operations. For more information about CA certificates, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).

Deletion protection

You can only delete clusters that don't have deletion protection enabled. You can delete DB instances within the cluster, but not the cluster itself. That way, the cluster volume containing all your data is safe. Aurora enforces deletion protection for a DB cluster whether you try to delete the cluster using the console, the AWS CLI, or the RDS API.

Deletion protection is enabled by default when you create a production DB cluster using the AWS Management Console. However, deletion protection is disabled by default if you create a cluster using the AWS CLI or API. Enabling or disabling deletion protection doesn't cause an outage. To be able to delete the cluster, modify the cluster and disable deletion protection. For more information about turning deletion protection on and off, see Modifying the DB cluster by using the console, CLI, and API (p. 327).

**Tip**

Even if all the DB instances are deleted, you can access the data by creating a new DB instance in the cluster. For information about Aurora clusters that have zero DB instances, see Deleting an empty Aurora cluster (p. 398).

Aurora clusters with a single DB instance

If you try to delete the last DB instance in your Aurora cluster, the behavior depends on the method you use. You can delete the last DB instance using the AWS Management Console. Doing so also deletes the DB cluster. You can also delete the last DB instance through the AWS CLI or API. Enabling or disabling deletion protection doesn't cause an outage. To be able to delete the cluster, modify the cluster and disable deletion protection. For more information about turning deletion protection on and off, see Modifying the DB cluster by using the console, CLI, and API (p. 327).

Deleting an empty Aurora cluster

If you use the AWS Management Console, Aurora automatically deletes your cluster when you delete the last DB instance in that cluster. Thus, the procedures for deleting an empty cluster only apply when you use the AWS CLI or the RDS API.
To delete an empty Aurora DB cluster by using the AWS CLI, call the `delete-db-cluster` command.

To delete an empty Aurora DB cluster by using the Amazon RDS API, call the `DeleteDBInstance` operation.

### Aurora MySQL clusters that are read replicas

For Aurora MySQL, you can't delete a DB instance in a DB cluster if both of the following conditions are true:

- The DB cluster is a read replica of another Aurora DB cluster.
- The DB instance is the only instance in the DB cluster.

To delete a DB instance in this case, first promote the DB cluster so that it's no longer a read replica. After the promotion completes, you can delete the final DB instance in the DB cluster. For more information, see Replicating Amazon Aurora MySQL DB clusters across AWS Regions (p. 733).

### Deleting a DB instance

You can delete a DB instance using the AWS Management Console, the AWS CLI, or the RDS API.

For Aurora DB clusters, deleting a DB instance doesn't necessarily delete the entire cluster. You can delete a DB instance in an Aurora cluster to reduce compute capacity and associated charges when the cluster isn't busy. For information about the special circumstances for Aurora clusters that have one DB instance or zero DB instances, see Aurora clusters with a single DB instance (p. 398) and Deleting an empty Aurora cluster (p. 398).

**Note**

You can't delete a DB cluster when deletion protection is enabled for it. For more information, see Deletion protection (p. 398).

You can disable deletion protection by modifying the DB cluster. For more information, see Modifying an Amazon Aurora DB cluster (p. 327).

### Console

#### To delete a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to delete.
3. For **Actions**, choose **Delete**.
4. Enter `delete me` in the box.
5. Choose **Delete**.

### AWS CLI

To delete a DB instance by using the AWS CLI, call the `delete-db-instance` command and specify the `--db-instance-identifier` value.

**Example**

For Linux, macOS, or Unix:

```
aws rds delete-db-instance \
```
Deleting a DB instance

For Windows:

```bash
aws rds delete-db-instance
  --db-instance-identifier mydbinstance
```

**RDS API**

To delete a DB instance by using the Amazon RDS API, call the `DeleteDBInstance` operation and specify the `DBInstanceIdentifier` parameter.
Tagging Amazon RDS resources

You can use Amazon RDS tags to add metadata to your Amazon RDS resources. You can also use these tags with IAM policies to manage access to Amazon RDS resources and to control what actions can be applied to the Amazon RDS resources. Finally, you can use these tags to track costs by grouping expenses for similarly tagged resources.

All Amazon RDS resources can be tagged

- DB instances
- DB clusters
- Read replicas
- DB snapshots
- DB cluster snapshots
- Reserved DB instances
- Event subscriptions
- DB option groups
- DB parameter groups
- DB cluster parameter groups
- DB security groups
- DB subnet groups

For information on managing access to tagged resources with IAM policies, see Identity and access management in Amazon Aurora (p. 1222).

Overview of Amazon RDS resource tags

An Amazon RDS tag is a name-value pair that you define and associate with an Amazon RDS resource. The name is referred to as the key. Supplying a value for the key is optional. You can use tags to assign arbitrary information to an Amazon RDS resource. You can use a tag key, for example, to define a category, and the tag value might be an item in that category. For example, you might define a tag key of "project" and a tag value of "Salix", indicating that the Amazon RDS resource is assigned to the Salix project. You can also use tags to designate Amazon RDS resources as being used for test or production by using a key such as environment=test or environment=production. We recommend that you use a consistent set of tag keys to make it easier to track metadata associated with Amazon RDS resources.

Use tags to organize your AWS bill to reflect your own cost structure. To do this, sign up to get your AWS account bill with tag key values included. Then, to see the cost of combined resources, organize your billing information according to resources with the same tag key values. For example, you can tag several resources with a specific application name, and then organize your billing information to see the total cost of that application across several services. For more information, see Cost Allocation and Tagging in About AWS Billing and Cost Management.

Each Amazon RDS resource has a tag set, which contains all the tags that are assigned to that Amazon RDS resource. A tag set can contain as many as 50 tags, or it can be empty. If you add a tag to an Amazon RDS resource that has the same key as an existing tag on resource, the new value overwrites the old value.

AWS does not apply any semantic meaning to your tags; tags are interpreted strictly as character strings. Amazon RDS can set tags on a DB instance or other Amazon RDS resources, depending on the settings that you use when you create the resource. For example, Amazon RDS might add a tag indicating that a DB instance is for production or for testing.
The tag key is the required name of the tag. The string value can be from 1 to 128 Unicode characters in length and cannot be prefixed with "aws:" or "rds:". The string can contain only the set of Unicode letters, digits, white-space, '_', ';', ':', '/', '=', '+', '-', '@' (Java regex: "^([\p{L}\p{Z}\p{N}_.:/=+\-\@])$").

The tag value is an optional string value of the tag. The string value can be from 1 to 256 Unicode characters in length and cannot be prefixed with "aws:". The string can contain only the set of Unicode letters, digits, white-space, '_', ';', ':', '/', '=', '+', '-', '@' (Java regex: "^([\p{L}\p{Z}\p{N}_.:/=+\-\@])$").

Values do not have to be unique in a tag set and can be null. For example, you can have a key-value pair in a tag set of `project=Trinity` and `cost-center=Trinity`.

**Note**
You can add a tag to a snapshot, however, your bill will not reflect this grouping.

You can use the AWS Management Console, the command line interface, or the Amazon RDS API to add, list, and delete tags on Amazon RDS resources. When using the command line interface or the Amazon RDS API, you must provide the Amazon Resource Name (ARN) for the Amazon RDS resource you want to work with. For more information about constructing an ARN, see [Constructing an ARN for Amazon RDS](p. 406).

Tags are cached for authorization purposes. Because of this, additions and updates to tags on Amazon RDS resources can take several minutes before they are available.

**Console**

The process to tag an Amazon RDS resource is similar for all resources. The following procedure shows how to tag an Amazon RDS DB instance.

**To add a tag to a DB instance**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Databases**.

   **Note**
   To filter the list of DB instances in the **Databases** pane, enter a text string for **Filter databases**. Only DB instances that contain the string appear.

3. Choose the name of the DB instance that you want to tag to show its details.
4. In the details section, scroll down to the **Tags** section.
5. Choose **Add**. The **Add tags** window appears.
6. Enter a value for Tag key and Value.
7. To add another tag, you can choose Add another Tag and enter a value for its Tag key and Value. Repeat this step as many times as necessary.
8. Choose Add.

**To delete a tag from a DB instance**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
   
   **Note**
   
   To filter the list of DB instances in the Databases pane, enter a text string in the Filter databases box. Only DB instances that contain the string appear.
3. Choose the name of the DB instance to show its details.
4. In the details section, scroll down to the Tags section.
5. Choose the tag you want to delete.

6. Choose Delete, and then choose Delete in the Delete tags window.

**AWS CLI**

You can add, list, or remove tags for a DB instance using the AWS CLI.
• To add one or more tags to an Amazon RDS resource, use the AWS CLI command `add-tags-to-resource`.
• To list the tags on an Amazon RDS resource, use the AWS CLI command `list-tags-for-resource`.
• To remove one or more tags from an Amazon RDS resource, use the AWS CLI command `remove-tags-from-resource`.

To learn more about how to construct the required ARN, see Constructing an ARN for Amazon RDS (p. 406).

RDS API

You can add, list, or remove tags for a DB instance using the Amazon RDS API.

• To add a tag to an Amazon RDS resource, use the `AddTagsToResource` operation.
• To list tags that are assigned to an Amazon RDS resource, use the `ListTagsForResource`.
• To remove tags from an Amazon RDS resource, use the `RemoveTagsFromResource` operation.

To learn more about how to construct the required ARN, see Constructing an ARN for Amazon RDS (p. 406).

When working with XML using the Amazon RDS API, tags use the following schema:

```xml
<Tagging>
  <TagSet>
    <Tag>
      <Key>Project</Key>
      <Value>Trinity</Value>
    </Tag>
    <Tag>
      <Key>User</Key>
      <Value>Jones</Value>
    </Tag>
  </TagSet>
</Tagging>
```

The following table provides a list of the allowed XML tags and their characteristics. Values for Key and Value are case-dependent. For example, project=Trinity and PROJECT=Trinity are two distinct tags.

<table>
<thead>
<tr>
<th>Tagging element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TagSet</td>
<td>A tag set is a container for all tags assigned to an Amazon RDS resource. There can be only one tag set per resource. You work with a TagSet only through the Amazon RDS API.</td>
</tr>
<tr>
<td>Tag</td>
<td>A tag is a user-defined key-value pair. There can be from 1 to 50 tags in a tag set.</td>
</tr>
<tr>
<td>Key</td>
<td>A key is the required name of the tag. The string value can be from 1 to 128 Unicode characters in length and cannot be prefixed with &quot;rds:&quot; or &quot;aws:&quot;. The string can only contain only the set of Unicode letters, digits, white-space, '<em>', '.', '/', '=', '+', '-' (Java regex: &quot;^[\p{L}\p{Z}\p{N}</em>.:/=+-]*$&quot;). Keys must be unique to a tag set. For example, you cannot have a key-pair in a tag set with the key the same but with different values, such as project/Trinity and project/Xanadu.</td>
</tr>
</tbody>
</table>
### Tagging element | Description
--- | ---
Value | A value is the optional value of the tag. The string value can be from 1 to 256 Unicode characters in length and cannot be prefixed with "rds:" or "aws:". The string can only contain only the set of Unicode letters, digits, white-space, '-', '+', '/', ':', '*' and '-' (Java regex: `"^[\p{L}\p{Z}\p{N}\p{Ll}\p{Lm}\p{Lo}\p{Nd}\p{Zs}\p{Zp}\p{Zl}\p{Zx}\p{Zc}\p{Zs}\p{Zp}\p{Zl}\p{Zx}\p{Zc}]+\p{Zs}\p{Zp}\p{Zl}\p{Zx}\p{Zc}]$`).

Values do not have to be unique in a tag set and can be null. For example, you can have a key-value pair in a tag set of project/Trinity and cost-center/Trinity.
Working with Amazon Resource Names (ARNs) in Amazon RDS

Resources created in Amazon Web Services are each uniquely identified with an Amazon Resource Name (ARN). For certain Amazon RDS operations, you must uniquely identify an Amazon RDS resource by specifying its ARN. For example, when you create an RDS DB instance read replica, you must supply the ARN for the source DB instance.

Constructing an ARN for Amazon RDS

Resources created in Amazon Web Services are each uniquely identified with an Amazon Resource Name (ARN). You can construct an ARN for an Amazon RDS resource using the following syntax.

```
arn:aws:rds:<region>:<account number>:<resourcetype>:<name>
```

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (Ohio)</td>
<td>us-east-2</td>
<td>rds.us-east-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rds-fips.us-east-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>rds.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rds-fips.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>us-west-1</td>
<td>rds.us-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rds-fips.us-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>rds.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rds-fips.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
<td>rds.af-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>ap-east-1</td>
<td>rds.ap-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1</td>
<td>rds.ap-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Osaka-Local)</td>
<td>ap-northeast-3</td>
<td>rds.ap-northeast-3.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>rds.ap-northeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Region Name</td>
<td>Region Name</td>
<td>Endpoint</td>
<td>Protocol</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------</td>
<td>-----------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>rds.ap-southeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>rds.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>rds.ap-northeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>rds.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>cn-north-1</td>
<td>rds.cn-north-1.amazonaws.com.cn</td>
<td>HTTPS</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>cn-northwest-1</td>
<td>rds.cn-northwest-1.amazonaws.com.cn</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>rds.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>eu-west-1</td>
<td>rds.eu-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>rds.eu-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>eu-south-1</td>
<td>rds.eu-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>eu-west-3</td>
<td>rds.eu-west-3.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>eu-north-1</td>
<td>rds.eu-north-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td>me-south-1</td>
<td>rds.me-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>sa-east-1</td>
<td>rds.sa-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS GovCloud (US-East)</td>
<td>us-gov-east-1</td>
<td>rds.us-gov-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rds.us-gov-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>us-gov-west-1</td>
<td>rds.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rds.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
The following table shows the format that you should use when constructing an ARN for a particular Amazon RDS resource type.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>ARN format</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB instance</td>
<td>arn:aws:rds:&lt;region&gt;:&lt;account&gt;:db:&lt;name&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td>DB cluster</td>
<td>arn:aws:rds:&lt;region&gt;:&lt;account&gt;:cluster:&lt;name&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td>DB parameter group</td>
<td>arn:aws:rds:&lt;region&gt;:&lt;account&gt;:pg:&lt;name&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td>DB cluster parameter group</td>
<td>arn:aws:rds:&lt;region&gt;:&lt;account&gt;:cluster-pg:&lt;name&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td>Reserved DB instance</td>
<td>arn:aws:rds:&lt;region&gt;:&lt;account&gt;:ri:&lt;name&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td>DB security group</td>
<td>arn:aws:rds:&lt;region&gt;:&lt;account&gt;:secgrp:&lt;name&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
</tbody>
</table>
### Getting an existing ARN

You can get the ARN of an RDS resource by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or RDS API.

**Console**

To get an ARN from the AWS Management Console, navigate to the resource you want an ARN for, and view the details for that resource. For example, you can get the ARN for a DB instance from the **Configuration** tab of the DB instance details, as shown following.
To get an ARN from the AWS CLI for a particular RDS resource, you use the `describe` command for that resource. The following table shows each AWS CLI command, and the ARN property used with the command to get an ARN.

<table>
<thead>
<tr>
<th>AWS CLI command</th>
<th>ARN property</th>
</tr>
</thead>
<tbody>
<tr>
<td>describe-event-subscriptions</td>
<td>EventSubscriptionArn</td>
</tr>
<tr>
<td>describe-certificates</td>
<td>CertificateArn</td>
</tr>
</tbody>
</table>
### AWS CLI command

<table>
<thead>
<tr>
<th>AWS CLI command</th>
<th>ARN property</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>describe-db-parameter-groups</code></td>
<td><code>DBParameterGroupArn</code></td>
</tr>
<tr>
<td><code>describe-db-cluster-parameter-groups</code></td>
<td><code>DBClusterParameterGroupArn</code></td>
</tr>
<tr>
<td><code>describe-db-instances</code></td>
<td><code>DBInstanceArn</code></td>
</tr>
<tr>
<td><code>describe-db-security-groups</code></td>
<td><code>DBSecurityGroupArn</code></td>
</tr>
<tr>
<td><code>describe-db-snapshots</code></td>
<td><code>DBSnapshotArn</code></td>
</tr>
<tr>
<td><code>describe-events</code></td>
<td><code>SourceArn</code></td>
</tr>
<tr>
<td><code>describe-reserved-db-instances</code></td>
<td><code>ReservedDBInstanceArn</code></td>
</tr>
<tr>
<td><code>describe-db-subnet-groups</code></td>
<td><code>DBSubnetGroupArn</code></td>
</tr>
<tr>
<td><code>describe-db-clusters</code></td>
<td><code>DBClusterArn</code></td>
</tr>
<tr>
<td><code>describe-db-cluster-snapshots</code></td>
<td><code>DBClusterSnapshotArn</code></td>
</tr>
</tbody>
</table>

For example, the following AWS CLI command gets the ARN for a DB instance.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds describe-db-instances \
  --db-instance-identifier DBInstanceIdentifier \
  --region us-west-2 \
  --query "*[].{DBInstanceIdentifier:DBInstanceIdentifier, DBInstanceArn:DBInstanceArn}"
```

For Windows:

```bash
aws rds describe-db-instances ^
  --db-instance-identifier DBInstanceIdentifier ^
  --region us-west-2 ^
  --query "*[].{DBInstanceIdentifier:DBInstanceIdentifier, DBInstanceArn:DBInstanceArn}"
```

The output of that command is like the following:

```json
[
  {
    "DBInstanceIdentifier": "instance_id"
  }
]
```

**RDS API**

To get an ARN for a particular RDS resource, you can call the following RDS API operations and use the ARN properties shown following.
<table>
<thead>
<tr>
<th>RDS API operation</th>
<th>ARN property</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeEventSubscriptions</td>
<td>EventSubscriptionArn</td>
</tr>
<tr>
<td>DescribeCertificates</td>
<td>CertificateArn</td>
</tr>
<tr>
<td>DescribeDBParameterGroups</td>
<td>DBParameterGroupArn</td>
</tr>
<tr>
<td>DescribeDBClusterParameterGroups</td>
<td>DBClusterParameterGroupArn</td>
</tr>
<tr>
<td>DescribeDBInstances</td>
<td>DBInstanceArn</td>
</tr>
<tr>
<td>DescribeDBSecurityGroups</td>
<td>DBSecurityGroupArn</td>
</tr>
<tr>
<td>DescribeDBSnapshots</td>
<td>DBSnapshotArn</td>
</tr>
<tr>
<td>DescribeEvents</td>
<td>SourceArn</td>
</tr>
<tr>
<td>DescribeReservedDBInstances</td>
<td>ReservedDBInstanceArn</td>
</tr>
<tr>
<td>DescribeDBSubnetGroups</td>
<td>DBSubnetGroupArn</td>
</tr>
<tr>
<td>DescribeDBClusters</td>
<td>DBClusterArn</td>
</tr>
<tr>
<td>DescribeDBClusterSnapshots</td>
<td>DBClusterSnapshotArn</td>
</tr>
</tbody>
</table>
Amazon Aurora updates

Amazon Aurora releases updates regularly. Updates are applied to Amazon Aurora DB clusters during system maintenance windows. The timing when updates are applied depends on the region and maintenance window setting for the DB cluster, and also the type of update. Updates require a database restart, so you typically experience 20 to 30 seconds of downtime. After this downtime, you can resume using your DB cluster or clusters. You can view or change your maintenance window settings from the AWS Management Console.

Note
The time required to reboot your DB instance depends on the crash recovery process, database activity at the time of reboot, and the behavior of your specific DB engine. To improve the reboot time, we recommend that you reduce database activity as much as possible during the reboot process. Reducing database activity reduces rollback activity for in-transit transactions.

Following, you can find information on general updates to Amazon Aurora. Some of the updates applied to Amazon Aurora are specific to a database engine supported by Aurora. For more information about database engine updates for Aurora, see the following table.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Aurora MySQL</td>
<td>See Database engine updates for Amazon Aurora MySQL (p. 874)</td>
</tr>
<tr>
<td>Amazon Aurora PostgreSQL</td>
<td>See Database engine updates for Amazon Aurora PostgreSQL (p. 1147)</td>
</tr>
</tbody>
</table>

Identifying your Amazon Aurora version

Amazon Aurora includes certain features that are general to Aurora and available to all Aurora DB clusters. Aurora includes other features that are specific to a particular database engine that Aurora supports. These features are available only to those Aurora DB clusters that use that database engine, such as Aurora PostgreSQL.

An Aurora DB instance provides two version numbers, the Aurora version number and the Aurora database engine version number. Aurora version numbers use the following format.

<major version>.<minor version>.<patch version>

To get the Aurora version number from an Aurora DB instance using a particular database engine, use one of the following queries.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Aurora MySQL</td>
<td>SELECT AURORA_VERSION();</td>
</tr>
<tr>
<td></td>
<td>SHOW @@aurora_version;</td>
</tr>
<tr>
<td>Amazon Aurora PostgreSQL</td>
<td>SELECT AURORA_VERSION();</td>
</tr>
</tbody>
</table>
Backing up and restoring an Amazon Aurora DB cluster

This section shows how to back up and restore Amazon Aurora DB clusters.

Topics
- Overview of backing up and restoring an Aurora DB cluster (p. 415)
- Understanding Aurora backup storage usage (p. 417)
- Creating a DB cluster snapshot (p. 418)
- Restoring from a DB cluster snapshot (p. 420)
- Copying a DB cluster snapshot (p. 423)
- Sharing a DB cluster snapshot (p. 433)
- Exporting DB snapshot data to Amazon S3 (p. 439)
- Restoring a DB cluster to a specified time (p. 454)
- Deleting a DB cluster snapshot (p. 457)
Overview of backing up and restoring an Aurora DB cluster

In the following sections, you can find information about Aurora backups and how to restore your Aurora DB cluster using the AWS Management Console.

Tip
The Aurora high availability features and automatic backup capabilities help to keep your data safe without requiring extensive setup from you. Before you implement a backup strategy, learn about the ways that Aurora maintains multiple copies of your data and helps you to access them across multiple DB instances and AWS Regions. For details, see High availability for Amazon Aurora (p. 55).

Backups

Aurora backs up your cluster volume automatically and retains restore data for the length of the backup retention period. Aurora backups are continuous and incremental so you can quickly restore to any point within the backup retention period. No performance impact or interruption of database service occurs as backup data is being written. You can specify a backup retention period, from 1 to 35 days, when you create or modify a DB cluster. Aurora backups are stored in Amazon S3.

If you want to retain a backup beyond the backup retention period, you can also take a snapshot of the data in your cluster volume. Because Aurora retains incremental restore data for the entire backup retention period, you only need to create a snapshot for data that you want to retain beyond the backup retention period. You can create a new DB cluster from the snapshot.

Note
- For Amazon Aurora DB clusters, the default backup retention period is one day regardless of how the DB cluster is created.
- You can't disable automated backups on Aurora. The backup retention period for Aurora is managed by the DB cluster.

Your costs for backup storage depend upon the amount of Aurora backup and snapshot data you keep and how long you keep it. For information about the storage associated with Aurora backups and snapshots, see Understanding Aurora backup storage usage (p. 417). For pricing information about Aurora backup storage, see Amazon RDS for Aurora pricing. After the Aurora cluster associated with a snapshot is deleted, storing that snapshot incurs the standard backup storage charges for Aurora.

Note
You can also use AWS Backup to manage backups of Amazon Aurora DB clusters. Backups managed by AWS Backup are considered manual DB cluster snapshots, but don't count toward the DB cluster snapshot quota for Aurora. Backups that were created with AWS Backup have names ending in awsbackup:AWS-Backup-job-number. For information about AWS Backup, see the AWS Backup Developer Guide.

Restoring data

You can recover your data by creating a new Aurora DB cluster from the backup data that Aurora retains, or from a DB cluster snapshot that you have saved. You can quickly restore a new copy of a DB cluster created from backup data to any point in time during your backup retention period. The continuous and incremental nature of Aurora backups during the backup retention period means you don't need to take frequent snapshots of your data to improve restore times.

To determine the latest or earliest restorable time for a DB instance, look for the Latest Restorable Time or Earliest Restorable Time values on the RDS console. For information about viewing these
values, see Viewing an Amazon Aurora DB cluster (p. 473). The latest restorable time for a DB cluster is the most recent point at which you can restore your DB cluster, typically within 5 minutes of the current time. The earliest restorable time specifies how far back within the backup retention period that you can restore your cluster volume.

You can determine when the restore of a DB cluster is complete by checking the Latest Restorable Time and Earliest Restorable Time values. The Latest Restorable Time and Earliest Restorable Time values return NULL until the restore operation is complete. You can't request a backup or restore operation if Latest Restorable Time or Earliest Restorable Time returns NULL.

For information about restoring a DB cluster to a specified time, see Restoring a DB cluster to a specified time (p. 454).

Database cloning for Aurora

You can also use database cloning to clone the databases of your Aurora DB cluster to a new DB cluster, instead of restoring a DB cluster snapshot. The clone databases use only minimal additional space when first created. Data is copied only as data changes, either on the source databases or the clone databases. You can make multiple clones from the same DB cluster, or create additional clones even from other clones. For more information, see Cloning an Aurora DB cluster volume (p. 355).

Backtrack

Aurora MySQL now supports "rewinding" a DB cluster to a specific time, without restoring data from a backup. For more information, see Backtracking an Aurora DB cluster (p. 677).
Understanding Aurora backup storage usage

Aurora stores continuous backups (within the backup retention period) and snapshots in Aurora backup storage. To control your backup storage usage, you can reduce the backup retention interval, remove old manual snapshots when they are no longer needed, or both. For general information about Aurora backups, see Backups (p. 415). For pricing information about Aurora backup storage, see the Amazon Aurora pricing webpage.

To control your costs, you can monitor the amount of storage consumed by continuous backups and manual snapshots that persist beyond the retention period. Then you can reduce the backup retention interval and remove manual snapshots when they are no longer needed.

You can use the Amazon CloudWatch metrics `TotalBackupStorageBilled`, `SnapshotStorageUsed`, and `BackupRetentionPeriodStorageUsed` to review and monitor the amount of storage used by your Aurora backups, as follows:

- `BackupRetentionPeriodStorageUsed` represents the amount of backup storage used, in bytes, for storing continuous backups at the current time. This value depends on the size of the cluster volume and the amount of changes you make during the retention period. However, for billing purposes it doesn’t exceed the cumulative cluster volume size during the retention period. For example, if your cluster's `VolumeBytesUsed` size is 107,374,182,400 bytes (100 GiB), and your retention period is two days, the maximum value for `BackupRetentionPeriodStorageUsed` is 214,748,364,800 bytes (100 GiB + 100 GiB).

- `SnapshotStorageUsed` represents the amount of backup storage used, in bytes, for storing manual snapshots beyond the backup retention period. Manual snapshots don’t count against your snapshot backup storage while their creation timestamp is within the retention period. All automatic snapshots also don’t count against your snapshot backup storage. The size of each snapshot is the size of the cluster volume at the time you take the snapshot. The `SnapshotStorageUsed` value depends on the number of snapshots you keep and the size of each snapshot. For example, suppose you have one manual snapshot outside the retention period, and the cluster’s `VolumeBytesUsed` size was 100 GiB when that snapshot was taken. The amount of `SnapshotStorageUsed` is 107,374,182,400 bytes (100 GiB).

- `TotalBackupStorageBilled` represents the sum, in bytes, of `BackupRetentionPeriodStorageUsed` and `SnapshotStorageUsed`, minus an amount of free backup storage, which equals the size of the cluster volume for one day. The free backup storage is equal to the latest volume size. For example if your cluster's `VolumeBytesUsed` size is 100 GiB, your retention period is two days, and you have one manual snapshot outside the retention period, the `TotalBackupStorageBilled` is 214,748,364,800 bytes (200 GiB + 100 GiB - 100 GiB).

- These metrics are computed independently for each Aurora DB cluster.

You can monitor your Aurora clusters and build reports using CloudWatch metrics through the CloudWatch console. For more information about how to use CloudWatch metrics, see Overview of monitoring Amazon Aurora (p. 460) and the table of metrics in Amazon Aurora Metrics (p. 464).

The backtrack setting for an Aurora DB cluster doesn’t affect the volume of backup data for that cluster. Amazon bills the storage for backtrack data separately. You can also find the backtrack pricing information on the Amazon Aurora pricing web page.

If you share a snapshot with another user, you are still the owner of that snapshot. The storage costs apply to the snapshot owner. If you delete a shared snapshot that you own, nobody can access it. To keep access to a shared snapshot owned by someone else, you can copy that snapshot. Doing so makes you the owner of the new snapshot. Any storage costs for the copied snapshot apply to your account.
Creating a DB cluster snapshot

Amazon RDS creates a storage volume snapshot of your DB cluster, backing up the entire DB cluster and not just individual databases. When you create a DB cluster snapshot, you need to identify which DB cluster you are going to back up, and then give your DB cluster snapshot a name so you can restore from it later. The amount of time it takes to create a DB cluster snapshot varies with the size your databases. Since the snapshot includes the entire storage volume, the size of files, such as temporary files, also affects the amount of time it takes to create the snapshot.

Unlike automated backups, manual snapshots aren't subject to the backup retention period. Snapshots don't expire.

For very long-term backups, we recommend exporting snapshot data to Amazon S3. If the major version of your DB engine is no longer supported, you can't restore to that version from a snapshot. For more information, see Exporting DB snapshot data to Amazon S3 (p. 439).

You can create a DB cluster snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

**Console**

**To create a DB cluster snapshot**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. In the list of DB instances, choose a writer instance for the DB cluster.
4. Choose **Actions**, and then choose **Take snapshot**.

   The **Take DB Snapshot** window appears.
5. Enter the name of the DB cluster snapshot in the **Snapshot name** box.

6. Choose **Take Snapshot**.

**AWS CLI**

When you create a DB cluster snapshot using the AWS CLI, you need to identify which DB cluster you are going to back up, and then give your DB cluster snapshot a name so you can restore from it later.
You can do this by using the AWS CLI `create-db-cluster-snapshot` command with the following parameters:

- `--db-cluster-identifier`
- `--db-cluster-snapshot-identifier`

In this example, you create a DB cluster snapshot named `mydbclustersnapshot` for a DB cluster called `mydbcluster`.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds create-db-cluster-snapshot \
   --db-cluster-identifier mydbcluster \
   --db-cluster-snapshot-identifier mydbclustersnapshot
```

For Windows:

```bash
aws rds create-db-cluster-snapshot ^
   --db-cluster-identifier mydbcluster ^
   --db-cluster-snapshot-identifier mydbclustersnapshot
```

**RDS API**

When you create a DB cluster snapshot using the Amazon RDS API, you need to identify which DB cluster you are going to back up, and then give your DB cluster snapshot a name so you can restore from it later. You can do this by using the Amazon RDS API `CreateDBClusterSnapshot` command with the following parameters:

- `DBClusterIdentifier`
- `DBClusterSnapshotIdentifier`

**Determining whether the DB cluster snapshot is available**

You can check that the DB cluster snapshot is available by looking under `Snapshots` on the `Maintenance & backups` tab on the detail page for the cluster in the AWS Management Console, by using the `describe-db-cluster-snapshots` CLI command, or by using the `DescribeDBClusterSnapshots` API action.

You can also use the `wait db-cluster-snapshot-available` CLI command to poll the API every 30 seconds until the snapshot is available.
Restoring from a DB cluster snapshot

Amazon RDS creates a storage volume snapshot of your DB cluster, backing up the entire DB instance and not just individual databases. You can create a DB cluster by restoring from this DB cluster snapshot. When you restore the DB cluster, you provide the name of the DB cluster snapshot to restore from, and then provide a name for the new DB cluster that is created from the restore. You can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore.

**Note**
You can't restore a DB cluster from a DB cluster snapshot that is both shared and encrypted. Instead, you can make a copy of the DB cluster snapshot and restore the DB cluster from the copy.

Parameter group considerations

We recommend that you retain the parameter group for any DB cluster snapshots you create, so that you can associate your restored DB cluster with the correct parameter group. You can specify the parameter group when you restore the DB cluster.

Security group considerations

When you restore a DB cluster, the default security group is associated with the restored cluster by default.

**Note**
- If you're using the Amazon RDS console, you can specify a custom security group to associate with the cluster or create a new VPC security group.
- If you're using the AWS CLI, you can specify a custom security group to associate with the cluster by including the `--vpc-security-group-ids` option in the `restore-db-cluster-from-snapshot` command.
- If you're using the Amazon RDS API, you can include the `VpcSecurityGroupIds.VpcSecurityGroupId.N` parameter in the `RestoreDBClusterFromSnapshot` action.

As soon as the restore is complete and your new DB cluster is available, you can associate any custom security groups used by the snapshot you restored from. You must apply these changes by modifying the DB cluster with the RDS console, the AWS CLI `modify-db-cluster` command, or the `ModifyDBCluster` Amazon RDS API operation. For more information, see Modifying an Amazon Aurora DB cluster (p. 327).

Amazon Aurora considerations

With Aurora, you restore a DB cluster snapshot to a DB cluster.

With Aurora MySQL, you can also restore a DB cluster snapshot to an Aurora Serverless DB cluster. For more information, see Restoring an Aurora Serverless v1 DB cluster (p. 150).

With Aurora MySQL, you can restore a DB cluster snapshot from a cluster without parallel query to a cluster with parallel query. Because parallel query is typically used with very large tables, the snapshot mechanism is the fastest way to ingest large volumes of data to an Aurora MySQL parallel query-enabled cluster. For more information, see Working with parallel query for Amazon Aurora MySQL (p. 697).
Restoring from a snapshot

You can restore a DB cluster from a DB cluster snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To restore a DB cluster from a DB cluster snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Snapshots.
3. Choose the DB cluster snapshot that you want to restore from.
4. For Actions, choose Restore Snapshot.
5. On the Restore DB Instance page, for DB Instance Identifier, enter the name for your restored DB cluster.
6. Choose Restore DB Instance.

AWS CLI

To restore a DB cluster from a DB cluster snapshot, use the AWS CLI command restore-db-cluster-from-snapshot.

In this example, you restore from a previously created DB cluster snapshot named mydbclustersnapshot. You restore to a new DB cluster named mynewdbcluster.

Example

For Linux, macOS, or Unix:

```bash
aws rds restore-db-cluster-from-snapshot \
--db-cluster-identifier mynewdbcluster \
--snapshot-identifier mydbclustersnapshot \
--engine aurora|aurora-postgresql
```

For Windows:

```bash
aws rds restore-db-cluster-from-snapshot ^
--db-cluster-identifier mynewdbcluster ^
--snapshot-identifier mydbclustersnapshot ^
--engine aurora|aurora-postgresql
```

After the DB cluster has been restored, you must add the DB cluster to the security group used by the DB cluster used to create the DB cluster snapshot if you want the same functionality as that of the previous DB cluster.

Important

If you use the console to restore a DB cluster, then Amazon RDS automatically creates the primary instance (writer) for your DB cluster. If you use the AWS CLI to restore a DB cluster, you must explicitly create the primary instance for your DB cluster. The primary instance is the first instance that is created in a DB cluster. Call the create-db-instance AWS CLI command to create the primary instance for your DB cluster. Include the name of the DB cluster as the --db-cluster-identifier option value.
RDS API

To restore a DB cluster from a DB cluster snapshot, call the RDS API operation RestoreDBClusterFromSnapshot with the following parameters:

- DBClusterIdentifier
- SnapshotIdentifier

**Important**

If you use the console to restore a DB cluster, then Amazon RDS automatically creates the primary instance (writer) for your DB cluster. If you use the RDS API to restore a DB cluster, you must explicitly create the primary instance for your DB cluster. The primary instance is the first instance that is created in a DB cluster. Call the RDS API operation CreateDBInstance to create the primary instance for your DB cluster. Include the name of the DB cluster as the DBClusterIdentifier parameter value.
Copying a DB cluster snapshot

With Amazon RDS, you can copy automated or manual DB cluster snapshots. After you copy a snapshot, the copy is a manual snapshot.

You can copy a snapshot within the same AWS Region, you can copy a snapshot across AWS Regions, and you can copy shared snapshots.

You can't copy a DB cluster snapshot across Regions and accounts in a single step. Perform one step for each of these copy actions. As an alternative to copying, you can also share manual snapshots with other AWS accounts. For more information, see Sharing a DB cluster snapshot (p. 433).

Note
Amazon bills you based upon the amount of Aurora backup and snapshot data you keep and the period of time that you keep it. For information about the storage associated with Aurora backups and snapshots, see Understanding Aurora backup storage usage (p. 417). For pricing information about Aurora storage, see Amazon RDS for Aurora pricing.

Limitations

The following are some limitations when you copy snapshots:

- You can't copy a snapshot to or from the following AWS Regions: China (Beijing) or China (Ningxia).
- You can copy a snapshot between AWS GovCloud (US-East) and AWS GovCloud (US-West), but you can't copy a snapshot between these AWS GovCloud (US) Regions and other AWS Regions.
- If you delete a source snapshot before the target snapshot becomes available, the snapshot copy may fail. Verify that the target snapshot has a status of AVAILABLE before you delete a source snapshot.
- You can have up to five snapshot copy requests in progress to a single destination Region per account.
- Depending on the Regions involved and the amount of data to be copied, a cross-Region snapshot copy can take hours to complete. If there is a large number of cross-Region snapshot copy requests from a given source AWS Region, Amazon RDS might put new cross-Region copy requests from that source AWS Region into a queue until some in-progress copies complete. No progress information is displayed about copy requests while they are in the queue. Progress information is displayed when the copy starts.

Snapshot retention

Amazon RDS deletes automated snapshots at the end of their retention period, when you disable automated snapshots for a DB cluster, or when you delete a DB cluster. If you want to keep an automated snapshot for a longer period, copy it to create a manual snapshot, which is retained until you delete it. Amazon RDS storage costs might apply to manual snapshots if they exceed your default storage space.

For more information about backup storage costs, see Amazon RDS pricing.

Copying shared snapshots

You can copy snapshots shared to you by other AWS accounts. If you are copying an encrypted snapshot that has been shared from another AWS account, you must have access to the AWS KMS customer master key (CMK) that was used to encrypt the snapshot.

You can only copy a shared DB cluster snapshot, whether encrypted or not, in the same AWS Region. For more information, see Sharing an encrypted snapshot (p. 433).
Handling encryption

You can copy a snapshot that has been encrypted using an AWS KMS customer master key (CMK). If you copy an encrypted snapshot, the copy of the snapshot must also be encrypted. If you copy an encrypted snapshot within the same AWS Region, you can encrypt the copy with the same AWS KMS CMK as the original snapshot, or you can specify a different AWS KMS CMK. If you copy an encrypted snapshot across Regions, you can't use the same AWS KMS CMK for the copy as used for the source snapshot, because AWS KMS CMKs are Region-specific. Instead, you must specify a AWS KMS CMK valid in the destination AWS Region.

The source snapshot remains encrypted throughout the copy process. For more information, see Limitations of Amazon Aurora encrypted DB clusters (p. 1210).

Note
For Amazon Aurora DB cluster snapshots, you can't encrypt an unencrypted DB cluster snapshot when you copy the snapshot.

Copying snapshots across AWS Regions

Depending on the AWS Regions involved and the amount of data to be copied, a cross-Region snapshot copy can take hours to complete. In some cases, there might be a large number of cross-Region snapshot copy requests from a given source AWS Region. In these cases, Amazon RDS might put new cross-Region copy requests from that source AWS Region into a queue until some in-progress copies complete. No progress information is displayed about copy requests while they are in the queue. Progress information is displayed when the copy starts.

Cross-Region snapshot copy isn't supported in the following opt-in AWS Regions:

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Europe (Milan)
- Middle East (Bahrain)

When you copy a snapshot to an AWS Region that is different from the source snapshot's AWS Region, the copy is a full snapshot copy. A full snapshot copy contains all of the data and metadata required to restore the DB instance.

Parameter group considerations

When you copy a snapshot across Regions, the copy doesn't include the parameter group used by the original DB cluster. When you restore a snapshot to create a new DB cluster, that DB cluster gets the default parameter group for the AWS Region it is created in. To give the new DB cluster the same parameters as the original, you must do the following:

1. In the destination AWS Region, create a DB cluster parameter group with the same settings as the original DB cluster. If one already exists in the new AWS Region, you can use that one.
2. After you restore the snapshot in the destination AWS Region, modify the new DB cluster and add the new or existing parameter group from the previous step.

Copying a DB cluster snapshot

Use the procedures in this topic to copy a DB cluster snapshot. If your source database engine is Aurora, then your snapshot is a DB cluster snapshot.
For each AWS account, you can copy up to five DB cluster snapshots at a time from one AWS Region to another. Copying both encrypted and unencrypted DB cluster snapshots is supported. If you copy a DB cluster snapshot to another AWS Region, you create a manual DB cluster snapshot that is retained in that AWS Region. Copying a DB cluster snapshot out of the source AWS Region incurs Amazon RDS data transfer charges.

For more information about data transfer pricing, see Amazon RDS pricing.

After the DB cluster snapshot copy has been created in the new AWS Region, the DB cluster snapshot copy behaves the same as all other DB cluster snapshots in that AWS Region.

**Console**

This procedure works for copying encrypted or unencrypted DB cluster snapshots, in the same AWS Region or across Regions.

To cancel a copy operation once it is in progress, delete the target DB cluster snapshot while that DB cluster snapshot is in **copying** status.

**To copy a DB cluster snapshot**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Snapshots**.
3. Select the check box for the DB cluster snapshot you want to copy.
4. For **Actions**, choose **Copy Snapshot**. The **Make Copy of DB Snapshot** page appears.
5. (Optional) To copy the DB cluster snapshot to a different AWS Region, choose that AWS Region for **Destination Region**.
6. Type the name of the DB cluster snapshot copy in **New DB Snapshot Identifier**.
7. To copy tags and values from the snapshot to the copy of the snapshot, choose **Copy Tags**.
8. Choose **Copy Snapshot**.

**Copying an unencrypted DB cluster snapshot by using the AWS CLI or Amazon RDS API**

Use the procedures in the following sections to copy an unencrypted DB cluster snapshot by using the AWS CLI or Amazon RDS API.

To cancel a copy operation once it is in progress, delete the target DB cluster snapshot identified by --target-db-cluster-snapshot-identifier or TargetDBClusterSnapshotIdentifier while that DB cluster snapshot is in **copying** status.
AWS CLI

To copy a DB cluster snapshot, use the AWS CLI `copy-db-cluster-snapshot` command. If you are copying the snapshot to another AWS Region, run the command in the AWS Region to which the snapshot will be copied.

The following options are used to copy an unencrypted DB cluster snapshot:

- `--source-db-cluster-snapshot-identifier` – The identifier for the DB cluster snapshot to be copied. If you are copying the snapshot to another AWS Region, this identifier must be in the ARN format for the source AWS Region.
- `--target-db-cluster-snapshot-identifier` – The identifier for the new copy of the DB cluster snapshot.

The following code creates a copy of DB cluster snapshot `arn:aws:rds:us-east-1:123456789012:cluster-snapshot:aurora-cluster1-snapshot-20130805` named `myclustersnapshotcopy` in the AWS Region in which the command is run. When the copy is made, all tags on the original snapshot are copied to the snapshot copy.

Example

For Linux, macOS, or Unix:

```bash
aws rds copy-db-cluster-snapshot \
  --target-db-cluster-snapshot-identifier myclustersnapshotcopy \
  --copy-tags
```

For Windows:

```bash
aws rds copy-db-cluster-snapshot ^
  --target-db-cluster-snapshot-identifier myclustersnapshotcopy ^
  --copy-tags
```

RDS API

To copy a DB cluster snapshot, use the Amazon RDS API `CopyDBClusterSnapshot` operation. If you are copying the snapshot to another AWS Region, perform the action in the AWS Region to which the snapshot will be copied.

The following parameters are used to copy an unencrypted DB cluster snapshot:

- `SourceDBClusterSnapshotIdentifier` – The identifier for the DB cluster snapshot to be copied. If you are copying the snapshot to another AWS Region, this identifier must be in the ARN format for the source AWS Region.
- `TargetDBClusterSnapshotIdentifier` – The identifier for the new copy of the DB cluster snapshot.

The following code creates a copy of a snapshot `arn:aws:rds:us-east-1:123456789012:cluster-snapshot:aurora-cluster1-snapshot-20130805` named `myclustersnapshotcopy` in the us-west-1 Region. When the copy is made, all tags on the original snapshot are copied to the snapshot copy.
Copying a DB cluster snapshot

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=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddfed2

Copying an encrypted DB cluster snapshot by using the AWS CLI or Amazon RDS API

Use the procedures in the following sections to copy an encrypted DB cluster snapshot by using the AWS CLI or Amazon RDS API.

To cancel a copy operation once it is in progress, delete the target DB cluster snapshot identified by `--target-db-cluster-snapshot-identifier` or TargetDBClusterSnapshotIdentifier while that DB cluster snapshot is in copying status.

**AWS CLI**

To copy a DB cluster snapshot, use the AWS CLI `copy-db-cluster-snapshot` command. If you are copying the snapshot to another AWS Region, run the command in the AWS Region to which the snapshot will be copied.

The following options are used to copy an encrypted DB cluster snapshot:

- `--source-region` – If you are copying the snapshot to another AWS Region, specify the AWS Region that the encrypted DB cluster snapshot will be copied from.

If you are copying the snapshot to another AWS Region and you don't specify `source-region`, you must specify the `pre-signed-url` option instead. The pre-signed-url value must be a URL that contains a Signature Version 4 signed request for the `CopyDBClusterSnapshot` action to be called in the source AWS Region where the DB cluster snapshot is copied from. To learn more about the pre-signed-url, see `copy-db-cluster-snapshot`.

- `--source-db-cluster-snapshot-identifier` – The identifier for the encrypted DB cluster snapshot to be copied. If you are copying the snapshot to another AWS Region, this identifier must be in the ARN format for the source AWS Region. If that is the case, the AWS Region specified in `source-db-cluster-snapshot-identifier` must match the AWS Region specified for `--source-region`.

- `--target-db-cluster-snapshot-identifier` – The identifier for the new copy of the encrypted DB cluster snapshot.

- `--kms-key-id` – The AWS KMS key identifier for the key to use to encrypt the copy of the DB cluster snapshot.

You can optionally use this option if the DB cluster snapshot is encrypted, you are copying the snapshot in the same AWS Region, and you want to specify a new AWS KMS CMK to use to encrypt the copy. Otherwise, the copy of the DB cluster snapshot is encrypted with the same AWS KMS CMK as the source DB cluster snapshot.
You must use this option if the DB cluster snapshot is encrypted and you are copying the snapshot to another AWS Region. In that case, you must specify a AWS KMS CMK for the destination AWS Region.

The following code example copies the encrypted DB cluster snapshot from the us-west-2 Region to the us-east-1 Region. The command is called in the us-east-1 Region.

**Example**

For Linux, macOS, or Unix:

```
aws rds copy-db-cluster-snapshot \
  --target-db-cluster-snapshot-identifier myclustersnapshotcopy \
  --source-region us-west-2 \
  --kms-key-id my-us-east-1-key
```

For Windows:

```
aws rds copy-db-cluster-snapshot ^
  --target-db-cluster-snapshot-identifier myclustersnapshotcopy ^
  --source-region us-west-2 ^
  --kms-key-id my-us-east-1-key
```

**RDS API**

To copy a DB cluster snapshot, use the Amazon RDS API CopyDBClusterSnapshot operation. If you are copying the snapshot to another AWS Region, perform the action in the AWS Region to which the snapshot will be copied.

The following parameters are used to copy an encrypted DB cluster snapshot:

- **SourceDBClusterSnapshotIdentifier** – The identifier for the encrypted DB cluster snapshot to be copied. If you are copying the snapshot to another AWS Region, this identifier must be in the ARN format for the source AWS Region.
- **TargetDBClusterSnapshotIdentifier** – The identifier for the new copy of the encrypted DB cluster snapshot.
- **KmsKeyId** – The AWS KMS key identifier for the key to use to encrypt the copy of the DB cluster snapshot.

You can optionally use this parameter if the DB cluster snapshot is encrypted, you are copying the snapshot in the same AWS Region, and you want to specify a new AWS KMS CMK to use to encrypt the copy. Otherwise, the copy of the DB cluster snapshot is encrypted with the same AWS KMS CMK as the source DB cluster snapshot.

You must use this parameter if the DB cluster snapshot is encrypted and you are copying the snapshot to another AWS Region. In that case, you must specify a AWS KMS CMK for the destination AWS Region.

- **PreSignedUrl** – If you are copying the snapshot to another AWS Region, you must specify the PreSignedUrl parameter. The PreSignedUrl value must be a URL that contains a Signature Version 4 signed request for the CopyDBClusterSnapshot action to be called in the source AWS
Region where the DB cluster snapshot is copied from. To learn more about using a presigned URL, see `CopyDBClusterSnapshot`.

To automatically rather than manually generate a presigned URL, use the AWS CLI `copy-database-cluster-snapshot` command with the `--source-region` option instead.

The following code example copies the encrypted DB cluster snapshot from the us-west-2 Region to the us-east-1 Region. The action is called in the us-east-1 Region.

**Example**

```plaintext
https://rds.us-east-1.amazonaws.com/
?Action=CopyDBClusterSnapshot
&KmsKeyId=my-us-east-1-key
&PreSignedUrl=https%3A%2F%2Frds.us-west-2.amazonaws.com%252F%252FAction%252DCopyDBClusterSnapshot
%2526DestinationRegion%252Dus-east-1
%2526KmsKeyId%252Dus-west-2-key
%2526SourceDBClusterSnapshotIdentifier%252Darn%25253Aaws%25253Ards%25253Aus-west-2%25253A123456789012%25253Acluster-snapshot%25253Aaurora-cluster1-snapshot-20161115
%2526SignatureMethod%252D%252Dus-east-1
%2526SignatureVersion%252D%252Dus-east-1
%2526SourceRegion%252Dus-west-2
%2526TargetDBClusterSnapshotIdentifier%252Dmyclustersnapshotcopy
%2526ObjectContent%252Dus-east-1
%2526Version%252D%252Dus-east-1
%2526X-Amz-Algorithm%252DAWS4-HMAC-SHA256
%2526X-Amz-Credential%252DAKIADQKE4SARGYLE%252F20161117%252Fus-east-1%252Frds%252Faws4_request
%2526X-Amz-Date%252D%252Dus-east-1
%2526X-Amz-Expires%252D%252Dus-east-1
%2526X-Amz-SignedHeaders%252Dcontent-type%252Bhost%252Buser-agent%252Bx-amz-content-sha256%252Bx-amz-date
%2526X-Amz-Signature%252Dus-east-1
&SignatureMethod=AWS4-HMAC-SHA256
&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%3Bhost%3Buser-agent%3Bx-amz-content-sha256%3Bx-amz-date
&X-Amz-Signature=da4f2da66739d2e722c85fcfd225dc27bba7e2b8d8ea8d8612434378e52adccf
```

**Copying a DB cluster snapshot across accounts**

You can enable other AWS accounts to copy DB cluster snapshots that you specify by using the Amazon RDS API `ModifyDBClusterSnapshotAttribute` and `CopyDBClusterSnapshot` actions. You can only copy DB cluster snapshots across accounts in the same AWS Region. The cross-account copying process works as follows, where Account A is making the snapshot available to copy, and Account B is copying it.

1. Using Account A, call `ModifyDBClusterSnapshotAttribute`, specifying `restore` for the `AttributeName` parameter, and the ID for Account B for the `ValuesToAdd` parameter.

2. (If the snapshot is encrypted) Using Account A, update the key policy for the AWS KMS CMK, first adding the ARN of Account B as a `Principal`, and then allow the `kms:CreateGrant` action.

3. (If the snapshot is encrypted) Using Account B, choose or create an IAM user and attach an IAM policy to that user that allows it to copy an encrypted DB cluster snapshot using your AWS KMS CMK.
4. Using Account B, call `CopyDBClusterSnapshot` and use the `SourceDBClusterSnapshotIdentifier` parameter to specify the ARN of the DB cluster snapshot to be copied, which must include the ID for Account A.

To list all of the AWS accounts permitted to restore a DB cluster snapshot, use the `DescribeDBSnapshotAttributes` or `DescribeDBClusterSnapshotAttributes` API operation.

To remove sharing permission for an AWS account, use the `ModifyDBSnapshotAttribute` or `ModifyDBClusterSnapshotAttribute` action with `AttributeName` set to `restore` and the ID of the account to remove in the `ValuesToRemove` parameter.

### Copying an unencrypted DB cluster snapshot to another account

Use the following procedure to copy an unencrypted DB cluster snapshot to another account in the same AWS Region.

1. In the source account for the DB cluster snapshot, call `ModifyDBClusterSnapshotAttribute`, specifying `restore` for the `AttributeName` parameter, and the ID for the target account for the `ValuesToAdd` parameter.

   Running the following example using the account 987654321 permits two AWS account identifiers, 123451234512 and 123456789012, to restore the DB cluster snapshot named 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=ef38f1ce3dab4e1dbf113d8d2a265c67d17ece1999ff3d6be85714ed36dddbb3
   ```

2. In the target account, call `CopyDBClusterSnapshot` and use the `SourceDBClusterSnapshotIdentifier` parameter to specify the ARN of the DB cluster snapshot to be copied, which must include the ID for the source account.

   Running the following example using the account 123451234512 copies the DB cluster snapshot aurora-cluster1-snapshot-20130805 from account 987654321 and creates a DB cluster snapshot named dbclustersnapshot1.

   ```
   https://rds.us-west-2.amazonaws.com/?Action=CopyDBClusterSnapshot
   &CopyTags=true
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &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=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddfed2
   ```
Copying an encrypted DB cluster snapshot to another account

Use the following procedure to copy an encrypted DB cluster snapshot to another account in the same AWS Region.

1. In the source account for the DB cluster snapshot, call `ModifyDBClusterSnapshotAttribute`, specifying `restore` for the `AttributeName` parameter, and the ID for the target account for the `ValuesToAdd` parameter.

   Running the following example using the account 987654321 permits two AWS account identifiers, 123451234512 and 123456789012, to restore the DB cluster snapshot named manual-snapshot1.

   ```
https://rds.us-west-2.amazonaws.com/?Action=ModifyDBClusterSnapshotAttribute &AttributeName=restore &DBClusterSnapshotIdentifier=manual-snapshot1 &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=ef38f1ce3dad4e1dbf113d8d2a265c67d17ece1999fd36b85714ed36d0bb3
   ```

2. In the source account for the DB cluster snapshot, update the key policy for the AWS KMS CMK, first adding the ARN of the target account as a `Principal`, and then allow the `kms:CreateGrant` action. For more information, see Allowing access to an AWS KMS customer master key (CMK) (p. 434).

3. In the target account, choose or create an IAM user and attach an IAM policy to that user that allows it to copy an encrypted DB cluster snapshot using your AWS KMS CMK. For more information, see Creating an IAM policy to enable copying of the encrypted snapshot (p. 435).

4. In the target account, call `CopyDBClusterSnapshot` and use the `SourceDBClusterSnapshotIdentifier` parameter to specify the ARN of the DB cluster snapshot to be copied, which must include the ID for the source account.

   Running the following example using the account 123451234512 copies the DB cluster snapshot aurora-cluster1-snapshot-20130805 from account 987654321 and creates a DB cluster snapshot named dbclustersnapshot1.

   ```
   ```
Sharing a DB cluster snapshot

Using Amazon RDS, you can share a manual DB cluster snapshot in the following ways:

- Sharing a manual DB cluster snapshot, whether encrypted or unencrypted, enables authorized AWS accounts to copy the snapshot.
- Sharing a manual DB cluster snapshot, whether encrypted or unencrypted, enables authorized AWS accounts to directly restore a DB cluster from the snapshot instead of taking a copy of it and restoring from that.

**Note**

To share an automated DB cluster snapshot, create a manual DB cluster snapshot by copying the automated snapshot, and then share that copy. This process also applies to AWS Backup–generated resources.

For more information on copying a snapshot, see Copying a DB cluster snapshot (p. 423). For more information on restoring a DB instance from a DB cluster snapshot, see Restoring from a DB cluster snapshot (p. 420).

For more information on restoring a DB cluster from a DB cluster snapshot, see Overview of backing up and restoring an Aurora DB cluster (p. 415).

You can share a manual snapshot with up to 20 other AWS accounts. You can also share an unencrypted manual snapshot as public, which makes the snapshot available to all AWS accounts. Take care when sharing a snapshot as public so that none of your private information is included in any of your public snapshots.

The following limitations apply when sharing manual snapshots with other AWS accounts:

- When you restore a DB cluster from a shared snapshot using the AWS Command Line Interface (AWS CLI) or Amazon RDS API, you must specify the Amazon Resource Name (ARN) of the shared snapshot as the snapshot identifier.

Sharing an encrypted snapshot

You can share DB cluster snapshots that have been encrypted "at rest" using the AES-256 encryption algorithm, as described in Encrypting Amazon Aurora resources (p. 1208). To do this, you must take the following steps:

1. Share the AWS Key Management Service (AWS KMS) customer master key (CMK) that was used to encrypt the snapshot with any accounts that you want to be able to access the snapshot.

   You can share AWS KMS CMKs with another AWS account by adding the other account to the AWS KMS key policy. For details on updating a key policy, see Key policies in the AWS KMS Developer Guide. For an example of creating a key policy, see Allowing access to an AWS KMS customer master key (CMK) (p. 434) later in this topic.

2. Use the AWS Management Console, AWS CLI, or Amazon RDS API to share the encrypted snapshot with the other accounts.

These restrictions apply to sharing encrypted snapshots:

- You can’t share encrypted snapshots as public.
- You can’t share a snapshot that has been encrypted using the default AWS KMS CMK of the AWS account that shared the snapshot.
Allowing access to an AWS KMS customer master key (CMK)

For another AWS account to copy an encrypted DB cluster snapshot shared from your account, the account that you share your snapshot with must have access to the AWS KMS customer master key (CMK) that encrypted the snapshot. To allow another AWS account access to an AWS KMS CMK, update the key policy for the AWS KMS CMK with the ARN of the AWS account that you are sharing to as a Principal in the AWS KMS key policy, and then allow the kms:CreateGrant action.

After you have given an AWS account access to your AWS KMS CMK, to copy your encrypted snapshot, that AWS account must create an AWS Identity and Access Management (IAM) user if it doesn't already have one. In addition, that AWS account must also attach an IAM policy to that IAM user that allows the IAM user to copy an encrypted DB cluster snapshot using your AWS KMS CMK. The account must be an IAM user and cannot be a root AWS account identity due to AWS KMS security restrictions.

In the following key policy example, user 111122223333 is the owner of the AWS KMS CMK, and user 444455556666 is the account that the key is being shared with. This updated key policy gives the AWS account access to the AWS KMS CMK by including the ARN of the root AWS account identity for user 444455556666 as a Principal for the policy, and by allowing the kms:CreateGrant action.

```json
{
  "Id": "key-policy-1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::111122223333:user/KeyUser",
        "arn:aws:iam::444455556666: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::111122223333:user/KeyUser",
        "arn:aws:iam::444455556666:root"
      ]},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
    }
  ]
}
```
Creating an IAM policy to enable copying of the encrypted snapshot

Once the external AWS account has access to your AWS KMS customer master key (CMK), the owner of that AWS account can create a policy that allows an IAM user created for that account to copy an encrypted snapshot encrypted with that AWS KMS CMK.

The following example shows a policy that can be attached to an IAM user for AWS account 444455556666 that enables the IAM user to copy a shared snapshot from AWS account 111122223333 that has been encrypted with the AWS KMS CMK c989c1dd-a3f2-4a5d-8d96-e793d082ab26 in the us-west-2 region.

```json
{
  "Version": "2012-10-17",
  "Statement": [ 
    { 
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [ 
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
      ],
      "Resource": [ "arn:aws:kms:us-west-2:111122223333:key/c989c1dd-a3f2-4a5d-8d96-e793d082ab26" ]
    },
    { 
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [ 
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [ "arn:aws:kms:us-west-2:111122223333:key/c989c1dd-a3f2-4a5d-8d96-e793d082ab26" ],
      "Condition": { 
        "Bool": { 
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
```

For details on updating a key policy, see Key policies in the AWS KMS Developer Guide.

Sharing a snapshot

You can share a DB cluster snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

Console

Using the Amazon RDS console, you can share a manual DB cluster snapshot with up to 20 AWS accounts. You can also use the console to stop sharing a manual snapshot with one or more accounts.
To share a manual DB cluster snapshot by using the Amazon RDS console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Snapshots.
3. Select the manual snapshot that you want to share.
4. For Actions, choose Share Snapshot.
5. Choose one of the following options for DB snapshot visibility.
   - If the source is unencrypted, choose Public to permit all AWS accounts to restore a DB cluster from your manual DB cluster snapshot, or choose Private to permit only AWS accounts that you specify to restore a DB cluster from your manual DB cluster snapshot.
     Warning
     If you set DB snapshot visibility to Public, all AWS accounts can restore a DB cluster from your manual DB cluster snapshot and have access to your data. Do not share any manual DB cluster snapshots that contain private information as Public.
   - If the source is encrypted, DB snapshot visibility is set as Private because encrypted snapshots can't be shared as public.
6. For AWS Account ID, type the AWS account identifier for an account that you want to permit to restore a DB cluster from your manual snapshot, and then choose Add. Repeat to include additional AWS account identifiers, up to 20 AWS accounts.

If you make an error when adding an AWS account identifier to the list of permitted accounts, you can delete it from the list by choosing Delete at the right of the incorrect AWS account identifier.

7. After you have added identifiers for all of the AWS accounts that you want to permit to restore the manual snapshot, choose Save to save your changes.
To stop sharing a manual DB cluster snapshot with an AWS account

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Snapshots.
3. Select the manual snapshot that you want to stop sharing.
4. Choose Actions, and then choose Share Snapshot.
5. To remove permission for an AWS account, choose Delete for the AWS account identifier for that account from the list of authorized accounts.
6. Choose Save to save your changes.

AWS CLI

To share a DB cluster snapshot, use the `aws rds modify-db-cluster-snapshot-attribute` command. Use the `--values-to-add` parameter to add a list of the IDs for the AWS accounts that are authorized to restore the manual snapshot.

The following example enables two AWS account identifiers, 111122223333 and 444455556666, to restore the DB cluster snapshot named manual-cluster-snapshot1.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster-snapshot-attribute \
  --db-cluster-snapshot-identifier manual-cluster-snapshot1 \
  --attribute-name restore \
  --values-to-add ("111122223333","444455556666")
```
Sharing a snapshot

For Windows:

```
aws rds modify-db-cluster-snapshot-attribute ^
  --db-cluster-snapshot-identifier manual-cluster-snapshot1 ^
  --attribute-name restore ^
  --values-to-add "["111122223333","444455556666"]"
```

**Note**
When using the Windows command prompt, you must escape double quotes (") in JSON code by prefixing them with a backslash (\).

To remove an AWS account identifier from the list, use the `--values-to-remove` parameter. The following example prevents AWS account ID 444455556666 from restoring the snapshot.

**Example**

For Linux, macOS, or Unix:

```
aws rds modify-db-cluster-snapshot-attribute \
  --db-cluster-snapshot-identifier manual-cluster-snapshot1 \
  --attribute-name restore \
  --values-to-remove {"444455556666"}
```

For Windows:

```
aws rds modify-db-cluster-snapshot-attribute ^
  --db-cluster-snapshot-identifier manual-cluster-snapshot1 ^
  --attribute-name restore ^
  --values-to-remove "["444455556666"]"
```

**Note**
When using the Windows command prompt, you must escape double quotes (") in JSON code by prefixing them with a backslash (\).

To list the AWS accounts enabled to restore a snapshot, use the `describe-db-cluster-snapshot-attributes` AWS CLI command.

**RDS API**

You can also share a manual DB cluster snapshot with other AWS accounts by using the Amazon RDS API. To do so, call the `ModifyDBClusterSnapshotAttribute` operation. Specify `restore` for `AttributeName`, and use the `ValuesToAdd` parameter to add a list of the IDs for the AWS accounts that are authorized to restore the manual snapshot.

To make a manual snapshot public and restorable by all AWS accounts, use the value `all`. However, take care not to add the all value for any manual snapshots that contain private information that you don't want to be available to all AWS accounts. Also, don't specify all for encrypted snapshots, because making such snapshots public isn't supported.

To remove sharing permission for an AWS account, use the `ModifyDBClusterSnapshotAttribute` operation with `AttributeName` set to `restore` and the `ValuesToRemove` parameter. To mark a manual snapshot as private, remove the value all from the values list for the `restore` attribute.

To list all of the AWS accounts permitted to restore a snapshot, use the `DescribeDBClusterSnapshotAttributes` API operation.
Exporting DB snapshot data to Amazon S3

You can export DB snapshot data to an Amazon S3 bucket. After the data is exported, you can analyze the exported data directly through tools like Amazon Athena or Amazon Redshift Spectrum. The export process runs in the background and doesn't affect the performance of your active DB cluster.

When you export a DB snapshot, Amazon Aurora extracts data from the snapshot and stores it in an Amazon S3 bucket in your account. The data is stored in an Apache Parquet format that is compressed and consistent.

You can export manual snapshots and automated system snapshots. By default, all data in the snapshot is exported. However, you can choose to export specific sets of databases, schemas, or tables.

Amazon RDS supports exporting snapshots in all AWS Regions except the following:

- AWS GovCloud (US-East)
- AWS GovCloud (US-West)
- China

The following table shows the Aurora MySQL engine versions that are supported for exporting snapshot data to Amazon S3. For more information about Aurora MySQL engine versions, see Database engine updates for Amazon Aurora MySQL (p. 874).

<table>
<thead>
<tr>
<th>Aurora MySQL version</th>
<th>MySQL-compatible version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.04.4 and higher</td>
<td>5.7</td>
</tr>
<tr>
<td>1.19.2 and higher</td>
<td>5.6</td>
</tr>
</tbody>
</table>

The following table shows the Aurora PostgreSQL engine versions that are supported for exporting snapshot data to Amazon S3. For more information about Aurora PostgreSQL engine versions, see Engine versions for Amazon Aurora PostgreSQL (p. 1148).

<table>
<thead>
<tr>
<th>Aurora PostgreSQL version</th>
<th>PostgreSQL-compatible version</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0 and higher</td>
<td>11.4 and higher</td>
</tr>
<tr>
<td>2.2 and higher</td>
<td>10.6 and higher</td>
</tr>
<tr>
<td>1.4 and higher</td>
<td>9.6.11 and higher</td>
</tr>
</tbody>
</table>

Topics

- Overview of exporting snapshot data (p. 440)
- Setting up access to an Amazon S3 bucket (p. 440)
- Exporting a snapshot to an Amazon S3 bucket (p. 442)
- Monitoring snapshot exports (p. 444)
- Canceling a snapshot export task (p. 446)
- Troubleshooting PostgreSQL permissions errors (p. 447)
- Data conversion when exporting to an Amazon S3 bucket (p. 447)
Overview of exporting snapshot data

The following procedure provides a high-level view of how to export DB snapshot data to an Amazon S3 bucket. For more details, see the following sections.

To export DB snapshot data to Amazon S3

1. Identify the snapshot to export.
   
   Use an existing automated or manual snapshot, or create a manual snapshot of a DB instance.

2. Set up access to the Amazon S3 bucket.

   A bucket is a container for Amazon S3 objects or files. To provide the information to access a bucket, take the following steps:
   
   a. Identify the S3 bucket where the snapshot is to be exported to. The S3 bucket must be in the same AWS Region as the snapshot. For more information, see Identifying the Amazon S3 bucket for export (p. 440).
   
   b. Create an AWS Key Management Service (AWS KMS) customer master key (CMK) for the server-side encryption. The AWS KMS CMK is used by the snapshot export task to set up AWS KMS server-side encryption when writing the export data to S3. For more information, see Encrypting Amazon Aurora resources (p. 1208).
   
   c. Create an AWS Identity and Access Management (IAM) role that grants the snapshot export task access to the S3 bucket. For more information, see Providing access to an Amazon S3 bucket using an IAM role (p. 441).

3. Export the snapshot to Amazon S3 using the console or the \texttt{start-export-task} CLI command. For more information, see Exporting a snapshot to an Amazon S3 bucket (p. 442).

4. To access your exported data in the Amazon S3 bucket, see Uploading, downloading, and managing objects in the Amazon Simple Storage Service Console User Guide.

Setting up access to an Amazon S3 bucket

To export DB snapshot data to an Amazon S3 file, you first give the snapshot permission to access the Amazon S3 bucket. You then create an IAM role to allow the Amazon Aurora service to write to the Amazon S3 bucket.

Topics

- Identifying the Amazon S3 bucket for export (p. 440)
- Providing access to an Amazon S3 bucket using an IAM role (p. 441)

Identifying the Amazon S3 bucket for export

Identify the Amazon S3 bucket to export the DB snapshot to. Use an existing S3 bucket or create a new S3 bucket.

Note

The S3 bucket to export to must be in the same AWS Region as the snapshot.

For more information about working with Amazon S3 buckets, see the following in the Amazon Simple Storage Service Console User Guide:

- How do I view the properties for an S3 bucket?
- How do I enable default encryption for an Amazon S3 bucket?
- How do I create an S3 bucket?
Providing access to an Amazon S3 bucket using an IAM role

Before you export DB snapshot data to Amazon S3, give the snapshot export tasks write-access permission to the Amazon S3 bucket.

To do this, create an IAM policy that provides access to the bucket. Then create an IAM role and attach the policy to the role. You later assign the IAM role to your snapshot export task.

Important
If you plan to use the AWS Management Console to export your snapshot, you can choose to create the IAM policy and the role automatically when you export the snapshot. For instructions, see Exporting a snapshot to an Amazon S3 bucket (p. 442).

To give DB snapshot tasks access to Amazon S3

1. Create an IAM policy. This policy provides the bucket and object permissions that allow your snapshot export task to access Amazon S3.

   Include in the policy the following required actions to allow the transfer of files from Amazon Aurora to an S3 bucket:

   • s3:PutObject*
   • s3:GetObject*
   • s3:ListBucket
   • s3:DeleteObject*
   • s3:GetBucketLocation

   Include in the policy the following resources to identify the S3 bucket and objects in the bucket. The following list of resources shows the Amazon Resource Name (ARN) format for accessing Amazon S3.

   • arn:aws:s3:::your-s3-bucket
   • arn:aws:s3:::your-s3-bucket/*

   For more information on creating an IAM policy for Amazon Aurora, see Creating and using an IAM policy for IAM database access (p. 1241). See also Tutorial: Create and attach your first customer managed policy in the IAM User Guide.

   The following AWS CLI command creates an IAM policy named ExportPolicy with these options. It grants access to a bucket named your-s3-bucket.

   Note
   After you create the policy, note the ARN of the policy. You need the ARN for a subsequent step when you attach the policy to an IAM role.

   ```
   aws iam create-policy --policy-name ExportPolicy --policy-document '{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": ["s3:PutObject", "s3:GetObject", "s3:ListBucket", "s3:DeleteObject", "s3:GetBucketLocation"],
           "Resource": ["arn:aws:s3:::your-s3-bucket"]
       },
       {
           "Effect": "Allow",
           "Action": ["s3:PutObject", "s3:GetObject", "s3:ListBucket", "s3:DeleteObject", "s3:GetBucketLocation"],
           "Resource": ["arn:aws:s3:::your-s3-bucket/*"]
       }
   ]
   '}
   ```
2. Create an IAM role. You do this so that Aurora can assume this IAM role on your behalf to access your Amazon S3 buckets. For more information, see Creating a role to delegate permissions to an IAM user in the IAM User Guide.

The following example shows using the AWS CLI command to create a role named 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. Attach the IAM policy that you created to the IAM role that you created.

The following AWS CLI command attaches the policy created earlier to the role named rds-s3-export-role. Replace your-policy-arn with the policy ARN that you noted in an earlier step.

```
aws iam attach-role-policy --policy-arn your-policy-arn --role-name rds-s3-export-role
```

### Exporting a snapshot to an Amazon S3 bucket

You can export a DB snapshot to Amazon S3 using the AWS Management Console, the AWS CLI, or the RDS API.

**Note**

Exporting RDS snapshots can take a while depending on your database type and size. The export task first restores and scales the entire database before extracting the data to Amazon S3. The task's progress during this phase displays as Starting. When the task switches to exporting data to S3, progress displays as In progress. The time it takes for the export to complete depends on the data stored in the database. For example, tables with well distributed numeric primary key or index columns will export the fastest. Tables that don't contain a column suitable for partitioning and tables with only one index on a string-based column will take longer because the export uses a slower single threaded process.

You can export a DB snapshot to Amazon S3 using the AWS Management Console, the AWS CLI, or the RDS API.
If you use a Lambda function to export a snapshot, add the kms:DescribeKey action to the Lambda function policy. For more information, see AWS Lambda permissions.

Console

The Export to Amazon S3 console option appears only for snapshots that can be exported to Amazon S3. A snapshot might not be available for export because of the following reasons:

- The DB engine isn't supported for S3 export.
- The DB instance version isn't supported for S3 export.
- S3 export isn't supported in the AWS Region where the snapshot was created.

To export a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Snapshots.
3. From the tabs, choose the type of snapshot that you want to export.
4. In the list of snapshots, choose the snapshot that you want to export.
5. For Actions, choose Export to Amazon S3.

The Export to Amazon S3 window appears.

6. For Export identifier, enter a name to identify the export task. This value is also used for the name of the file created in the S3 bucket.
7. Choose the amount of data to be exported:
   - Choose All to export all data in the snapshot.
   - Choose Partial to export specific parts of the snapshot. To identify which parts of the snapshot to export, enter one or more tables for Identifiers.
8. For S3 bucket, choose the bucket to export to.

To assign the exported data to a folder path in the S3 bucket, enter the optional path for S3 prefix.

9. For IAM role, either choose a role that grants you write access to your chosen S3 bucket, or create a new role.
   - If you created a role by following the steps in Providing access to an Amazon S3 bucket using an IAM role (p. 441), choose that role.
   - If you didn't create a role that grants you write access to your chosen S3 bucket, choose Create a new role to create the role automatically. Next, enter a name for the role in IAM role name.
10. For Master key, enter the ARN for the key to use for encrypting the exported data.
11. Choose Export to Amazon S3.

AWS CLI

To export a DB snapshot to Amazon S3 using the AWS CLI, use the start-export-task command with the following required options:

- --export-task-identifier
- --source-arn
- --s3-bucket-name
- --iam-role-arn
- --kms-key-id
In the following examples, the snapshot export task is named `my_snapshot_export`, which exports a snapshot to an S3 bucket named `my_export_bucket`.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds start-export-task
   --export-task-identifier my_snapshot_export
   --s3-bucket-name my_export_bucket
   --iam-role-arn iam_role
   --kms-key-id master_key
```

For Windows:

```bash
aws rds start-export-task
   --export-task-identifier my_snapshot_export
   --s3-bucket-name my_export_bucket
   --iam-role-arn iam_role
   --kms-key-id master_key
```

Sample output follows.

```json
{
   "Status": "STARTING",
   "IamRoleArn": "iam_role",
   "ExportTime": "2019-08-12T01:23:53.109Z",
   "S3Bucket": "my_export_bucket",
   "PercentProgress": 0,
   "KmsKeyId": "master_key",
   "ExportTaskIdentifier": "my_snapshot_export",
   "TotalExtractedDataInGB": 0,
   "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot_name"
}
```

To provide a folder path in the S3 bucket for the snapshot export, include the `--s3-prefix` option in the `start-export-task` command.

**RDS API**

To export a DB snapshot to Amazon S3 using the Amazon RDS API, use the `StartExportTask` operation with the following required parameters:

- `ExportTaskIdentifier`
- `SourceArn`
- `S3BucketName`
- `IamRoleArn`
- `KmsKeyId`

**Monitoring snapshot exports**

You can monitor DB snapshot exports using the AWS Management Console, the AWS CLI, or the RDS API.
Console

To monitor DB snapshot exports

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Snapshots.
3. To view the list of snapshot exports, choose the Exports in Amazon S3 tab.
4. To view information about a specific snapshot export, choose the export task.

AWS CLI

To monitor DB snapshot exports using the AWS CLI, use the describe-export-tasks command.

The following example shows how to display current information about all of your snapshot exports.

Example

```bash
aws rds describe-export-tasks
{
   "ExportTasks": [
   {
     "Status": "CANCELED",
     "TaskEndTime": "2019-11-01T17:36:46.961Z",
     "S3Prefix": "something",
     "S3Bucket": "examplebucket",
     "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,
   },
   {
     "Status": "COMPLETE",
     "WarningMessage": "{"skippedTables":[],"skippedObjectives":[]},
     "general": [{"reason":"FAILED_TO_EXTRACT_TABLES_LIST_FOR_DATABASE"}],
     "S3Prefix": "",
     "ExportTime": "2019-10-31T06:44:53.452Z",
     "S3Bucket": "examplebucket1",
     "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",
   },
   {
     "Status": "FAILED",
     "TaskEndTime": "2019-10-31T02:12:36.409Z",
     "FailureCause": "The S3 bucket edgcuc-export isn't located in the current AWS Region. Please, review your S3 bucket name and retry the export."
   }
   ]
}```
To display information about a specific snapshot export, include the `--export-task-identifier` option with the `describe-export-tasks` command. To filter the output, include the `--Filters` option. For more options, see the `describe-export-tasks` command.

**RDS API**

To display information about DB snapshot exports using the Amazon RDS API, use the `DescribeExportTasks` operation.

To track completion of the export workflow or to trigger another workflow, you can subscribe to Amazon Simple Notification Service topics. For more information on Amazon SNS, see Using Amazon RDS event notification (p. 594).

### Canceling a snapshot export task

You can cancel a DB snapshot export task using the AWS Management Console, the AWS CLI, or the RDS API.

**Note**

Canceling a snapshot export task doesn't remove any data that was exported to Amazon S3. For information about how to delete the data using the console, see How do I delete objects from an S3 bucket? To delete the data using the CLI, use the `delete-object` command.

**Console**

To cancel a snapshot export task

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Snapshots**.
3. Choose the **Exports in Amazon S3** tab.
4. Choose the snapshot export task that you want to cancel.
5. Choose **Cancel**.
6. Choose **Cancel export task** on the confirmation page.

**AWS CLI**

To cancel a snapshot export task using the AWS CLI, use the `cancel-export-task` command. The command requires the `--export-task-identifier` option.

**Example**

```
aws rds cancel-export-task --export-task-identifier my_export
```
Troubleshooting PostgreSQL permissions errors

When exporting PostgreSQL databases to Amazon S3, you might see a `PERMISSIONS_DO_NOT_EXIST` error stating that certain tables were skipped. This is usually caused by the superuser, which you specify when creating the DB instance, not having permissions to access those tables.

To fix this error, run the following command:

```
grant all privileges on all tables in schema schema_name to superuser_name
```

For more information on superuser privileges, see Master user account privileges (p. 1276).

Data conversion when exporting to an Amazon S3 bucket

When you export a DB snapshot to an Amazon S3 bucket, Amazon Aurora converts data to, exports data in, and stores data in the Parquet format. For more information about Parquet, see the Apache Parquet website.

Parquet stores all data as one of the following primitive types:

- BOOLEAN
- INT32
- INT64
- INT96
- FLOAT
- DOUBLE
- BYTE_ARRAY – A variable-length byte array, also known as binary
- FIXED_LEN_BYTE_ARRAY – A fixed-length byte array used when the values have a constant size

The Parquet data types are few to reduce the complexity of reading and writing the format. Parquet provides logical types for extending primitive types. A `logical` type is implemented as an annotation with the data in a `LogicalType` metadata field. The logical type annotation explains how to interpret the primitive type.
When the `STRING` logical type annotates a `BYTE_ARRAY` type, it indicates that the byte array should be interpreted as a UTF-8 encoded character string. After an export task completes, Amazon Aurora notifies you if any string conversion occurred. The underlying data exported is always the same as the data from the source. However, due to the encoding difference in UTF-8, some characters might appear different from the source when read in tools such as Athena.

For more information, see Parquet logical type definitions in the Parquet documentation.

**Note**

- Some characters aren't supported in database table column names. Tables with the following characters in column names are skipped during export.

```
,;{}\n=```

- If the data contains a huge value close to or greater than 500 MB, the export fails.
- If the database, schema, or table name contains spaces, partial export isn't supported. However, you can export the entire DB snapshot.

**Topics**

- [MySQL data type mapping to Parquet](#) (p. 448)
- [PostgreSQL data type mapping to Parquet](#) (p. 451)

### MySQL data type mapping to Parquet

The following table shows the mapping from MySQL data types to Parquet data types when data is converted and exported to Amazon S3.

<table>
<thead>
<tr>
<th>Source data type</th>
<th>Parquet primitive type</th>
<th>Logical type annotation</th>
<th>Conversion notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Numeric data types</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIGINT</td>
<td>INT64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIGINT UNSIGNED</td>
<td>FIXED_LEN_BYTE_ARRAY(9)DECIMAL(20,0)</td>
<td>Parquet supports only signed types, so the mapping requires an additional byte (8 plus 1) to store the BIGINT_UNSIGNED type.</td>
<td></td>
</tr>
<tr>
<td>BIT</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DECIMAL</td>
<td>INT32</td>
<td>DECIMAL(p,s)</td>
<td>If the source value is less than $2^{31}$, it's stored as INT32.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If the source value is $2^{31}$ or greater, but less than $2^{63}$, it's stored as INT64.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If the source value is $2^{63}$ or greater, it's stored as FIXED_LEN_BYTE_ARRAY(N).</td>
</tr>
</tbody>
</table>
### Data conversion

<table>
<thead>
<tr>
<th>Source data type</th>
<th>Parquet primitive type</th>
<th>Logical type annotation</th>
<th>Conversion notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOUBLE</td>
<td>DOUBLE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FLOAT</td>
<td>DOUBLE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INT</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INT UNSIGNED</td>
<td>INT64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEDIUMINT</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEDIUMINT UNSIGNED</td>
<td>INT64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NUMERIC</td>
<td>INT32</td>
<td>DECIMAL(p,s)</td>
<td>If the source value is less than $2^{31}$, it's stored as INT32.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If the source value is $2^{31}$ or greater, but less than $2^{63}$, it's stored as INT64.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If the source value is $2^{63}$ or greater, it's stored as FIXED_LEN_BYTE_ARRAY(N).</td>
</tr>
<tr>
<td>FIXED_LEN_ARRAY(N)</td>
<td></td>
<td>DECIMAL(p,s)</td>
<td></td>
</tr>
<tr>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
<td>Parquet doesn't support Decimal precision greater than 38. This Numeric value is converted to a string in a BYTE_ARRAY type and encoded as UTF8.</td>
</tr>
<tr>
<td>SMALLINT</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMALLINT UNSIGNED</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TINYINT</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TINYINT UNSIGNED</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**String data types**

<table>
<thead>
<tr>
<th>String data type</th>
<th>Parquet primitive type</th>
<th>Logical type annotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>BINARY</td>
<td>BYTE_ARRAY</td>
<td></td>
</tr>
<tr>
<td>BLOB</td>
<td>BYTE_ARRAY</td>
<td></td>
</tr>
<tr>
<td>CHAR</td>
<td>BYTE_ARRAY</td>
<td></td>
</tr>
<tr>
<td>ENUM</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
</tr>
</tbody>
</table>
### Data conversion

<table>
<thead>
<tr>
<th>Source data type</th>
<th>Parquet primitive type</th>
<th>Logical type annotation</th>
<th>Conversion notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINESTRING</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LONGBLOB</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LONGTEXT</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>MEDIUMBLOB</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEDIUMLONGTEXT</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>MULTILINestring</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SET</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TEXT</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TINYBLOB</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TINYTEXT</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>VARBINARY</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VARCHAR</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
</tbody>
</table>

### Date and time data types

<table>
<thead>
<tr>
<th>Date and time data type</th>
<th>Parquet primitive type</th>
<th>Logical type annotation</th>
<th>Conversion notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>DATETIME</td>
<td>INT64</td>
<td>TIMESTAMP_MICROS</td>
<td></td>
</tr>
<tr>
<td>TIME</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>INT64</td>
<td>TIMESTAMP_MICROS</td>
<td></td>
</tr>
<tr>
<td>YEAR</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Geometric data types

<table>
<thead>
<tr>
<th>Geometric data type</th>
<th>Parquet primitive type</th>
<th>Logical type annotation</th>
<th>Conversion notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEOMETRY</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GEOMETRYCOLLECTION</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MULTIPOINT</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MULTIPOLYGON</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POINT</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POLYGON</td>
<td>BYTE_ARRAY</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### JSON data type

<table>
<thead>
<tr>
<th>JSON data type</th>
<th>Parquet primitive type</th>
<th>Logical type annotation</th>
<th>Conversion notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
</tbody>
</table>
**PostgreSQL data type mapping to Parquet**

The following table shows the mapping from PostgreSQL data types to Parquet data types when data is converted and exported to Amazon S3.

<table>
<thead>
<tr>
<th>PostgreSQL data type</th>
<th>Parquet primitive type</th>
<th>Logical type annotation</th>
<th>Mapping notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Numeric data types</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIGINT</td>
<td>INT64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIGSERIAL</td>
<td>INT64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DECIMAL</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td>A DECIMAL type is converted to a string in a BYTE_ARRAY type and encoded as UTF8. This conversion is to avoid complications due to data precision and data values that are not a number (NaN).</td>
</tr>
<tr>
<td>DOUBLE PRECISION</td>
<td>DOUBLE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INTEGER</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MONEY</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>REAL</td>
<td>FLOAT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SERIAL</td>
<td>INT32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMALLINT</td>
<td>INT32</td>
<td>INT_16</td>
<td></td>
</tr>
<tr>
<td>SMALLSERIAL</td>
<td>INT32</td>
<td>INT_16</td>
<td></td>
</tr>
<tr>
<td><strong>String and related data types</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARRAY</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td>An array is converted to a string and encoded as BINARY (UTF8). This conversion is to avoid complications due to data precision, data values that are not a number (NaN), and time data values.</td>
</tr>
<tr>
<td>BIT</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>BIT VARYING</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>BYTEA</td>
<td>BINARY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHAR</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL data type</td>
<td>Parquet primitive type</td>
<td>Logical type annotation</td>
<td>Mapping notes</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------</td>
<td>-------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>CHAR(N)</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>ENUM</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>NAME</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TEXT</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TEXT SEARCH</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>VARCHAR(N)</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>Date and time data types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATE</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>INTERVAL</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TIME</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TIME WITH TIME Zone</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>TIMESTAMP WITH TIME Zone</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>Geometric data types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOX</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>CIRCLE</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>LINE</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>LINESEGMENT</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>PATH</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>POINT</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>POLYGON</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>JSON data types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JSON</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>JSONB</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>Other data types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOOLEAN</td>
<td>BOOLEAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIDR</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td>Network data type</td>
</tr>
<tr>
<td>COMPOSITE</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>DOMAIN</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL data type</td>
<td>Parquet primitive type</td>
<td>Logical type annotation</td>
<td>Mapping notes</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------</td>
<td>-------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>INET</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td>Network data type</td>
</tr>
<tr>
<td>MACADDR</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>OBJECT IDENTIFIER</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PG_LSN</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>RANGE</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
<tr>
<td>UUID</td>
<td>BYTE_ARRAY</td>
<td>STRING</td>
<td></td>
</tr>
</tbody>
</table>
Restoring a DB cluster to a specified time

You can restore a DB cluster to a specific point in time, creating a new DB cluster. When you restore a DB cluster to a point in time, the default DB security group is applied to the new DB cluster. If you need custom DB security groups applied to your DB cluster, you must apply them explicitly using the AWS Management Console, the AWS CLI `modify-db-cluster` command, or the Amazon RDS API `ModifyDBCluster` operation after the DB instance is available.

**Note**
For more information about backing up and restoring an Aurora DB cluster, see Overview of backing up and restoring an Aurora DB cluster (p. 415). For Aurora MySQL, you can restore a provisioned DB cluster to an Aurora Serverless DB cluster. For more information, see Restoring an Aurora Serverless v1 DB cluster (p. 150).

You can restore a DB cluster to a point in time using the AWS Management Console, the AWS CLI, or the RDS API.

**Console**

**To restore a DB cluster to a specified time**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. Choose the DB cluster that you want to restore.
4. For **Actions**, choose **Restore to point in time**.

The Launch DB Instance window appears.
5. Choose **Latest restorable time** to restore to the latest possible time, or choose **Custom** to choose a time.

If you chose **Custom**, enter the date and time to which you want to restore the cluster.

**Note**

Times are shown in Coordinated Universal Time (UTC).

6. For **DB instance identifier**, enter the name of the target restored DB cluster.

7. Choose other options as needed.

8. Choose **Launch DB Instance**.
AWS CLI

To restore a DB cluster to a specified time, use the AWS CLI command `restore-db-cluster-to-point-in-time` to create a new DB cluster.

Example

For Linux, macOS, or Unix:

```bash
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
```

For Windows:

```bash
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
```

RDS API

To restore a DB cluster to a specified time, call the Amazon RDS API `RestoreDBClusterToPointInTime` operation with the following parameters:

- `SourceDBClusterIdentifier`
- `DBClusterIdentifier`
- `RestoreToTime`
Deleting a DB cluster snapshot

You can delete DB cluster snapshots managed by Amazon RDS when you no longer need them.

**Note**
To delete backups managed by AWS Backup, use the AWS Backup console. For information about AWS Backup, see the *AWS Backup Developer Guide*.

Deleting a DB cluster snapshot

You can delete a DB cluster snapshot using the console, the AWS CLI, or the RDS API.

To delete a shared or public snapshot, you must sign in to the AWS account that owns the snapshot.

**Console**

**To delete a DB cluster snapshot**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Snapshots**.
3. Choose the DB cluster snapshot that you want to delete.
4. For **Actions**, choose **Delete Snapshot**.
5. Choose **Delete** on the confirmation page.

**AWS CLI**

You can delete a DB cluster snapshot by using the AWS CLI command `delete-db-cluster-snapshot`.

The following options are used to delete a DB cluster snapshot.

- `--db-cluster-snapshot-identifier` – The identifier for the DB cluster snapshot.

**Example**

The following code deletes the `mydbclustersnapshot` DB cluster snapshot.

For Linux, macOS, or Unix:

```
aws rds delete-db-cluster-snapshot \ 
  --db-cluster-snapshot-identifier mydbclustersnapshot
```

For Windows:

```
aws rds delete-db-cluster-snapshot ^
  --db-cluster-snapshot-identifier mydbclustersnapshot
```

**RDS API**

You can delete a DB cluster snapshot by using the Amazon RDS API operation `DeleteDBClusterSnapshot`.

The following parameters are used to delete a DB cluster snapshot.
• **DBClusterSnapshotIdentifier** – The identifier for the DB cluster snapshot.
Monitoring an Amazon Aurora DB cluster

This section shows how to monitor Amazon Aurora. Aurora involves clusters of database servers that are connected in a replication topology. Monitoring an Aurora cluster typically requires checking the health of multiple DB instances. The instances might have specialized roles, handling mostly write operations, only read operations, or a combination of both. You also monitor the overall health of the cluster by measuring the **replication lag**, the amount of time for changes made by one DB instance to be available to the other instances.

**Topics**
- Overview of monitoring Amazon Aurora (p. 460)
- Viewing an Amazon Aurora DB cluster (p. 473)
- DB cluster status (p. 479)
- DB instance status (p. 481)
- Using Amazon Aurora recommendations (p. 484)
- Monitoring Amazon Aurora DB cluster metrics (p. 489)
- Enhanced Monitoring (p. 504)
- Using Amazon RDS Performance Insights (p. 514)
- Using Database Activity Streams with Amazon Aurora (p. 565)
- Using Amazon RDS event notification (p. 594)
- Viewing Amazon RDS events (p. 612)
- Getting CloudWatch Events and Amazon EventBridge events for Amazon Aurora (p. 614)
- Amazon Aurora database log files (p. 618)
- Working with AWS CloudTrail and Amazon RDS (p. 630)
Overview of monitoring Amazon Aurora

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Aurora and your AWS solutions. To more easily debug multi-point failures, we recommend that you collect monitoring data from all parts of your AWS solution.

Monitoring plan

Before you start monitoring Amazon Aurora, we recommend that you create a monitoring plan. This plan should answer the following questions:

- What are your monitoring goals?
- Which resources will you monitor?
- How often will you monitor these resources?
- Which monitoring tools will you use?
- Who will perform the monitoring tasks?
- Whom should be notified when something goes wrong?

Performance baseline

To achieve your monitoring goals, you need to establish a baseline. To do this, measure performance under different load conditions at various times in your Amazon Aurora environment. You can monitor metrics such as the following:

- Network throughput
- Client connections
- I/O for read, write, or metadata operations
- Burst credit balances for your DB instances

We recommend that you store historical performance data for Amazon Aurora. Using the stored data, you can compare current performance against past trends. You can also distinguish normal performance patterns from anomalies, and devise methods to address issues.

Performance guidelines

In general, acceptable values for performance metrics depend on what your application is doing relative to your baseline. Investigate consistent or trending variances from your baseline. The following metrics are often the source of performance issues:

- **High CPU or RAM consumption** – High values for CPU or RAM consumption might be appropriate, if they’re in keeping with your goals for your application (like throughput or concurrency) and are expected.
- **Disk space consumption** – Investigate disk space consumption if space used is consistently at or above 85 percent of the total disk space. See if it is possible to delete data from the instance or archive data to a different system to free up space.
- **Network traffic** – For network traffic, talk with your system administrator to understand what expected throughput is for your domain network and internet connection. Investigate network traffic if throughput is consistently lower than expected.
- **Database connections** – If you see high numbers of user connections and also decreases in instance performance and response time, consider constraining database connections. The best number of user connections for your DB instance varies based on your instance class and the complexity of the
operations being performed. To determine the number of database connections, associate your DB instance with a parameter group where the *User Connections* parameter is set to a value other than 0 (unlimited). You can either use an existing parameter group or create a new one. For more information, see *Working with DB parameter groups and DB cluster parameter groups* (p. 298).

- **IOPS metrics** – The expected values for IOPS metrics depend on disk specification and server configuration, so use your baseline to know what is typical. Investigate if values are consistently different than your baseline. For best IOPS performance, make sure that your typical working set fits into memory to minimize read and write operations.

When performance falls outside your established baseline, you might need to make changes to optimize your database availability for your workload. For example, you might need to change the instance class of your DB instance. Or you might need to change the number of DB instances and read replicas that are available for clients.

### Monitoring tools

AWS provides various tools that you can use to monitor Amazon Aurora. You can configure some of these tools to do the monitoring for you, and other tools require manual intervention.

#### Automated monitoring tools

We recommend that you automate monitoring tasks as much as possible.

You can use the following automated tools to watch Amazon Aurora and report when something is wrong:

- **Amazon RDS events** – Subscribe to Amazon RDS events to be notified when changes occur with a DB instance, DB cluster, DB cluster snapshot, DB parameter group, or DB security group. For more information, see *Using Amazon RDS event notification* (p. 594).

- **Database log files** – View, download, or watch database log files using the Amazon RDS console or Amazon RDS API operations. You can also query some database log files that are loaded into database tables. For more information, see *Amazon Aurora database log files* (p. 618).

- **Amazon RDS Enhanced Monitoring** – Look at metrics in real time for the operating system. For more information, see *Enhanced Monitoring* (p. 504).

- **Amazon RDS Performance Insights** – Assess the load on your database, and determine when and where to take action. For more information, see *Using Amazon RDS Performance Insights* (p. 514).

- **Amazon RDS recommendations** – Look at automated recommendations for database resources, such as DB instances, DB clusters, and DB cluster parameter groups. For more information, see *Using Amazon Aurora recommendations* (p. 484).

#### Integrated monitoring tools

Amazon RDS integrates with Amazon CloudWatch, Amazon EventBridge, and AWS CloudTrail for additional monitoring capabilities.

- **Amazon CloudWatch** – This service monitors your AWS resources and the applications you run on AWS in real time. You can use the following Amazon CloudWatch features with Amazon Aurora:

  - **Amazon CloudWatch metrics** – Amazon RDS automatically sends metrics to CloudWatch every minute for each active database. You don’t get additional charges for Amazon RDS metrics in CloudWatch. For more information, see the section called “Viewing DB instance metrics” (p. 470).

  - **Amazon CloudWatch alarms** – You can watch a single Amazon RDS metric over a specific time period. You can then perform one or more actions based on the value of the metric relative to a threshold that you set. For more information, see *Monitoring with Amazon CloudWatch* (p. 463).
Monitoring tools

• **Amazon CloudWatch Logs** – Most DB engines enable you to monitor, store, and access your database log files in CloudWatch Logs. For more information, see [Amazon CloudWatch Logs User Guide](#).

• **Amazon EventBridge** – is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, Software-as-a-Service (SaaS) applications, and AWS services and routes that data to targets such as Lambda. This enables you to monitor events that happen in services, and build event-driven architectures. For more information, see [Getting CloudWatch Events and Amazon EventBridge events for Amazon Aurora](#).

• **AWS CloudTrail** – You can view a record of actions taken by a user, role, or an AWS service in Amazon RDS. CloudTrail captures all API calls for Amazon RDS as events. These captures include calls from the Amazon RDS console and from code calls to the Amazon RDS API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon RDS. If you don’t configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. For more information, see [Working with AWS CloudTrail and Amazon RDS](#).

**Manual monitoring tools**

You need to manually monitor those items that the CloudWatch alarms don’t cover. The Amazon RDS, CloudWatch, AWS Trusted Advisor and other AWS console dashboards provide an at-a-glance view of the state of your AWS environment. We recommend that you also check the log files on your DB instance.

• From the Amazon RDS console, you can monitor the following items for your resources:
  • The number of connections to a DB instance
  • The amount of read and write operations to a DB instance
  • The amount of storage that a DB instance is currently using
  • The amount of memory and CPU being used for a DB instance
  • The amount of network traffic to and from a DB instance

• From the Trusted Advisor dashboard, you can review the following cost optimization, security, fault tolerance, and performance improvement checks:
  • Amazon RDS Idle DB Instances
  • Amazon RDS Security Group Access Risk
  • Amazon RDS Backups
  • Amazon RDS Multi-AZ
  • Aurora DB Instance Accessibility

For more information on these checks, see [Trusted Advisor best practices (checks)](#).

• CloudWatch home page shows:
  • Current alarms and status
  • Graphs of alarms and resources
  • Service health status

In addition, you can use CloudWatch to do the following:
  • Create **customized dashboards** to monitor the services that you care about.
  • Graph metric data to troubleshoot issues and discover trends.
  • Search and browse all your AWS resource metrics.
  • Create and edit alarms to be notified of problems.
Monitoring with Amazon CloudWatch

You can monitor DB instances using Amazon CloudWatch, which collects and processes raw data from Amazon Aurora into readable, near real-time metrics. By default, Amazon Aurora metric data is automatically sent to CloudWatch in 1-minute periods. For more information about CloudWatch, see What is Amazon CloudWatch? in the Amazon CloudWatch User Guide.

Data points with a period of 60 seconds (1 minute) are available for 15 days. This means that you can access historical information and gain a better perspective on how your web application or service is performing. For more information about CloudWatch metrics retention, see Metrics retention in the Amazon CloudWatch User Guide.

Note
If you are using Amazon RDS Performance Insights, additional metrics are available. For more information, see Performance Insights metrics published to Amazon CloudWatch (p. 561).

Amazon Aurora metrics and dimensions

When you use Amazon Aurora resources, Amazon Aurora sends metrics and dimensions to Amazon CloudWatch every minute. You can use the following procedures to view the metrics for Amazon Aurora.

To view metrics using the Amazon CloudWatch console

Metrics are grouped first by the service namespace, and then by the various dimension combinations within each namespace.

2. If necessary, change the AWS Region. From the navigation bar, choose the AWS Region where your AWS resources are. For more information, see Regions and endpoints.
3. In the navigation pane, choose Metrics. Choose the RDS metric namespace.
4. Choose a metric dimension, for example **By Database Class**.
5. To sort the metrics, use the column heading. To graph a metric, select the check box next to the metric. To filter by resource, choose the resource ID, and then choose **Add to search**. To filter by metric, choose the metric name, and then choose **Add to search**.

![Amazon Aurora User Guide for Aurora Monitoring with CloudWatch](image)

To view metrics using the AWS CLI
- At a command prompt, use the following command.

```
aws cloudwatch list-metrics --namespace AWS/RDS
```

**Amazon Aurora Metrics**

The **AWS/RDS** namespace includes the following metrics.

**Note**
The Amazon RDS console might display metrics in units that are different from the units sent to Amazon CloudWatch. For example, the Amazon RDS console might display a metric in megabytes (MB), while the metric is sent to Amazon CloudWatch in bytes.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Console name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BinLogDiskUsage</td>
<td>Binary Log Disk Usage (MB)</td>
<td>The amount of disk space occupied by binary logs on the primary. Applies to MySQL read replicas. Units: Bytes</td>
</tr>
<tr>
<td>BurstBalance</td>
<td>Burst Balance (Percent)</td>
<td>The percent of General Purpose SSD (gp2) burst-bucket I/O credits available. Units: Percent</td>
</tr>
<tr>
<td>CPUUtilization</td>
<td>CPU Utilization (Percent)</td>
<td>The percentage of CPU utilization.</td>
</tr>
<tr>
<td>Metric</td>
<td>Console name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CPUCreditUsage      | CPU Credit Usage (Count)      | (T2 instances) The number of CPU credits spent by the instance for CPU utilization. One CPU credit equals one vCPU running at 100 percent utilization for one minute or an equivalent combination of vCPUs, utilization, and time. For example, you might have one vCPU running at 50 percent utilization for two minutes or two vCPUs running at 25 percent utilization for two minutes.  

CPU credit metrics are available at a five-minute frequency only. If you specify a period greater than five minutes, use the Sum statistic instead of the Average statistic.  

Units: Credits (vCPU-minutes)                                                                                                                                                                                                                     |
| CPUCreditBalance    | CPU Credit Balance (Count)    | (T2 instances) The number of earned CPU credits that an instance has accrued since it was launched or started. For T2 Standard, the CPUCreditBalance also includes the number of launch credits that have been accrued.  

Credits are accrued in the credit balance after they are earned, and removed from the credit balance when they are spent. The credit balance has a maximum limit, determined by the instance size. After the limit is reached, any new credits that are earned are discarded. For T2 Standard, launch credits don't count towards the limit.  

The credits in the CPUCreditBalance are available for the instance to spend to burst beyond its baseline CPU utilization.  

When an instance is running, credits in the CPUCreditBalance don't expire. When the instance stops, the CPUCreditBalance does not persist, and all accrued credits are lost.  

CPU credit metrics are available at a five-minute frequency only.  

Units: Credits (vCPU-minutes)                                                                                                                                                                                                                     |
| DatabaseConnections | DB Connections (Count)        | The number of database connections in use.  

The metric value might not include broken database connections that haven't been cleaned up by your database yet. So, the number of database connections recorded by your database might be higher than the metric value.  

Units: Count                                                                                                                                                                                                                                           |
<table>
<thead>
<tr>
<th>Metric</th>
<th>Console name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiskQueueDepth</td>
<td>Queue Depth (Count)</td>
<td>The number of outstanding I/Os (read/write requests) waiting to access the disk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>FailedSQLServerAgentJobsCount</td>
<td>Failed SQL Server Agent Jobs Count (Count/Minute)</td>
<td>The number of failed Microsoft SQL Server Agent jobs during the last minute.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count/Minute</td>
</tr>
<tr>
<td>FreeableMemory</td>
<td>Freeable Memory (MB)</td>
<td>The amount of available random access memory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Aurora, this metric reports the value of the MemAvailable field of /proc/meminfo.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes</td>
</tr>
<tr>
<td>FreeStorageSpace</td>
<td>Free Storage Space (MB)</td>
<td>The amount of available storage space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes</td>
</tr>
<tr>
<td>MaximumUsedTransactionIDs</td>
<td>Maximum Used Transaction IDs (Count)</td>
<td>The maximum transaction IDs that have been used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applies to PostgreSQL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>NetworkReceiveThroughput</td>
<td>Network Receive Throughput (MB/Second)</td>
<td>The incoming (receive) network traffic on the DB instance, including both customer database traffic and Amazon RDS traffic used for monitoring and replication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes/Second</td>
</tr>
<tr>
<td>NetworkTransmitThroughput</td>
<td>Network Transmit Throughput (MB/Second)</td>
<td>The outgoing (transmit) network traffic on the DB instance, including both customer database traffic and Amazon RDS traffic used for monitoring and replication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes/Second</td>
</tr>
<tr>
<td>OldestReplicationSlotLag</td>
<td>Oldest Replication Slot Lag (MB)</td>
<td>The lagging size of the replica lagging the most in terms of write-ahead log (WAL) data received. Applies to PostgreSQL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes</td>
</tr>
<tr>
<td>ReadIOPS</td>
<td>Read IOPS (Count/Second)</td>
<td>The average number of disk read I/O operations per second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Count/Second</td>
</tr>
<tr>
<td>ReadLatency</td>
<td>Read Latency (Milliseconds)</td>
<td>The average amount of time taken per disk I/O operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Seconds</td>
</tr>
<tr>
<td>Metric</td>
<td>Console name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ReadThroughput</td>
<td>Read Throughput (MB/Second)</td>
<td>The average number of bytes read from disk per second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes/Second</td>
</tr>
<tr>
<td>ReplicaLag</td>
<td>Replica Lag (Milliseconds)</td>
<td>The amount of time a read replica DB instance lags behind the source DB instance. Applies to MySQL, MariaDB, Oracle, PostgreSQL, and SQL Server read replicas.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Seconds</td>
</tr>
<tr>
<td>ReplicationSlotDisk</td>
<td>Replica Slot Disk Usage (MB)</td>
<td>The disk space used by replication slot files. Applies to PostgreSQL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes</td>
</tr>
<tr>
<td>SwapUsage</td>
<td>Swap Usage (MB)</td>
<td>The amount of swap space used on the DB instance. This metric is not available for SQL Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes</td>
</tr>
<tr>
<td>TransactionLogsDisk</td>
<td>Transaction Logs Disk Usage</td>
<td>The disk space used by transaction logs. Applies to PostgreSQL.</td>
</tr>
<tr>
<td></td>
<td>(MB)</td>
<td>Units: Bytes</td>
</tr>
<tr>
<td>TransactionLogsGen</td>
<td>Transaction Logs Generation</td>
<td>The size of transaction logs generated per second. Applies to PostgreSQL.</td>
</tr>
<tr>
<td></td>
<td>(MB/Second)</td>
<td>Units: Bytes/Second</td>
</tr>
<tr>
<td>WriteIOPS</td>
<td>Write IOPS (Count/Second)</td>
<td>The average number of disk write I/O operations per second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Count/Second</td>
</tr>
<tr>
<td>WriteLatency</td>
<td>Write Latency (Milliseconds)</td>
<td>The average amount of time taken per disk I/O operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Seconds</td>
</tr>
<tr>
<td>WriteThroughput</td>
<td>Write Throughput (MB/Second)</td>
<td>The average number of bytes written to disk per second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Units: Bytes/Second</td>
</tr>
</tbody>
</table>

**Aurora Dimensions**

You can filter Aurora metrics data by using any dimension in the following table.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBInstanceIdentifier</td>
<td>This dimension filters the data that you request for a specific DB instance.</td>
</tr>
</tbody>
</table>
### Creating CloudWatch alarms to monitor Amazon RDS

You can create a CloudWatch alarm that sends an Amazon SNS message when the alarm changes state. An alarm watches a single metric over a time period that you specify. The alarm can also perform one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic or Amazon EC2 Auto Scaling policy.

Alarms invoke actions for sustained state changes only. CloudWatch alarms don't invoke actions simply because they are in a particular state. The state must have changed and have been maintained for a specified number of time periods. The following procedures show how to create alarms for Amazon RDS.

**Note**

For Aurora, use **WRITER** or **READER** role metrics to set up alarms instead of relying on metrics for specific DB instances. Aurora DB instance roles can change roles over time. You can find these role-based metrics in the CloudWatch console.

Aurora Auto Scaling automatically sets alarms based on **READER** role metrics. For more information about Aurora Auto Scaling, see Using Amazon Aurora Auto Scaling with Aurora replicas (p. 372).

#### To set alarms using the CloudWatch console

2. Choose **Alarms** and then choose **Create Alarm**. Doing this launches the Create Alarm Wizard.
3. Choose **RDS Metrics** and scroll through the Amazon RDS metrics to find the metric that you want to place an alarm on. To display just Amazon RDS metrics, search for the identifier of your resource. Choose the metric to create an alarm on and then choose **Next**.
4. Enter **Name**, **Description**, and **Whenever** values for the metric.
5. If you want CloudWatch to send you an email when the alarm state is reached, for **Whenever this alarm**, choose **State is ALARM**. For **Send notification to**, choose an existing SNS topic. If you choose **Create topic**, you can set the name and email addresses for a new email subscription list. This list is saved and appears in the field for future alarms.
If you use Create topic to create a new Amazon SNS topic, the email addresses must be verified before they receive notifications. Emails are only sent when the alarm enters an alarm state. If this alarm state change happens before the email addresses are verified, the addresses don’t receive a notification.

6. Preview the alarm that you’re about to create in the Alarm Preview area, and then choose Create Alarm.

To set an alarm using the AWS CLI

• Call put-metric-alarm. For more information, see AWS CLI Command Reference.

To set an alarm using the CloudWatch API

• Call PutMetricAlarm. For more information, see Amazon CloudWatch API Reference

Publishing database engine logs to Amazon CloudWatch Logs

You can configure your Amazon Aurora database engine to publish log data to a log group in Amazon CloudWatch Logs. With CloudWatch Logs, you can perform real-time analysis of the log data, and use CloudWatch to create alarms and view metrics. You can use CloudWatch Logs to store your log records in highly durable storage, which you can manage with the CloudWatch Logs Agent. For example, you can determine when to rotate log records from a host to the log service, so you can access the raw logs when you need to.

For engine-specific information, see the following topics:

• Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs (p. 824)
• Publishing Aurora PostgreSQL logs to Amazon CloudWatch Logs (p. 1075)

Before you enable log data publishing, make sure that you have a service-linked role in AWS Identity and Access Management (IAM). For more information about service-linked roles, see Using service-linked roles for Amazon Aurora (p. 1277).

Configuring CloudWatch log integration

To publish your database log files to CloudWatch Logs, choose which logs to publish. Make this choice in the Advanced Settings section when you create a new DB instance. You can also modify an existing DB instance to begin publishing.
After you have enabled publishing, Amazon Aurora continuously streams all of the DB instance log records to a log group. For example, you have a log group `/aws/rds/instance/log_type` for each type of log that you publish. This log group is in the same AWS Region as the database instance that generates the log.

After you have published log records, you can use CloudWatch Logs to search and filter the records. For more information about searching and filtering logs, see Searching and filtering log data.

**Viewing DB instance metrics**

Amazon RDS provides metrics so that you can monitor the health of your DB instances. You can monitor both DB instance metrics and operating system (OS) metrics.

Following, you can find details about how to view metrics for your DB instance using the RDS console and CloudWatch. For information on monitoring metrics for your DB instance's operating system in real time using CloudWatch Logs, see Enhanced Monitoring (p. 504).

**Viewing metrics by using the console**

**To view DB and OS metrics for a DB instance**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that you need information about to show its details.
4. Choose the **Monitoring** tab.
5. For **Monitoring**, choose the option for how you want to view your metrics from these:
   - **CloudWatch** – Shows a summary of DB instance metrics available from Amazon CloudWatch. Each metric includes a graph showing the metric monitored over a specific time span.
   - **Enhanced monitoring** – Shows a summary of OS metrics available for a DB instance with Enhanced Monitoring enabled. Each metric includes a graph showing the metric monitored over a specific time span.
   - **OS Process list** – Shows details for each process running in the selected instance.
   - **Performance Insights** – Opens the Amazon RDS Performance Insights console for your DB instance.
To choose the time range of the metrics represented by the graphs, you can use the time range list.
To bring up a more detailed view, you can choose any graph. You can also apply metric-specific filters to the data.

**Tip**
To choose the time range of the metrics represented by the graphs, you can use the time range list.
To bring up a more detailed view, you can choose any graph. You can also apply metric-specific filters to the data.

**Viewing DB instance metrics with the CLI or API**

Amazon RDS integrates with CloudWatch metrics to provide a variety of DB instance metrics. You can view CloudWatch metrics using the RDS console, AWS CLI, or API.

For a complete list of Amazon RDS metrics, go to Amazon RDS dimensions and metrics in the Amazon CloudWatch User Guide.

**Viewing DB metrics by using the CloudWatch CLI**

**Note**
The following CLI example requires the CloudWatch command line tools. For more information on CloudWatch and to download the developer tools, see Amazon CloudWatch on the AWS website. The Start Time and End Time values supplied in this example are for illustration only. Substitute appropriate start and end time values for your DB instance.
To view usage and performance statistics for a DB instance

- Use the CloudWatch command `mon-get-stats` with the following parameters.

```plaintext
PROMPT> mon-get-stats FreeStorageSpace --dimensions="DBInstanceIdentifier=mydbinstance"
     --statistics= Average
     --namespace="AWS/RDS" --start-time 2009-10-16T00:00:00 --end-time 2009-10-16T00:02:00
```

Viewing DB metrics by using the CloudWatch API

The `StartTime` and `EndTime` values supplied in this example are for illustration only. Substitute appropriate start and end time values for your DB instance.

To view usage and performance statistics for a DB instance

- Call the CloudWatch API `GetMetricStatistics` with the following parameters:
  - `Statistics.member.1 = Average`
  - `Namespace = AWS/RDS`
  - `StartTime = 2009-10-16T00:00:00`
  - `EndTime = 2009-10-16T00:02:00`
  - `Period = 60`
  - `MeasureName = FreeStorageSpace`
Viewing an Amazon Aurora DB cluster

You have several options for viewing information about your Amazon Aurora DB clusters and the DB instances in your DB clusters.

- You can view DB clusters and DB instances in the Amazon RDS console by choosing **Databases** from the navigation pane.
- You can get DB cluster and DB instance information using the AWS Command Line Interface (AWS CLI).
- You can get DB cluster and DB instance information using the Amazon RDS API.

**Console**

In the Amazon RDS, you can see details about a DB cluster by choosing **Databases** from the console's navigation pane. You can also see details about DB instances that are members of an Amazon Aurora DB cluster on the **Databases** page.

The **Databases** list shows all of the DB clusters for your AWS account. When you choose a DB cluster, you see both information about the DB cluster and also a list of the DB instances that are members of that DB cluster. You can choose the identifier for a DB instance in the list to go directly to the details page for that DB instance in the RDS console.

To view the details page for a DB cluster, choose **Databases** in the navigation pane, and then choose the name of the DB cluster.

You can modify your DB cluster by choosing **Databases** from the console's navigation pane to go to the **Databases** list. To modify a DB cluster, select the DB cluster from the **Databases** list and choose **Modify**.

To modify a DB instance that is a member of a DB cluster, choose **Databases** from the console's navigation pane to go to the **Databases** list.

For example, the following image shows the details page for the DB cluster named **aurora-test**. The DB cluster has four DB instances shown in the **DB identifier** list. The writer DB instance, **dbinstance4**, is the primary DB instance for the DB cluster.
If you click the link for the `dbinstance4` DB instance identifier, the Amazon RDS console shows the details page for the `dbinstance4` DB instance, as shown in the following image.
AWS CLI

To view DB cluster information by using the AWS CLI, use the `describe-db-clusters` command. For example, the following AWS CLI command lists the DB cluster information for all of the DB clusters in the `us-east-1` region for the configured AWS account.

```
aws rds describe-db-clusters --region us-east-1
```

The command returns the following output if your AWS CLI is configured for JSON output.

```
{
  "DBClusters": [
  {
    "Status": "available",
    "Engine": "aurora",
    "Endpoint": "sample-cluster1.cluster-123456789012.us-east-1.rds.amazonaws.com",
    "AllocatedStorage": 1,
    "DBClusterIdentifier": "sample-cluster1",
    "MasterUsername": "mymasteruser",
    "EarliestRestorableTime": "2016-03-30T03:35:42.563Z",
  }
  ]
}
```
"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": "5.6.10a",
"DBClusterParameterGroup": "default.aurora5.6",
"BackupRetentionPeriod": 1,
"AvailabilityZones": [
  "us-east-1b",
  "us-east-1c",
  "us-east-1d"
],
"LatestRestorableTime": "2016-03-31T20:06:08.903Z",
"PreferredMaintenanceWindow": "wed:08:15-wed:08:45"
},
{
  "Status": "available",
  "Engine": "aurora",
  "Endpoint": "aurora-sample.cluster-123456789012.us-east-1.rds.amazonaws.com",
  "AllocatedStorage": 1,
  "DBClusterIdentifier": "aurora-sample-cluster",
  "MasterUsername": "mymasteruser",
  "EarliestRestorableTime": "2016-03-30T10:21:34.826Z",
  "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": "5.6.10a",
  "PreferredMaintenanceWindow": "sun:08:15-sun:08:45"
}
"DBClusterParameterGroup": "default.aurora5.6",
"BackupRetentionPeriod": 1,
"AvailabilityZones": [
    "us-east-1b",
    "us-east-1c",
    "us-east-1d"
],
"LatestRestorableTime": "2016-03-31T20:11:49.1Z",
"PreferredMaintenanceWindow": "sun:03:53-sun:04:23"
}
]

### RDS API

To view DB cluster information using the Amazon RDS API, use the `DescribeDBClusters` operation. For example, the following Amazon RDS API command lists the DB cluster information for all of the DB clusters in the `us-east-1` region.

```xml
https://rds.us-east-1.amazonaws.com/
 ?Action=DescribeDBClusters
 &MaxRecords=100
 &SignatureMethod=HmacSHA256
 &SignatureVersion=4
 &Version=2014-10-31
 &X-Amz-Algorithm=AWS4-HMAC-SHA256
 &X-Amz-Credential=AKIADQKE4SARGYLE/20140722/us-east-1/rds/aws4_request
 &X-Amz-Date=20140722T200807Z
 &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
 &X-Amz-Signature=2d4f2b9e8abc31122b5546f94c0499bba47de813cb875f9b9c78e8e19c9afe1b
```

The action returns the following output:

```xml
 <DescribeDBClustersResult>
   <DBClusters>
     <DBCluster>
       <Engine>aurora5.6</Engine>
       <Status>available</Status>
       <BackupRetentionPeriod>0</BackupRetentionPeriod>
       <DBSubnetGroup>my-subgroup</DBSubnetGroup>
       <EngineVersion>5.6.10a</EngineVersion>
       <Endpoint>sample-cluster2.cluster-cbfvmgb0y5fy.us-east-1.rds.amazonaws.com</Endpoint>
       <DBClusterIdentifier>sample-cluster2</DBClusterIdentifier>
       <PreferredBackupWindow>04:45-05:15</PreferredBackupWindow>
       <PreferredMaintenanceWindow>sat:05:56-sat:06:26</PreferredMaintenanceWindow>
     </DBClusterMembers/>
     <AllocatedStorage>15</AllocatedStorage>
     <MasterUsername>awsuser</MasterUsername>
   </DBCluster>
   <DBCluster>
     <Engine>aurora5.6</Engine>
     <Status>available</Status>
     <BackupRetentionPeriod>0</BackupRetentionPeriod>
     <DBSubnetGroup>my-subgroup</DBSubnetGroup>
     <EngineVersion>5.6.10a</EngineVersion>
     <Endpoint>sample-cluster3.cluster-cefgqfx9y5fy.us-east-1.rds.amazonaws.com</Endpoint>
     <DBClusterIdentifier>sample-cluster3</DBClusterIdentifier>
     <PreferredBackupWindow>07:06-07:36</PreferredBackupWindow>
     <PreferredMaintenanceWindow>tue:10:18-tue:10:48</PreferredMaintenanceWindow>
   </DBCluster>
 </DBClusters>
</DescribeDBClustersResponse>
```

477
<DBClusterMembers>
  <DBClusterMember>
    <IsClusterWriter>true</IsClusterWriter>
    <DBInstanceIdentifier>sample-cluster3-master</DBInstanceIdentifier>
  </DBClusterMember>
  <DBClusterMember>
    <IsClusterWriter>false</IsClusterWriter>
    <DBInstanceIdentifier>sample-cluster3-read1</DBInstanceIdentifier>
  </DBClusterMember>
</DBClusterMembers>
<AllocatedStorage>15</AllocatedStorage>
<MasterUsername>awsuser</MasterUsername>
</DBCluster>
</DBClusters>
</DescribeDBClustersResult>
<ResponseMetadata>
  <RequestId>d682b02c-1383-11b4-a6bb-172dfac7f170</RequestId>
</ResponseMetadata>
</DescribeDBClustersResponse>
DB cluster status

The status of a DB cluster indicates the health of the DB cluster. You can view the status of a DB cluster by using the Amazon RDS console, the AWS CLI command `describe-db-clusters`, or the API operation `DescribeDBClusters`.

**Note**
Aurora also uses another status called *maintenance status*, which is shown in the Maintenance column of the Amazon RDS console. This value indicates the status of any maintenance patches that need to be applied to a DB cluster. Maintenance status is independent of DB cluster status. For more information on *maintenance status*, see Applying updates for a DB cluster (p. 390).

Find the possible status values for DB clusters in the following table.

<table>
<thead>
<tr>
<th>DB cluster status</th>
<th>Billed</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>available</td>
<td>Billed</td>
<td>The DB cluster is healthy and available. When an Aurora Serverless cluster is available and paused, you're billed for storage only.</td>
</tr>
<tr>
<td>backing-up</td>
<td>Billed</td>
<td>The DB cluster is currently being backed up.</td>
</tr>
<tr>
<td>backtracking</td>
<td>Billed</td>
<td>The DB cluster is currently being backtracked. This status only applies to Aurora MySQL.</td>
</tr>
<tr>
<td>cloning-failed</td>
<td>Not billed</td>
<td>Cloning a DB cluster failed.</td>
</tr>
<tr>
<td>creating</td>
<td>Not billed</td>
<td>The DB cluster is being created. The DB cluster is inaccessible while it is being created.</td>
</tr>
<tr>
<td>deleting</td>
<td>Not billed</td>
<td>The DB cluster is being deleted.</td>
</tr>
<tr>
<td>failing-over</td>
<td>Billed</td>
<td>A failover from the primary instance to an Aurora Replica is being performed.</td>
</tr>
<tr>
<td>inaccessible-encryption-credentials</td>
<td>Not billed</td>
<td>The AWS Key Management Service customer master key (CMK) used to encrypt or decrypt the DB cluster can't be accessed.</td>
</tr>
<tr>
<td>maintenance</td>
<td>Billed</td>
<td>Amazon RDS is applying a maintenance update to the DB cluster. This status is used for DB cluster-level maintenance that RDS schedules well in advance.</td>
</tr>
<tr>
<td>migrating</td>
<td>Billed</td>
<td>A DB cluster snapshot is being restored to a DB cluster.</td>
</tr>
<tr>
<td>migration-failed</td>
<td>Not billed</td>
<td>A migration failed.</td>
</tr>
<tr>
<td>modifying</td>
<td>Billed</td>
<td>The DB cluster is being modified because of a customer request to modify the DB cluster.</td>
</tr>
<tr>
<td>promoting</td>
<td>Billed</td>
<td>A read replica is being promoted to a standalone DB cluster.</td>
</tr>
<tr>
<td>renaming</td>
<td>Billed</td>
<td>The DB cluster is being renamed because of a customer request to rename it.</td>
</tr>
<tr>
<td>DB cluster status</td>
<td>Billed</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>resetting-master-credentials</td>
<td>Billed</td>
<td>The master credentials for the DB cluster are being reset because of a customer request to reset them.</td>
</tr>
<tr>
<td>starting</td>
<td>Billed for storage</td>
<td>The DB cluster is starting.</td>
</tr>
<tr>
<td>stopped</td>
<td>Billed for storage</td>
<td>The DB cluster is stopped.</td>
</tr>
<tr>
<td>stopping</td>
<td>Billed for storage</td>
<td>The DB cluster is being stopped.</td>
</tr>
<tr>
<td>update-iam-db-auth</td>
<td>Billed</td>
<td>IAM authorization for the DB cluster is being updated.</td>
</tr>
<tr>
<td>upgrading</td>
<td>Billed</td>
<td>The DB cluster engine version is being upgraded.</td>
</tr>
</tbody>
</table>
DB instance status

The status of a DB instance indicates the health of the DB instance. You can view the status of a DB instance by using the Amazon RDS console, the AWS CLI command `describe-db-instances`, or the API operation `DescribeDBInstances`.

Note
Amazon RDS also uses another status called `maintenance status`, which is shown in the `Maintenance` column of the Amazon RDS console. This value indicates the status of any maintenance patches that need to be applied to a DB instance. Maintenance status is independent of DB instance status. For more information on `maintenance status`, see Applying updates for a DB cluster (p. 390).

Find the possible status values for DB instances in the following table, which also shows how you are billed for each status. It shows if you will be billed for the DB instance and storage, billed only for storage, or not billed. For all DB instance statuses, you are always billed for backup usage.

<table>
<thead>
<tr>
<th>DB instance status</th>
<th>Billed</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>available</td>
<td>Billed</td>
<td>The DB instance is healthy and available.</td>
</tr>
<tr>
<td>backing-up</td>
<td>Billed</td>
<td>The DB instance is currently being backed up.</td>
</tr>
<tr>
<td>backtracking</td>
<td>Billed</td>
<td>The DB instance is currently being backtracked. This status only applies to Aurora MySQL.</td>
</tr>
<tr>
<td>configuring-enhanced-monitoring</td>
<td>Billed</td>
<td>Enhanced Monitoring is being enabled or disabled for this DB instance.</td>
</tr>
<tr>
<td>configuring-iam-database-auth</td>
<td>Billed</td>
<td>AWS Identity and Access Management (IAM) database authentication is being enabled or disabled for this DB instance.</td>
</tr>
<tr>
<td>configuring-log-exports</td>
<td>Billed</td>
<td>Publishing log files to Amazon CloudWatch Logs is being enabled or disabled for this DB instance.</td>
</tr>
<tr>
<td>converting-to-vpc</td>
<td>Billed</td>
<td>The DB instance is being converted from a DB instance that is not in an Amazon Virtual Private Cloud (Amazon VPC) to a DB instance that is in an Amazon VPC.</td>
</tr>
<tr>
<td>creating</td>
<td>Not billed</td>
<td>The DB instance is being created. The DB instance is inaccessible while it is being created.</td>
</tr>
<tr>
<td>deleting</td>
<td>Not billed</td>
<td>The DB instance is being deleted.</td>
</tr>
<tr>
<td>failed</td>
<td>Not billed</td>
<td>The DB instance has failed and Amazon RDS can't recover it. Perform a point-in-time restore to the latest restorable time of the DB instance to recover the data.</td>
</tr>
<tr>
<td>inaccessible-encryption-credentials</td>
<td>Not billed</td>
<td>The AWS KMS customer master key (CMK) used to encrypt or decrypt the DB instance can't be accessed.</td>
</tr>
<tr>
<td>incompatible-network</td>
<td>Not billed</td>
<td>Amazon RDS is attempting to perform a recovery action on a DB instance but can't do so because the VPC is in a state that prevents the action from being completed. This status can occur if, for example, all available IP addresses in a subnet are in use and Amazon RDS can't get an IP address for the DB instance.</td>
</tr>
<tr>
<td>DB instance status</td>
<td>Billed</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>incompatible-option-group</td>
<td>Billed</td>
<td>Amazon RDS attempted to apply an option group change but can't do so, and Amazon RDS can't roll back to the previous option group state. For more information, check the <strong>Recent Events</strong> list for the DB instance. This status can occur if, for example, the option group contains an option such as TDE and the DB instance doesn't contain encrypted information.</td>
</tr>
<tr>
<td>incompatible-parameters</td>
<td>Billed</td>
<td>Amazon RDS can't start the DB instance because the parameters specified in the DB instance's DB parameter group aren't compatible with the DB instance. Revert the parameter changes or make them compatible with the DB instance to regain access to your DB instance. For more information about the incompatible parameters, check the <strong>Recent Events</strong> list for the DB instance.</td>
</tr>
<tr>
<td>incompatible-restore</td>
<td>Not billed</td>
<td>Amazon RDS can't do a point-in-time restore. Common causes for this status include using temp tables, using MyISAM tables with MySQL, or using Aria tables with MariaDB.</td>
</tr>
<tr>
<td>maintenance</td>
<td>Billed</td>
<td>Amazon RDS is applying a maintenance update to the DB instance. This status is used for instance-level maintenance that RDS schedules well in advance.</td>
</tr>
<tr>
<td>modifying</td>
<td>Billed</td>
<td>The DB instance is being modified because of a customer request to modify the DB instance.</td>
</tr>
<tr>
<td>moving-to-vpc</td>
<td>Billed</td>
<td>The DB instance is being moved to a new Amazon Virtual Private Cloud (Amazon VPC).</td>
</tr>
<tr>
<td>rebooting</td>
<td>Billed</td>
<td>The DB instance is being rebooted because of a customer request or an Amazon RDS process that requires the rebooting of the DB instance.</td>
</tr>
<tr>
<td>renaming</td>
<td>Billed</td>
<td>The DB instance is being renamed because of a customer request to rename it.</td>
</tr>
<tr>
<td>resetting-master-credentials</td>
<td>Billed</td>
<td>The master credentials for the DB instance are being reset because of a customer request to reset them.</td>
</tr>
<tr>
<td>restore-error</td>
<td>Billed</td>
<td>The DB instance encountered an error attempting to restore to a point-in-time or from a snapshot.</td>
</tr>
<tr>
<td>starting</td>
<td>Billed</td>
<td>The DB instance is starting.</td>
</tr>
<tr>
<td>stopped</td>
<td>Billed</td>
<td>The DB instance is stopped.</td>
</tr>
<tr>
<td>stopping</td>
<td>Billed</td>
<td>The DB instance is being stopped.</td>
</tr>
<tr>
<td>DB instance status</td>
<td>Billed</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>storage-full</td>
<td>Billed</td>
<td>The DB instance has reached its storage capacity allocation. This is a critical status, and we recommend that you fix this issue immediately. To do so, scale up your storage by modifying the DB instance. To avoid this situation, set Amazon CloudWatch alarms to warn you when storage space is getting low.</td>
</tr>
<tr>
<td>storage-optimization</td>
<td>Billed</td>
<td>Your DB instance is being modified to change the storage size or type. The DB instance is fully operational. However, while the status of your DB instance is <strong>storage-optimization</strong>, you can't request any changes to the storage of your DB instance. The storage optimization process is usually short, but can sometimes take up to and even beyond 24 hours.</td>
</tr>
<tr>
<td>upgrading</td>
<td>Billed</td>
<td>The database engine version is being upgraded.</td>
</tr>
</tbody>
</table>
Using Amazon Aurora recommendations

Amazon Aurora provides automated recommendations for database resources, such as DB instances, DB clusters, and DB cluster parameter groups. These recommendations provide best practice guidance by analyzing DB cluster configuration, DB instance configuration, usage, and performance data.

You can find examples of these recommendations in the following table.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Recommendation</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nondefault custom memory parameters</td>
<td>Your DB parameter group sets memory parameters that diverge too much from the default values.</td>
<td>Settings that diverge too much from the default values can cause poor performance and errors. We recommend setting custom memory parameters to their default values in the DB parameter group used by the DB instance.</td>
<td>Working with DB parameter groups and DB cluster parameter groups (p. 298)</td>
</tr>
<tr>
<td>Change buffering enabled for a MySQL DB instance</td>
<td>Your DB parameter group has change buffering enabled.</td>
<td>Change buffering allows a MySQL DB instance to defer some writes necessary to maintain secondary indexes. This configuration can improve performance slightly, but it can create a large delay in crash recovery. During crash recovery, the secondary index must be brought up to date. So, the benefits of change buffering are outweighed by the potentially very long crash recovery events. We recommend disabling change buffering.</td>
<td>Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance on the AWS Database Blog</td>
</tr>
<tr>
<td>Logging to table</td>
<td>Your DB parameter group sets logging output to TABLE.</td>
<td>Setting logging output to TABLE uses more storage than setting this parameter to FILE. To avoid reaching the storage limit, we recommend setting the logging output parameter to FILE.</td>
<td>MySQL database log files (p. 622)</td>
</tr>
<tr>
<td>DB cluster with one DB instance</td>
<td>Your DB cluster only contains one DB instance.</td>
<td>For improved performance and availability, we recommend adding another DB instance with the same DB instance class in a different Availability Zone.</td>
<td>High availability for Amazon Aurora (p. 55)</td>
</tr>
<tr>
<td>DB cluster in one Availability Zone</td>
<td>Your DB cluster has all of its DB instances in the same Availability Zone.</td>
<td>For improved availability, we recommend adding another DB instance with the same DB instance class in a different Availability Zone.</td>
<td>High availability for Amazon Aurora (p. 55)</td>
</tr>
<tr>
<td>DB cluster outdated</td>
<td>Your DB cluster is running an older engine version.</td>
<td>We recommend that you keep your DB cluster at the most current minor version because it includes the latest security and functionality fixes. Unlike major version upgrades, minor version upgrades include only changes.</td>
<td>Maintaining an Amazon Aurora DB cluster (p. 388)</td>
</tr>
</tbody>
</table>
Amazon Aurora generates recommendations for a resource when the resource is created or modified. Amazon Aurora also periodically scans your resources and generates recommendations.

**Responding to Amazon Aurora recommendations**

You can find recommendations in the AWS Management Console. You can perform the recommended action immediately, schedule it for the next maintenance window, or dismiss it.

**To respond to Amazon Aurora recommendations**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Recommendations**.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Recommendation</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB cluster with different parameter groups</td>
<td>Your DB cluster has different DB parameter groups assigned to its DB instances.</td>
<td>Using different parameter groups can cause incompatibilities between the DB instances. To avoid problems and for easier maintenance, we recommend using the same parameter group for all of the DB instances in the DB cluster.</td>
<td>Working with DB parameter groups and DB cluster parameter groups (p. 298)</td>
</tr>
<tr>
<td>DB cluster with different DB instance classes</td>
<td>Your DB cluster has DB instances that use different DB instance classes.</td>
<td>Using different DB instance classes for DB instances can cause problems. For example, performance might suffer if a less powerful DB instance class is promoted to replace a more powerful DB instance class. To avoid problems and for easier maintenance, we recommend using the same DB instance class for all of the DB instances in the DB cluster.</td>
<td>Aurora Replicas (p. 57)</td>
</tr>
</tbody>
</table>
The Recommendations page appears.

3. On the **Recommendations** page, choose one of the following:

- **Active** – Shows the current recommendations that you can apply, dismiss, or schedule.
- **Dismissed** – Shows the recommendations that have been dismissed. When you choose **Dismissed**, you can apply these dismissed recommendations.
- **Scheduled** – Shows the recommendations that are scheduled but not yet applied. These recommendations will be applied in the next scheduled maintenance window.
- **Applied** – Shows the recommendations that are currently applied.
From any list of recommendations, you can open a section to view the recommendations in that section.

**Recommendations**

<table>
<thead>
<tr>
<th>Active (2)</th>
<th>Dismissed (0)</th>
<th>Scheduled (0)</th>
<th>Applied (0)</th>
</tr>
</thead>
</table>

**Heterogeneous instance classes in DB cluster**

**DB clusters**

- **Resource**: cluster-1
- **Recommendation**: Your DB cluster cluster-1 has DB instances that use different DB instance classes. Using different DB instance classes for DB instances can cause problems. To avoid problems and for easier maintenance, we recommend using db.r3/small for all of the DB instances in the DB cluster.

<table>
<thead>
<tr>
<th>DB clusters</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-1</td>
</tr>
</tbody>
</table>

**Heterogeneous parameters for DB cluster**

**DB clusters**

- **Resource**: cluster-1
- **Recommendation**: Your DB cluster cluster-1 has DB instances that use different DB instance classes. Using different DB instance classes for DB instances can cause problems. To avoid problems and for easier maintenance, we recommend using db.r3/small for all of the DB instances in the DB cluster.

<table>
<thead>
<tr>
<th>DB clusters</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-1</td>
</tr>
</tbody>
</table>

To configure preferences for displaying recommendations in each section, choose the **Preferences** icon.

From the Preferences window that appears, you can set display options. These options include the visible columns and the number of recommendations to display on the page.

4. **Manage your active recommendations**:
   a. Choose **Active** and open one or more sections to view the recommendations in them.
   b. Choose one or more recommendations and choose **Apply now** (to apply them immediately), **Schedule** (to apply them in next maintenance window), or **Dismiss**.

If the **Apply now** button appears for a recommendation but is unavailable (grayed out), the DB instance is not available. You can apply recommendations immediately only if the DB instance status is **available**. For example, you can't apply recommendations immediately to the DB
instance if its status is **modifying**. In this case, wait for the DB instance to be available and then
apply the recommendation.

If the **Apply now** button doesn't appear for a recommendation, you can't apply the
recommendation using the **Recommendations** page. You can modify the DB instance to apply
the recommendation manually.

For more information about modifying a DB cluster, see Modifying an Amazon Aurora DB
cluster (p. 327).

**Note**
When you choose **Apply now**, a brief DB instance outage might result.
Monitoring Amazon Aurora DB cluster metrics

To determine the health and performance of your Aurora DB cluster, you can monitor Amazon CloudWatch metrics. You can access metrics using the Amazon RDS Management Console, AWS CLI, and CloudWatch API. For more information, see Monitoring an Amazon Aurora DB cluster (p. 459).

**Note**
If you are using Amazon RDS Performance Insights, additional metrics are available. For more information, see Performance Insights metrics published to Amazon CloudWatch (p. 561).

Amazon Aurora metrics

The AWS/RDS namespace includes the following metrics that apply to database entities running on Amazon Aurora. Some metrics apply to either Aurora MySQL, Aurora PostgreSQL, or both. Furthermore, some metrics are specific to a cluster, primary instance, replica instance, or all instances.

For Aurora global database metrics, see Amazon CloudWatch metrics for write forwarding (p. 242). For Aurora parallel query metrics, see Monitoring parallel query (p. 712).

Cluster-level metrics for Amazon Aurora

The following table describes metrics that are specific to Aurora clusters.

### Cluster-specific metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Applies to</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuroraGlobalDBReplicatedWriteIO</td>
<td>In an Aurora Global Database, the number of write I/O operations replicated from the primary AWS Region to the cluster volume in a secondary AWS Region. The billing calculations for the secondary AWS Regions in a global database use VolumeWriteIOPS to account for writes performed within the cluster. The billing calculations for the primary AWS Region in a global database use VolumeWriteIOPS to account for the write activity within that cluster, and AuroraGlobalDBReplicatedWriteIO to account for cross-Region replication within the global database.</td>
<td>Aurora MySQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>AuroraGlobalDBDataTransferBytes</td>
<td>In an Aurora Global Database, the amount of redo log data transferred from the master AWS Region to a secondary AWS Region.</td>
<td>Aurora MySQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Applies to</td>
<td>Units</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>AuroraGlobalDBReplicationLag</td>
<td>For an Aurora Global Database, the amount of lag when replicating updates from the primary AWS Region.</td>
<td>Aurora MySQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>AuroraVolumeBytesLeftTotal</td>
<td>The remaining available space for the cluster volume. As the cluster volume grows, this value decreases. If it reaches zero, the cluster reports an out-of-space error. If you want to detect whether your Aurora cluster is approaching the size limit of 128 tebibytes (TiB), this value is simpler and more reliable to monitor than VolumeBytesUsed. AuroraVolumeBytesLeftTotal takes into account storage used for internal housekeeping and other allocations that don't affect your storage billing. This parameter is available in more recent Aurora versions. For Aurora MySQL with MySQL 5.6 compatibility, use Aurora version 1.19.5 or higher. For Aurora MySQL with MySQL 5.7 compatibility, use Aurora version 2.04.5 or higher.</td>
<td>Aurora MySQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>BacktrackChangeRecordsCreationRate</td>
<td>The number of backtrack change records created over 5 minutes for your DB cluster.</td>
<td>Aurora MySQL</td>
<td>Count per 5 minutes</td>
</tr>
<tr>
<td>BacktrackChangeRecordsStored</td>
<td>The number of backtrack change records used by your DB cluster.</td>
<td>Aurora MySQL</td>
<td>Count</td>
</tr>
<tr>
<td>BackupRetentionPeriodStorageUsed</td>
<td>The total amount of backup storage used to support the point-in-time restore feature within the Aurora DB cluster's backup retention window. This amount is included in the total reported by the TotalBackupStorageBilled metric. It is computed separately for each Aurora cluster. For instructions, see Understanding Aurora backup storage usage (p. 417).</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Applies to</td>
<td>Units</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>ServerlessDatabaseCapacity</td>
<td>The current capacity of an Aurora Serverless v1 DB cluster.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Count</td>
</tr>
<tr>
<td>SnapshotStorageUsed</td>
<td>The total amount of backup storage consumed by all Aurora snapshots for an Aurora DB cluster outside its backup retention window. This amount is included in the total reported by the TotalBackupStorageBilled metric. It is computed separately for each Aurora cluster. For instructions, see Understanding Aurora backup storage usage (p. 417).</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>TotalBackupStorageBilled</td>
<td>The total amount of backup storage in bytes for which you are billed for a given Aurora DB cluster. The metric includes the backup storage measured by the BackupRetentionPeriodStorageUsed and SnapshotStorageUsed metrics. This metric is computed separately for each Aurora cluster. For instructions, see Understanding Aurora backup storage usage (p. 417).</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>VolumeBytesUsed</td>
<td>The amount of storage used by your Aurora DB instance. This value affects the cost of the Aurora DB cluster (for pricing information, see the Amazon RDS product page). This value doesn't reflect some internal storage allocations that don't affect storage billing. Thus, you can anticipate out-of-space issues more accurately by testing whether AuroraVolumeBytesLeftTotal is approaching zero instead of comparing VolumeBytesUsed against the storage limit of 128 TiB.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Applies to</td>
<td>Units</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>VolumeReadIOPs</td>
<td>The number of billed read I/O operations from a cluster volume within a 5-minute interval.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Count per 5 minutes</td>
</tr>
<tr>
<td></td>
<td>Billed read operations are calculated at the cluster volume level, aggregated from all instances in the Aurora DB cluster, and then reported at 5-minute intervals. The value is calculated by taking the value of the Read operations metric over a 5-minute period. You can determine the amount of billed read operations per second by taking the value of the Billed read operations metric and dividing by 300 seconds. For example, if the Billed read operations returns 13,686, then the billed read operations per second is 45 (13,686 / 300 = 45.62). You accrue billed read operations for queries that request database pages that aren't in the buffer cache and must be loaded from storage. You might see spikes in billed read operations as query results are read from storage and then loaded into the buffer cache.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VolumeWriteIOPs</td>
<td>The number of write disk I/O operations to the cluster volume, reported at 5-minute intervals. For a detailed description of how billed write operations are calculated, see VolumeReadIOPs.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Count per 5 minutes</td>
</tr>
</tbody>
</table>

**Instance-level metrics for Amazon Aurora**

The following instance-specific CloudWatch metrics apply to all Aurora MySQL and Aurora PostgreSQL instances unless noted otherwise.
## Instance-specific metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Applies to</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>AbortedClients</td>
<td>The number of client connections that have not been closed properly.</td>
<td>Aurora MySQL</td>
<td>Count</td>
</tr>
<tr>
<td>ActiveTransactions</td>
<td>The average number of current transactions executing on an Aurora database instance per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td></td>
<td>By default, Aurora doesn't enable this metric. To begin measuring this value, set <code>innodb_monitor_enable='all'</code> in the DB parameter group for a specific DB instance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AuroraBinlogReplicaLag</td>
<td>The amount of time a replica DB cluster running on Aurora with MySQL compatibility lags behind the source DB cluster.</td>
<td>Primary for Aurora MySQL</td>
<td>Seconds</td>
</tr>
<tr>
<td></td>
<td>This metric reports the value of the <code>Seconds_Behind_Master</code> field of the MySQL <code>SHOW SLAVE STATUS</code> command. This metric is useful for monitoring replica lag between Aurora DB clusters that are replicating across different AWS Regions. For more information, see <a href="#">Aurora MySQL replication</a>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AuroraReplicaLag</td>
<td>For an Aurora replica, the amount of lag when replicating updates from the primary instance.</td>
<td>Replica for Aurora MySQL and Aurora PostgreSQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>AuroraReplicaLagMaximum</td>
<td>The maximum amount of lag between the primary instance and each Aurora DB instance in the DB cluster.</td>
<td>Primary for Aurora MySQL and Aurora PostgreSQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>AuroraReplicaLagMinimum</td>
<td>The minimum amount of lag between the primary instance and each Aurora DB instance in the DB cluster.</td>
<td>Primary for Aurora MySQL and Aurora PostgreSQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Applies to</td>
<td>Units</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>BacktrackWindowActual</td>
<td>The difference between the target backtrack window and the actual backtrack window.</td>
<td>Primary for Aurora MySQL</td>
<td>Minutes</td>
</tr>
<tr>
<td>BacktrackWindowAlert</td>
<td>The number of times that the actual backtrack window is smaller than the target backtrack window for a given period of time.</td>
<td>Primary for Aurora MySQL</td>
<td>Count</td>
</tr>
<tr>
<td>BinLogDiskUsage</td>
<td>The amount of disk space occupied by binary logs on the primary instance.</td>
<td>Primary for Aurora MySQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>BlockedTransactions</td>
<td>The average number of transactions in the database that are blocked per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>BufferCacheHitRatio</td>
<td>The percentage of requests that are served by the buffer cache.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Percentage</td>
</tr>
<tr>
<td>CommitLatency</td>
<td>The latency for commit operations.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>CommitThroughput</td>
<td>The average number of commit operations per second.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>CPUCreditBalance</td>
<td>The number of CPU credits that an instance has accumulated, reported at 5-minute intervals. This metric applies only to db.t2.small and db.t2.medium instances. You can use this metric to determine how long an Aurora MySQL DB instance can burst beyond its baseline performance level at a given rate.</td>
<td>Aurora MySQL</td>
<td>Count</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Applies to</td>
<td>Units</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>CPUCreditUsage</td>
<td>The number of CPU credits consumed during the specified period, reported at 5-minute intervals. This metric applies only to db.t2.small and db.t2.medium instances. This metric measures the amount of time during which physical CPUs have been used for processing instructions by virtual CPUs allocated to the Aurora MySQL DB instance.</td>
<td>Aurora MySQL</td>
<td>Count</td>
</tr>
<tr>
<td>CPUUtilization</td>
<td>The percentage of CPU used by an Aurora DB instance.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Percentage</td>
</tr>
<tr>
<td>DatabaseConnections</td>
<td>The number of connections to an Aurora DB instance.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Count</td>
</tr>
<tr>
<td>DDLLatency</td>
<td>The latency for data definition language (DDL) requests such as example, create, alter, and drop requests.</td>
<td>Aurora MySQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>DDLThroughput</td>
<td>The average number of DDL requests per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>Deadlocks</td>
<td>The average number of deadlocks in the database per second.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>DeleteLatency</td>
<td>The latency for delete queries.</td>
<td>Aurora MySQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>DeleteThroughput</td>
<td>The average number of delete queries per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>DiskQueueDepth</td>
<td>The number of outstanding read/write requests waiting to access the disk.</td>
<td>Aurora PostgreSQL</td>
<td>Count</td>
</tr>
<tr>
<td>DMLLatency</td>
<td>The latency for inserts, updates, and deletes.</td>
<td>Aurora MySQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>DMLThroughput</td>
<td>The average number of inserts, updates, and deletes per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Applies to</td>
<td>Units</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>EngineUptime</td>
<td>The amount of time that the instance has been running.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Seconds</td>
</tr>
<tr>
<td>FreeableMemory</td>
<td>The amount of available random access memory.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Megabytes</td>
</tr>
<tr>
<td>FreeLocalStorage</td>
<td>The amount of local storage available.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Megabytes</td>
</tr>
<tr>
<td></td>
<td>Unlike for other DB engines, for Aurora DB instances this metric reports the amount of storage available to each DB instance. This value depends on the DB instance class (for pricing information, see the Amazon RDS product page). You can increase the amount of free storage space for an instance by choosing a larger DB instance class for your instance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>InsertLatency</td>
<td>The latency for insert queries.</td>
<td>Aurora MySQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>InsertThroughput</td>
<td>The average number of insert queries per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>LoginFailures</td>
<td>The average number of failed login attempts per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>MaximumUsedTransactionIDs</td>
<td>The age of the oldest unvacuumed transaction ID, in transactions. If this value reaches 2,146,483,648 (2^31 - 1,000,000), the database is forced into read-only mode, to avoid transaction ID wraparound. For more information, see Preventing transaction ID wraparound failures in the PostgreSQL documentation.</td>
<td>Aurora PostgreSQL</td>
<td>Count</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Applies to</td>
<td>Units</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>NetworkReceiveThroughput</td>
<td>The amount of network throughput received from clients by each instance in the Aurora MySQL DB cluster. This throughput doesn't include network traffic between instances in the Aurora DB cluster and the cluster volume.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Bytes per second (console shows Megabytes per second)</td>
</tr>
<tr>
<td>NetworkThroughput</td>
<td>The amount of network throughput both received from and transmitted to clients by each instance in the Aurora MySQL DB cluster. This throughput doesn't include network traffic between instances in the DB cluster and the cluster volume.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Bytes per second</td>
</tr>
<tr>
<td>NetworkTransmitThroughput</td>
<td>The amount of network throughput sent to clients by each instance in the Aurora DB cluster. This throughput doesn't include network traffic between instances in the DB cluster and the cluster volume.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Bytes per second (console shows Megabytes per second)</td>
</tr>
<tr>
<td>NumBinaryLogFiles</td>
<td>The number of binlog files generated.</td>
<td>Aurora MySQL</td>
<td>Count</td>
</tr>
<tr>
<td>Queries</td>
<td>The average number of queries executed per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>RDSToAuroraPostgreSQLReplicaLag</td>
<td>The lag when replicating updates from the primary RDS PostgreSQL instance to other nodes in the cluster.</td>
<td>Replica for Aurora PostgreSQL</td>
<td>Seconds</td>
</tr>
<tr>
<td>ReadIOPS</td>
<td>The average number of disk I/O operations per second.</td>
<td>Aurora PostgreSQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>ReadLatency</td>
<td>The average amount of time taken per disk I/O operation.</td>
<td>Aurora MySQL and Aurora PostgreSQL</td>
<td>Seconds</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Applies to</td>
<td>Units</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>ReadThroughput</td>
<td>The average number of bytes read from disk per second.</td>
<td>Aurora PostgreSQL</td>
<td>Bytes per second</td>
</tr>
<tr>
<td>ResultSetCacheHitRatio</td>
<td>The percentage of requests that are served by the Resultset cache.</td>
<td>Aurora MySQL</td>
<td>Percentage</td>
</tr>
<tr>
<td>RollbackSegmentHistoryListLength</td>
<td>The undo logs that record committed transactions with delete-marked records. These records are scheduled to be processed by the InnoDB purge operation.</td>
<td>Aurora MySQL</td>
<td></td>
</tr>
<tr>
<td>RowLockTime</td>
<td>The total time spent acquiring row locks for InnoDB tables.</td>
<td>Aurora MySQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>SelectLatency</td>
<td>The latency for select queries.</td>
<td>Aurora MySQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>SelectThroughput</td>
<td>The average number of select queries per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
<tr>
<td>SumBinaryLogSize</td>
<td>The total size of the binlog files.</td>
<td>Aurora MySQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>SwapUsage</td>
<td>The amount of swap space used on the Aurora PostgreSQL DB instance.</td>
<td>Aurora PostgreSQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>TransactionLogsDiskUsage</td>
<td>The amount of disk space consumed by transaction logs on the Aurora PostgreSQL DB instance. This metric is only generated when Aurora PostgreSQL is using logical replication or AWS Database Migration Service. By default, Aurora PostgreSQL uses log records, not transaction logs. When transaction logs aren't in use, the value for this metric is -1.</td>
<td>Primary for Aurora PostgreSQL</td>
<td>Bytes</td>
</tr>
<tr>
<td>UpdateLatency</td>
<td>The latency for update queries.</td>
<td>Aurora MySQL</td>
<td>Milliseconds</td>
</tr>
<tr>
<td>UpdateThroughput</td>
<td>The average number of update queries per second.</td>
<td>Aurora MySQL</td>
<td>Count per second</td>
</tr>
</tbody>
</table>
## View Aurora metrics in the Amazon RDS console

To monitor the health and performance of your Aurora DB cluster, you can view some, but not all, of the metrics provided by Amazon Aurora in the Amazon RDS console. For a detailed list of Aurora metrics available to the Amazon RDS console, see [Aurora metrics available in the Amazon RDS console](p. 501).

### To view Aurora metrics in the Amazon RDS console

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Instances**.
3. Choose the name of the DB instance you want to monitor to see its details.
4. In the Cloudwatch section, choose one of the following options from **Monitoring** for how you want to view your metrics:
   - **Cloudwatch** – Shows a summary of CloudWatch metrics. Each metric includes a graph showing the metric monitored over a specific time span. For more information, see [Monitoring with Amazon CloudWatch](p. 463).
   - **Enhanced monitoring** – Shows a summary of OS metrics available to an Aurora DB instance with Enhanced Monitoring enabled. Each metric includes a graph showing the metric monitored over a specific time span. For more information, see [Enhanced Monitoring](p. 504).
   - **OS process list** – Shows the processes running on the DB instance or DB cluster and their related metrics including CPU percentage, memory usage, and so on.
5. The following image shows the metrics view with Enhanced monitoring selected.
Aurora metrics available in the Amazon RDS console

Not all of the metrics provided by Amazon Aurora are available to you in the Amazon RDS console. You can view them using other tools, however, such as the AWS CLI and CloudWatch API. In addition, some of the metrics that are available in the Amazon RDS console are either shown only for specific instance classes, or with different names and different units of measurement.

The following Aurora metrics are not available in the Amazon RDS console:

- AuroraBinlogReplicaLag
- DeleteLatency
- DeleteThroughput
- EngineUptime
- InsertLatency
• InsertThroughput
• NetworkThroughput
• Queries
• UpdateLatency
• UpdateThroughput

In addition, some Aurora metrics are either shown only for specific instance classes, or only for DB instances, or with different names and different units of measurement:

• The CPUCreditBalance and CPUCreditUsage metrics are displayed only for db.t2.small and db.t2.medium instances
• The following metrics that are displayed with different names, as listed:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Display name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuroraReplicaLagMaximum</td>
<td>Replica lag maximum</td>
</tr>
<tr>
<td>AuroraReplicaLagMinimum</td>
<td>Replica lag minimum</td>
</tr>
<tr>
<td>DDLThroughput</td>
<td>DDL</td>
</tr>
<tr>
<td>NetworkReceiveThroughput</td>
<td>Network throughput</td>
</tr>
<tr>
<td>VolumeBytesUsed</td>
<td>[Billed] Volume bytes used</td>
</tr>
<tr>
<td>VolumeReadIOPs</td>
<td>[Billed] Volume read IOPs</td>
</tr>
<tr>
<td>VolumeWriteIOPs</td>
<td>[Billed] Volume write IOPs</td>
</tr>
</tbody>
</table>

• The following metrics apply to an entire Aurora DB cluster, but are displayed only when viewing DB instances for an Aurora DB cluster in the Amazon RDS console:
  • VolumeBytesUsed
  • VolumeReadIOPs
  • VolumeWriteIOPs

• The following metrics are displayed in megabytes, instead of bytes, in the Amazon RDS console:
  • FreeableMemory
  • FreeLocalStorage
  • NetworkReceiveThroughput
  • NetworkTransmitThroughput

**Latest metrics view**

You can view a subset of categorized Aurora metrics in the Latest Metrics view of the Amazon RDS console. The following table lists the categories and associated metrics displayed in the Amazon RDS console for an Aurora instance.

<table>
<thead>
<tr>
<th>Category</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL</td>
<td>ActiveTransactions</td>
</tr>
<tr>
<td></td>
<td>BlockedTransactions</td>
</tr>
<tr>
<td></td>
<td>BufferCacheHitRatio</td>
</tr>
</tbody>
</table>
## Aurora metrics available in the Amazon RDS console

<table>
<thead>
<tr>
<th>Category</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommitLatency</td>
<td></td>
</tr>
<tr>
<td>CommitThroughput</td>
<td></td>
</tr>
<tr>
<td>DatabaseConnections</td>
<td></td>
</tr>
<tr>
<td>DDLLatency</td>
<td></td>
</tr>
<tr>
<td>DDLThroughput</td>
<td></td>
</tr>
<tr>
<td>Deadlocks</td>
<td></td>
</tr>
<tr>
<td>DMLLatency</td>
<td></td>
</tr>
<tr>
<td>DMLThroughput</td>
<td></td>
</tr>
<tr>
<td>LoginFailures</td>
<td></td>
</tr>
<tr>
<td>ResultSetCacheHitRatio</td>
<td></td>
</tr>
<tr>
<td>SelectLatency</td>
<td></td>
</tr>
<tr>
<td>SelectThroughput</td>
<td></td>
</tr>
<tr>
<td><strong>System</strong></td>
<td><strong>AuroraReplicaLag</strong></td>
</tr>
<tr>
<td></td>
<td><strong>AuroraReplicaLagMaximum</strong></td>
</tr>
<tr>
<td></td>
<td><strong>AuroraReplicaLagMinimum</strong></td>
</tr>
<tr>
<td></td>
<td><strong>CPUCreditBalance</strong></td>
</tr>
<tr>
<td></td>
<td><strong>CPUCreditUsage</strong></td>
</tr>
<tr>
<td></td>
<td><strong>CPUUtilization</strong></td>
</tr>
<tr>
<td></td>
<td><strong>FreeableMemory</strong></td>
</tr>
<tr>
<td></td>
<td><strong>FreeLocalStorage</strong></td>
</tr>
<tr>
<td></td>
<td><strong>NetworkReceiveThroughput</strong></td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td><strong>AuroraReplicaLag</strong></td>
</tr>
<tr>
<td></td>
<td><strong>BufferCacheHitRatio</strong></td>
</tr>
<tr>
<td></td>
<td><strong>ResultSetCacheHitRatio</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SelectThroughput</strong></td>
</tr>
</tbody>
</table>
Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console. Also, you can consume the Enhanced Monitoring JSON output from Amazon CloudWatch Logs in a monitoring system of your choice.

By default, Enhanced Monitoring metrics are stored for 30 days in the CloudWatch Logs, which are different from typical CloudWatch metrics. To modify the amount of time the metrics are stored in the CloudWatch Logs, change the retention for the \texttt{RDSOSMetrics} log group in the CloudWatch console. For more information, see Change log data retention in CloudWatch logs in the Amazon CloudWatch Logs User Guide.

Because Enhanced Monitoring metrics are stored in the CloudWatch logs instead of in Cloudwatch metrics, the cost of Enhanced Monitoring depends on several factors:

- You are only charged for Enhanced Monitoring that exceeds the free tier provided by Amazon CloudWatch Logs.
  
  For more information about pricing, see Amazon CloudWatch pricing.
- A smaller monitoring interval results in more frequent reporting of OS metrics and increases your monitoring cost.
- Usage costs for Enhanced Monitoring are applied for each DB instance that Enhanced Monitoring is enabled for. Monitoring a large number of DB instances is more expensive than monitoring only a few.
- DB instances that support a more compute-intensive workload have more OS process activity to report and higher costs for Enhanced Monitoring.

### Differences between CloudWatch and Enhanced Monitoring metrics

CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance, and Enhanced Monitoring gathers its metrics from an agent on the instance. As a result, you might find differences between the measurements, because the hypervisor layer performs a small amount of work. The differences can be greater if your DB instances use smaller instance classes, because then there are likely more virtual machines (VMs) that are managed by the hypervisor layer on a single physical instance. Enhanced Monitoring metrics are useful when you want to see how different processes or threads on a DB instance use the CPU.

### Setting up and enabling Enhanced Monitoring

To use Enhanced Monitoring, you must create an IAM role, and then enable Enhanced Monitoring.

**Creating an IAM role for Enhanced Monitoring**

Enhanced Monitoring requires permission to act on your behalf to send OS metric information to CloudWatch Logs. You grant Enhanced Monitoring permissions using an AWS Identity and Access Management (IAM) role.

**Creating the IAM role when you enable Enhanced Monitoring**

When you enable Enhanced Monitoring in the RDS console, Amazon RDS can create the required IAM role for you. The role is named \texttt{rds-monitoring-role}. RDS uses this role for the specified DB instance or read replica.
To create the IAM role when enabling Enhanced Monitoring

1. Follow the steps in Enabling and disabling Enhanced Monitoring (p. 505).
2. Set Monitoring Role to Default in the step where you choose a role.

Creating the IAM role before you enable Enhanced Monitoring

You can create the required role before you enable Enhanced Monitoring. When you enable Enhanced Monitoring, specify your new role’s name. You must create this required role if you enable Enhanced Monitoring using the AWS CLI or the RDS API.

The user that enables Enhanced Monitoring must be granted the PassRole permission. For more information, see Example 2 in Granting a user permissions to pass a role to an AWS service in the IAM User Guide.

To create an IAM role for Amazon RDS enhanced monitoring

2. In the navigation pane, choose Roles.
3. Choose Create role.
4. Choose the AWS service tab, and then choose RDS from the list of services.
5. Choose RDS - Enhanced Monitoring, and then choose Next: Permissions.
6. Ensure that the Attached permissions policy page shows AmazonRDSEnhancedMonitoringRole, and then choose Next: Tags.
7. On the Add tags page, choose Next: Review.
8. For Role Name, enter a name for your role. For example, enter emaccess.
9. Choose Create role.

Enabling and disabling Enhanced Monitoring

You can enable and disable Enhanced Monitoring using the AWS Management Console, AWS CLI, or RDS API.

Console

You can enable Enhanced Monitoring when you create a DB cluster or read replica, or when you modify a DB cluster. If you modify a DB instance to enable Enhanced Monitoring, you don’t need to reboot your DB instance for the change to take effect.

You can enable Enhanced Monitoring in the RDS console when you do one of the following actions:

- Create a DB cluster – You can enable Enhanced Monitoring in the Monitoring section under Additional configuration.
- Create a read replica – You can enable Enhanced Monitoring in the Monitoring section.
- Modify a DB instance – You can enable Enhanced Monitoring in the Monitoring section.

To enable Enhanced Monitoring by using the RDS console

1. Scroll to the Monitoring section.
2. Choose **Enable enhanced monitoring** for your DB instance or read replica. To disable Enhanced Monitoring, choose **Disable enhanced monitoring**.

3. Set the **Monitoring Role** property to the IAM role that you created to permit Amazon RDS to communicate with Amazon CloudWatch Logs for you, or choose **Default** to have RDS create a role for you named `rds-monitoring-role`.

4. Set the **Granularity** property to the interval, in seconds, between points when metrics are collected for your DB instance or read replica. The **Granularity** property can be set to one of the following values: 1, 5, 10, 15, 30, or 60.

   **Note**
   The fastest that the RDS console refreshes is every 5 seconds. If you set the granularity to 1 second in the RDS console, you still see updated metrics only every 5 seconds. You can retrieve 1-second metric updates by using CloudWatch Logs.

**AWS CLI**

To enable Enhanced Monitoring using the AWS CLI, in the following commands, set the `--monitoring-interval` option to a value other than 0 and set the `--monitoring-role-arn` option to the role you created in Creating an IAM role for Enhanced Monitoring (p. 504).

- `create-db-instance`
- `create-db-instance-read-replica`
- `modify-db-instance`

The `--monitoring-interval` option specifies the interval, in seconds, between points when Enhanced Monitoring metrics are collected. Valid values for the option are 0, 1, 5, 10, 15, 30, and 60.

To disable Enhanced Monitoring using the AWS CLI, set the `--monitoring-interval` option to 0 in the these commands.

**Example**

The following example enables Enhanced Monitoring for a DB instance:

For Linux, macOS, or Unix:
aws rds modify-db-instance --db-instance-identifier mydbinstance --monitoring-interval 30 --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess

For Windows:
aws rds modify-db-instance --db-instance-identifier mydbinstance --monitoring-interval 30 --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess

RDS API

To enable Enhanced Monitoring using the RDS API, in the following operations, set the MonitoringInterval parameter to a value other than 0 and set the MonitoringRoleArn parameter to the role you created in Creating an IAM role for Enhanced Monitoring (p. 504).

- CreateDBInstance
- CreateDBInstanceReadReplica
- ModifyDBInstance

The MonitoringInterval parameter specifies the interval, in seconds, between points when Enhanced Monitoring metrics are collected. Valid values for the parameter are 0, 1, 5, 10, 15, 30, and 60.

To disable Enhanced Monitoring using the RDS API, set the MonitoringInterval parameter to 0 in the these operations.

Viewing Enhanced Monitoring

You can view OS metrics reported by Enhanced Monitoring in the RDS console by choosing Enhanced monitoring for Monitoring.

The Enhanced Monitoring page is shown following.
If you want to see details for the processes running on your DB instance, choose **OS process list** for Monitoring.

The **Process List** view is shown following.

![Process List](image)

The Enhanced Monitoring metrics shown in the Process list view are organized as follows:

- **RDS child processes** – Shows a summary of the RDS processes that support the DB instance, for example `aurora` for Amazon Aurora DB clusters. Process threads appear nested beneath the parent process. Process threads show CPU utilization only as other metrics are the same for all threads for the process. The console displays a maximum of 100 processes and threads. The results are a combination of the top CPU consuming and memory consuming processes and threads. If there are more than 50 processes and more than 50 threads, the console displays the top 50 consumers in each category. This display helps you identify which processes are having the greatest impact on performance.

- **RDS processes** – Shows a summary of the resources used by the RDS management agent, diagnostics monitoring processes, and other AWS processes that are required to support RDS DB instances.

- **OS processes** – Shows a summary of the kernel and system processes, which generally have minimal impact on performance.

The items listed for each process are:

- **VIRT** – Displays the virtual size of the process.
- **RES** – Displays the actual physical memory being used by the process.
- **CPU%** – Displays the percentage of the total CPU bandwidth being used by the process.
- **MEM%** – Displays the percentage of the total memory being used by the process.

The monitoring data that is shown in the RDS console is retrieved from Amazon CloudWatch Logs. You can also retrieve the metrics for a DB instance as a log stream from CloudWatch Logs. For more information, see Viewing Enhanced Monitoring by using CloudWatch Logs (p. 509).

Enhanced Monitoring metrics are not returned during the following:

- A failover of the DB instance.
- Changing the instance class of the DB instance (scale compute).

Enhanced Monitoring metrics are returned during a reboot of a DB instance because only the database engine is rebooted. Metrics for the operating system are still reported.
Viewing Enhanced Monitoring by using CloudWatch Logs

After you have enabled Enhanced Monitoring for your DB instance, you can view the metrics for your DB instance using CloudWatch Logs, with each log stream representing a single DB instance being monitored. The log stream identifier is the resource identifier (DbiResourceId) for the DB instance.

To view Enhanced Monitoring log data

2. If necessary, choose the region that your DB instance is in. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
3. Choose Logs in the navigation pane.
4. Choose RDSOSMetrics from the list of log groups.
5. Choose the log stream that you want to view from the list of log streams.

Available OS metrics

The following tables list the OS metrics available using Amazon CloudWatch Logs.

Metrics for Aurora

<table>
<thead>
<tr>
<th>Group</th>
<th>Metric</th>
<th>Console name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>engine</td>
<td>Not applicable</td>
<td>The database engine for the DB instance.</td>
</tr>
<tr>
<td></td>
<td>instanceID</td>
<td>Not applicable</td>
<td>The DB instance identifier.</td>
</tr>
<tr>
<td></td>
<td>instanceResourceID</td>
<td>Not applicable</td>
<td>An immutable identifier for the DB instance that is unique to an AWS Region, also used as the log stream identifier.</td>
</tr>
<tr>
<td></td>
<td>numVCPUs</td>
<td>Not applicable</td>
<td>The number of virtual CPUs for the DB instance.</td>
</tr>
<tr>
<td></td>
<td>timestamp</td>
<td>Not applicable</td>
<td>The time at which the metrics were taken.</td>
</tr>
<tr>
<td></td>
<td>uptime</td>
<td>Not applicable</td>
<td>The amount of time that the DB instance has been active.</td>
</tr>
<tr>
<td></td>
<td>version</td>
<td>Not applicable</td>
<td>The version of the OS metrics' stream JSON format.</td>
</tr>
<tr>
<td></td>
<td>cpuUtilization</td>
<td>CPU Guest</td>
<td>The percentage of CPU in use by guest programs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>idle</td>
<td>The percentage of CPU that is idle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>irq</td>
<td>The percentage of CPU in use by software interrupts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>nice</td>
<td>The percentage of CPU in use by programs running at lowest priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>steal</td>
<td>The percentage of CPU in use by other virtual machines.</td>
</tr>
<tr>
<td>Group</td>
<td>Metric</td>
<td>Console name</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>system</td>
<td>system</td>
<td>CPU System</td>
<td>The percentage of CPU in use by the kernel.</td>
</tr>
<tr>
<td>total</td>
<td>total</td>
<td>CPU Total</td>
<td>The total percentage of the CPU in use. This value includes the nice value.</td>
</tr>
<tr>
<td>user</td>
<td>user</td>
<td>CPU User</td>
<td>The percentage of CPU in use by user programs.</td>
</tr>
<tr>
<td>wait</td>
<td>wait</td>
<td>CPU Wait</td>
<td>The percentage of CPU unused while waiting for I/O access.</td>
</tr>
<tr>
<td>diskIO</td>
<td>avgQueueLen</td>
<td>Avg Queue Size</td>
<td>The number of requests waiting in the I/O device's queue.</td>
</tr>
<tr>
<td></td>
<td>avgReqSz</td>
<td>Ave Request Size</td>
<td>The average request size, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>await</td>
<td>Disk I/O Await</td>
<td>The number of milliseconds required to respond to requests, including queue time and service time.</td>
</tr>
<tr>
<td></td>
<td>device</td>
<td>Not applicable</td>
<td>The identifier of the disk device in use.</td>
</tr>
<tr>
<td></td>
<td>diskQueueDepth</td>
<td>Disk Queue Depth</td>
<td>The number of pending input and output (I/O) requests waiting to access the disk.</td>
</tr>
<tr>
<td></td>
<td>readIOsPS</td>
<td>Read IO/s</td>
<td>The number of read operations per second.</td>
</tr>
<tr>
<td></td>
<td>readKb</td>
<td>Read Total</td>
<td>The total number of kilobytes read.</td>
</tr>
<tr>
<td></td>
<td>readKbps</td>
<td>Read Kb/s</td>
<td>The number of kilobytes read per second.</td>
</tr>
</tbody>
</table>
|       | readLatency | Read Latency | The elapsed time between the submission of a read I/O request and its completion, in milliseconds. 
This metric is only available for Amazon Aurora. |
|       | readThroughput | Read Throughput | The amount of network throughput used by requests to the DB cluster, in bytes per second. 
This metric is only available for Amazon Aurora. |
|       | rrqmPS | Rrqms | The number of merged read requests queued per second. |
|       | tps | TPS | The number of I/O transactions per second. |
|       | util | Disk I/O Util | The percentage of CPU time during which requests were issued. |
|       | writeIOsPS | Write IO/s | The number of write operations per second. |
|       | writeKb | Write Total | The total number of kilobytes written. |
|       | writeKbps | Write Kb/s | The number of kilobytes written per second. |
|       | writeLatency | Write Latency | The average elapsed time between the submission of a write I/O request and its completion, in milliseconds. 
This metric is only available for Amazon Aurora. |
### Viewing Enhanced Monitoring by using CloudWatch Logs

<table>
<thead>
<tr>
<th>Group</th>
<th>Metric</th>
<th>Console name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>writeThrough</td>
<td>Write Throughput</td>
<td>The amount of network throughput used by responses from the DB cluster, in bytes per second. This metric is only available for Amazon Aurora.</td>
</tr>
<tr>
<td>fileSys</td>
<td>wrqmPS</td>
<td>Wrqms</td>
<td>The number of merged write requests queued per second.</td>
</tr>
<tr>
<td>fileSys</td>
<td>maxFiles</td>
<td>Max Inodes</td>
<td>The maximum number of files that can be created for the file system.</td>
</tr>
<tr>
<td>mountPoint</td>
<td></td>
<td></td>
<td>The path to the file system.</td>
</tr>
<tr>
<td>name</td>
<td></td>
<td></td>
<td>The name of the file system.</td>
</tr>
<tr>
<td>total</td>
<td>Total Filesystem</td>
<td></td>
<td>The total number of disk space available for the file system, in kilobytes.</td>
</tr>
<tr>
<td>used</td>
<td>Used Filesystem</td>
<td></td>
<td>The amount of disk space used by files in the file system, in kilobytes.</td>
</tr>
<tr>
<td>usedFilePercent</td>
<td>Used %</td>
<td></td>
<td>The percentage of available files in use.</td>
</tr>
<tr>
<td>usedFiles</td>
<td>Used Inodes</td>
<td></td>
<td>The number of files in the file system.</td>
</tr>
<tr>
<td>usedPercent</td>
<td>Used Inodes %</td>
<td></td>
<td>The percentage of the file-system disk space in use.</td>
</tr>
<tr>
<td>loadAverageMinute</td>
<td>Load Avg 15 min</td>
<td></td>
<td>The number of processes requesting CPU time over the last 15 minutes.</td>
</tr>
<tr>
<td>five</td>
<td>Load Avg 5 min</td>
<td></td>
<td>The number of processes requesting CPU time over the last 5 minutes.</td>
</tr>
<tr>
<td>one</td>
<td>Load Avg 1 min</td>
<td></td>
<td>The number of processes requesting CPU time over the last minute.</td>
</tr>
<tr>
<td>memory</td>
<td>active</td>
<td>Active Memory</td>
<td>The amount of assigned memory, in kilobytes.</td>
</tr>
<tr>
<td>buffers</td>
<td>Buffered Memory</td>
<td></td>
<td>The amount of memory used for buffering I/O requests prior to writing to the storage device, in kilobytes.</td>
</tr>
<tr>
<td>cached</td>
<td>Cached Memory</td>
<td></td>
<td>The amount of memory used for caching file system–based I/O.</td>
</tr>
<tr>
<td>dirty</td>
<td>Dirty Memory</td>
<td></td>
<td>The amount of memory pages in RAM that have been modified but not written to their related data block in storage, in kilobytes.</td>
</tr>
<tr>
<td>free</td>
<td>Free Memory</td>
<td></td>
<td>The amount of unassigned memory, in kilobytes.</td>
</tr>
<tr>
<td>hugePagesFree</td>
<td>Huge Pages Free</td>
<td></td>
<td>The number of free huge pages. Huge pages are a feature of the Linux kernel.</td>
</tr>
<tr>
<td>Group</td>
<td>Metric</td>
<td>Console name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>hugePagesRsvd</td>
<td></td>
<td>The number of committed huge pages.</td>
</tr>
<tr>
<td></td>
<td>hugePagesSize</td>
<td></td>
<td>The size for each huge pages unit, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>hugePagesSurp</td>
<td></td>
<td>The number of available surplus huge pages over the total.</td>
</tr>
<tr>
<td></td>
<td>hugePagesTotal</td>
<td></td>
<td>The total number of huge pages.</td>
</tr>
<tr>
<td></td>
<td>inactive</td>
<td></td>
<td>The amount of least-frequently used memory pages, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>mapped</td>
<td></td>
<td>The total amount of file-system contents that is memory mapped inside a process address space, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>pageTables</td>
<td></td>
<td>The amount of memory used by page tables, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>slab</td>
<td></td>
<td>The amount of reusable kernel data structures, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>total</td>
<td></td>
<td>The total amount of memory, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>writeback</td>
<td></td>
<td>The amount of dirty pages in RAM that are still being written to the backing storage, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>network</td>
<td>interface</td>
<td>The identifier for the network interface being used for the DB instance.</td>
</tr>
<tr>
<td></td>
<td>rx</td>
<td>RX</td>
<td>The number of bytes received per second.</td>
</tr>
<tr>
<td></td>
<td>tx</td>
<td>TX</td>
<td>The number of bytes uploaded per second.</td>
</tr>
<tr>
<td></td>
<td>processList</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>cpuUsedPc</td>
<td>CPU%</td>
<td>The percentage of CPU used by the process.</td>
</tr>
<tr>
<td></td>
<td>id</td>
<td></td>
<td>The identifier of the process.</td>
</tr>
<tr>
<td></td>
<td>memoryUsedPc</td>
<td>MEM%</td>
<td>The amount of memory used by the process, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td></td>
<td>The name of the process.</td>
</tr>
<tr>
<td></td>
<td>parentID</td>
<td></td>
<td>The process identifier for the parent process of the process.</td>
</tr>
<tr>
<td></td>
<td>rss</td>
<td>RES</td>
<td>The amount of RAM allocated to the process, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>tgid</td>
<td></td>
<td>The thread group identifier, which is a number representing the process ID to which a thread belongs. This identifier is used to group threads from the same process.</td>
</tr>
<tr>
<td></td>
<td>VIRT</td>
<td>VIRT</td>
<td>The amount of virtual memory allocated to the process, in kilobytes.</td>
</tr>
<tr>
<td>Group</td>
<td>Metric</td>
<td>Console name</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>swap</td>
<td>swap</td>
<td>Swap</td>
<td>The amount of swap memory available, in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>swap in</td>
<td>Swaps in</td>
<td>The amount of memory, in kilobytes, swapped in from disk.</td>
</tr>
<tr>
<td></td>
<td>swap out</td>
<td>Swaps out</td>
<td>The amount of memory, in kilobytes, swapped out to disk.</td>
</tr>
<tr>
<td>free</td>
<td>free</td>
<td>Free Swap</td>
<td>The amount of swap memory free, in kilobytes.</td>
</tr>
<tr>
<td>committed</td>
<td>committed</td>
<td>Committed Swap</td>
<td>The amount of swap memory, in kilobytes, used as cache memory.</td>
</tr>
<tr>
<td>tasks</td>
<td>blocked</td>
<td>Tasks Blocked</td>
<td>The number of tasks that are blocked.</td>
</tr>
<tr>
<td></td>
<td>running</td>
<td>Tasks Running</td>
<td>The number of tasks that are running.</td>
</tr>
<tr>
<td></td>
<td>sleeping</td>
<td>Tasks Sleeping</td>
<td>The number of tasks that are sleeping.</td>
</tr>
<tr>
<td></td>
<td>stopped</td>
<td>Tasks Stopped</td>
<td>The number of tasks that are stopped.</td>
</tr>
<tr>
<td></td>
<td>total</td>
<td>Tasks Total</td>
<td>The total number of tasks.</td>
</tr>
<tr>
<td>zombie</td>
<td>zombie</td>
<td>Tasks Zombie</td>
<td>The number of child tasks that are inactive with an active parent task.</td>
</tr>
</tbody>
</table>
Using Amazon RDS Performance Insights

Performance Insights expands on existing Amazon RDS monitoring features to illustrate your database’s performance and help you analyze any issues that affect it. With the Performance Insights dashboard, you can visualize the database load and filter the load by waits, SQL statements, hosts, or users.

Topics
- Overview of Performance Insights (p. 514)
- Enabling and disabling Performance Insights (p. 517)
- Accessing Performance Insights (p. 520)
- Monitoring with the Performance Insights dashboard (p. 522)
- Customizing the Performance Insights dashboard (p. 542)
- Retrieving data with the Performance Insights API (p. 549)
- Performance Insights metrics published to Amazon CloudWatch (p. 561)
- Logging Performance Insights calls by using AWS CloudTrail (p. 563)

Overview of Performance Insights

By default, Performance Insights is enabled in the console create wizard for Amazon RDS engines. If you have more than one database on a DB instance, Performance Insights aggregates performance data.

Topics
- DB load (p. 514)
- Maximum CPU (p. 516)
- Supported DB engines for Performance Insights (p. 516)

DB load

The central metric for Performance Insights is **DB Load**. The **DB Load** metric is collected every second.

**Active Sessions**

An *active session* is a connection that has submitted work to the DB engine and is waiting for a response. The DB load represents the *average active sessions* (AAS) for the DB engine. For example, if you submit a SQL query to the DB engine, the database session is active while the engine is processing the query.

To obtain the AAS, Performance Insights samples the number of sessions concurrently running a query. The AAS is the total number of sessions divided by the total number of samples. The following table shows 5 consecutive samples of a running query.

<table>
<thead>
<tr>
<th>Sample</th>
<th>Number of sessions running query</th>
<th>AAS</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2 sessions / 1 sample</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2 sessions / 2 samples</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>2</td>
<td>6 sessions / 3 samples</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>1.5</td>
<td>6 sessions / 4 samples</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>2</td>
<td>10 sessions / 5 samples</td>
</tr>
</tbody>
</table>
Related to AAS is the average active executions (AAE) per second. To calculate the AAE, Performance Insights divides the total execution time of a query by the time interval. The following table shows the AAE calculation for the same query in the preceding table.

<table>
<thead>
<tr>
<th>Elapsed time (s)</th>
<th>Total execution time (s)</th>
<th>AAE</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>120</td>
<td>2</td>
<td>120 execution seconds / 60 elapsed seconds</td>
</tr>
<tr>
<td>120</td>
<td>120</td>
<td>1</td>
<td>120 execution seconds / 120 elapsed seconds</td>
</tr>
<tr>
<td>180</td>
<td>380</td>
<td>2.11</td>
<td>360 execution seconds / 180 elapsed seconds</td>
</tr>
<tr>
<td>240</td>
<td>380</td>
<td>1.58</td>
<td>360 execution seconds / 240 elapsed seconds</td>
</tr>
<tr>
<td>300</td>
<td>600</td>
<td>2</td>
<td>600 execution seconds / 300 elapsed seconds</td>
</tr>
</tbody>
</table>

In most cases, the AAS and AAE for a query are approximately the same. However, because the inputs to the calculations are different data sources, the calculations often vary slightly.

**Dimensions**

The DB Load metric has subcomponents called dimensions. You can think of dimensions as categories for the different characteristics of the DB Load metric. When you are diagnosing performance issues, the most useful dimensions are wait events and top SQL.

**Wait events**

A wait event causes a SQL statement to wait for a specific event to happen before it can continue running. For example, a SQL statement might wait until a locked resource is unlocked. By combining DB Load with wait events, you can get a complete picture of the session state. Wait events vary by DB engine:

- For a list of the most commonly used wait events for Aurora MySQL, see Aurora MySQL events (p. 863).
- For information about all MySQL wait events, see Wait Event Summary Tables in the MySQL documentation.
- For a list of the most commonly used wait events for Aurora PostgreSQL, see Amazon Aurora PostgreSQL events (p. 1146).
- For information about all PostgreSQL wait events, see PostgreSQL Wait Events in the PostgreSQL documentation.

**Top SQL**

Whereas wait events show bottlenecks, top SQL shows which queries are contributing the most to DB load. For example, many queries might be currently running on the database, but a single query might consume 99% of the DB load. In this case, the high load might indicate a problem with the query.

By default, the Performance Insights console displays top SQL queries that are contributing to the database load. The console also shows relevant statistics for each statement. To diagnose performance problems for a specific statement, you can examine its execution plan.
Maximum CPU

In the dashboard, the Database load chart collects, aggregates, and displays session information. To see whether active sessions are exceeding the maximum CPU, look at their relationship to the Max vCPU line. The Max vCPU value is determined by the number of vCPU (virtual CPU) cores for your DB instance.

If the load is often above the Max vCPU line, and the primary wait state is CPU, the system CPU is overloaded. In these cases, you might want to throttle connections to the instance, tune any SQL queries with a high CPU load, or consider a larger instance class. High and consistent instances of any wait state indicate that there might be bottlenecks or resource contention issues to resolve. This can be true even if the load doesn't cross the Max vCPU line.

You can find an overview of Performance Insights in the following video.

Using Performance Insights to Analyze Performance of Amazon Aurora PostgreSQL

Supported DB engines for Performance Insights

Following, you can find the DB engines that support Performance Insights.

<table>
<thead>
<tr>
<th>DB Engine</th>
<th>Supported DB Engine Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Aurora with MySQL compatibility</td>
<td>2.04.2 and higher 2.x versions (compatible with MySQL 5.7), and 1.17.3 and higher 1.x versions (compatible with MySQL 5.6). Not supported on db.t2 or db.t3 DB instance classes. For DB clusters enabled for parallel query, the minimum Aurora MySQL versions are 2.09.0 and 1.23.0.</td>
</tr>
<tr>
<td>Amazon Aurora with PostgreSQL compatibility</td>
<td>All versions.</td>
</tr>
<tr>
<td>Amazon RDS for MariaDB</td>
<td>All 10.5 versions, all 10.4 versions, 10.3.13 and higher 10.3 versions, and 10.2.21 and higher 10.2 versions. Not supported for MariaDB version 10.0 or 10.1. Not supported for MariaDB version 10.3.13 DB instances in the Europe (Frankfurt) and Europe (Stockholm) AWS Regions. Not supported on the following DB instance classes: db.t2.micro, db.t2.small, db.t3.micro, and db.t3.small.</td>
</tr>
<tr>
<td>Amazon RDS for MySQL</td>
<td>8.0.17 and higher 8.0 versions, version 5.7.22 and higher 5.7 versions, and version 5.6.41 and higher 5.6 versions. Not supported for version 5.5. Not supported on the following DB instance classes: db.t2.micro, db.t2.small, db.t3.micro, and db.t3.small.</td>
</tr>
<tr>
<td>Amazon RDS for Microsoft SQL Server</td>
<td>All versions except SQL Server 2008.</td>
</tr>
<tr>
<td>Amazon RDS for PostgreSQL</td>
<td>Version 10, 11, and 12.</td>
</tr>
<tr>
<td>Amazon RDS for Oracle</td>
<td>All versions.</td>
</tr>
</tbody>
</table>

**Note**

Amazon RDS Performance Insights isn't supported in the Middle East (Bahrain) Region, Africa (Cape Town) Region, or in AWS GovCloud (US) Regions.
Enabling and disabling Performance Insights

To use Performance Insights, enable it on your DB instance. If needed, you can disable it later. Enabling and disabling Performance Insights doesn't cause downtime, a reboot, or a failover.

If you use Performance Insights together with Aurora Global Database, enable Performance Insights individually for the DB instances in each AWS Region. For details, see Monitoring an Amazon Aurora global database with Amazon RDS Performance Insights (p. 249).

The Performance Insights agent consumes limited CPU and memory on the DB host. When the DB load is high, the agent limits the performance impact by collecting data less frequently.

Console

In the console, you can enable or disable Performance Insights when you create or modify a new DB instance.

Enabling or disabling Performance Insights when creating an instance

When you create a new DB instance, enable Performance Insights by choosing **Enable Performance Insights** in the **Performance Insights** section. Or choose **Disable Performance Insights**.

To create a DB instance, follow the instructions for your DB engine in Creating an Amazon Aurora DB cluster (p. 118).

The following screenshot shows the **Performance Insights** section.

![Performance Insights Screenshot]

If you choose **Enable Performance Insights**, you have the following options:

- **Retention** – The amount of time to retain Performance Insights data. Choose either 7 days (the default) or 2 years.
- **Master key** – Specify your AWS Key Management Service (AWS KMS) customer master key (CMK). Performance Insights encrypts all potentially sensitive data using your AWS KMS CMK.
Data is encrypted in flight and at rest. For more information, see Encrypting Amazon Aurora resources (p. 1208).

Enabling or disabling Performance Insights when modifying an instance

In the console, you can modify a DB instance to enable or disable Performance Insights using the console.

To enable or disable Performance Insights for a DB instance using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Databases.
3. Choose a DB instance, and choose Modify.
4. In the Performance Insights section, choose either Enable Performance Insights or Disable Performance Insights.

If you choose Enable Performance Insights, you have the following options:

- **Retention** – The amount of time to retain Performance Insights data. Choose either 7 days (the default) or 2 years.
- **Master key** – Specify your AWS Key Management Service (AWS KMS) customer master key (CMK). Performance Insights encrypts all potentially sensitive data using your AWS KMS CMK. Data is encrypted in flight and at rest. For more information, see Encrypting Amazon Aurora resources (p. 1208).

5. Choose Continue.
6. For Scheduling of Modifications, choose one of the following:

- **Apply during the next scheduled maintenance window** – Wait to apply the Performance Insights modification until the next maintenance window.
- **Apply immediately** – Apply the Performance Insights modification as soon as possible.
7. Choose Modify instance.

AWS CLI


You can also specify these values using the following AWS CLI commands:

- create-db-instance-read-replica
- modify-db-instance
- restore-db-instance-from-s3

The following procedure describes how to enable or disable Performance Insights for a DB instance using the AWS CLI.

To enable or disable Performance Insights for a DB instance using the AWS CLI

- Call the modify-db-instance AWS CLI command and supply the following values:
  - --db-instance-identifier – The name of the DB instance.
• `--enable-performance-insights` to enable or `--no-enable-performance-insights` to disable

The following example enables Performance Insights for `sample-db-instance`.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-instance \
   --db-instance-identifier sample-db-instance \
   --enable-performance-insights
```

For Windows:

```bash
aws rds modify-db-instance ^
   --db-instance-identifier sample-db-instance ^
   --enable-performance-insights
```

When you enable Performance Insights, you can optionally specify the amount of time, in days, to retain Performance Insights data with the `--performance-insights-retention-period` option. Valid values are 7 (the default) or 731 (2 years).

The following example enables Performance Insights for `sample-db-instance` and specifies that Performance Insights data is retained for two years.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-instance \
   --db-instance-identifier sample-db-instance \
   --enable-performance-insights \
   --performance-insights-retention-period 731
```

For Windows:

```bash
aws rds modify-db-instance ^
   --db-instance-identifier sample-db-instance ^
   --enable-performance-insights ^
   --performance-insights-retention-period 731
```

**RDS API**

When you create a new DB instance using the `CreateDBInstance` operation Amazon RDS API operation, enable Performance Insights by setting `EnablePerformanceInsights` to `True`. To disable Performance Insights, set `EnablePerformanceInsights` to `False`.

You can also specify the `EnablePerformanceInsights` value using the following API operations:

- `ModifyDBInstance`
- `CreateDBInstanceReadReplica`
- `RestoreDBInstanceFromS3`
When you enable Performance Insights, you can optionally specify the amount of time, in days, to retain Performance Insights data with the `PerformanceInsightsRetentionPeriod` parameter. Valid values are 7 (the default) or 731 (2 years).

### Enabling the Performance Schema for Performance Insights on Aurora MySQL

When the Performance Schema feature is enabled for Aurora MySQL, Performance Insights provides more detailed information. For example, Performance Insights displays DB load categorized by detailed wait events. Without the Performance Schema enabled, Performance Insights displays DB load categorized by the list state of the MySQL process.

Performance Schema is enabled automatically when you create an Aurora MySQL DB instance with Performance Insights enabled. In this case, Performance Insights automatically manages the parameters in the following table.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>performance_schema</td>
<td>1 (the source parameter is set to engine-default)</td>
</tr>
<tr>
<td>performance-schema-consumer-events-waits-current</td>
<td>ON</td>
</tr>
<tr>
<td>performance-schema-instrument</td>
<td>wait/%=ON</td>
</tr>
<tr>
<td>performance-schema-consumer-global-instrumentation</td>
<td>ON</td>
</tr>
<tr>
<td>performance-schema-consumer-thread-instrumentation</td>
<td>ON</td>
</tr>
</tbody>
</table>

**Important**

When Performance Schema is enabled automatically, Performance Insights changes schema-related parameters on the DB instance. These changes aren't visible in the parameter group associated with the DB instance.

For more information, see Performance Schema Command Options and Performance Schema Option and Variable Reference in the MySQL documentation.

### Accessing Performance Insights

To access Performance Insights, you must have the appropriate permissions from AWS Identity and Access Management (IAM). There are two options available for granting access:

1. Attach the `AmazonRDSFullAccess` managed policy to an IAM user or role.
2. Create a custom IAM policy and attach it to an IAM user or role.

**AmazonRDSFullAccess managed policy**

`AmazonRDSFullAccess` is an AWS-managed policy that grants access to all of the Amazon RDS API operations. The policy also grants access to related services that are used by the Amazon RDS console—for example, event notifications using Amazon SNS.
In addition, AmazonRDSFullAccess contains all the permissions needed for using Performance Insights. If you attach this policy to an IAM user or role, the recipient can use Performance Insights along with other console features.

**Using a custom IAM policy**

For users who don’t have full access with the AmazonRDSFullAccess policy, you can grant access to Performance Insights by creating or modifying a user-managed IAM policy. When you attach the policy to an IAM user or role, the recipient can use Performance Insights.

**To create a custom policy**

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Policies**.
3. Choose **Create policy**.
4. On the **Create Policy** page, choose the JSON tab.
5. Copy and paste the following.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "pi:*",
      "Resource": "arn:aws:pi:*:*:metrics/rds/*"
    }
  ]
}
```
6. Choose **Review policy**.
7. Provide a name for the policy and optionally a description, and then choose **Create policy**.

You can now attach the policy to an IAM user or role. The following procedure assumes that you already have an IAM user available for this purpose.

**To attach the policy to an IAM user**

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Users**.
3. Choose an existing user from the list.

   **Important**
   
   To use Performance Insights, make sure that you have access to Amazon RDS in addition to the custom policy. For example, the AmazonRDSReadOnlyAccess predefined policy provides read-only access to Amazon RDS. For more information, see Managing access using policies (p. 1224).

4. On the **Summary** page, choose **Add permissions**.
5. Choose **Attach existing policies directly**. For **Search**, type the first few characters of your policy name, as shown following.
6. Choose your policy, and then choose Next: Review.
7. Choose Add permissions.

Monitoring with the Performance Insights dashboard

The Performance Insights dashboard contains database performance information to help you analyze and troubleshoot performance issues. On the main dashboard page, you can view information about the database load. You can also drill into details for a particular wait state, SQL query, host, or user.

Opening the Performance Insights dashboard

To see the Performance Insights dashboard, use the following procedure.

To view the Performance Insights dashboard in the AWS Management Console

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Performance Insights.
3. Choose a DB instance. The Performance Insights dashboard is displayed for that DB instance.

For DB instances with Performance Insights enabled, you can also reach the dashboard by choosing the Sessions item in the list of DB instances. Under Current activity, the Sessions item shows the database load in average active sessions over the last five minutes. The bar graphically shows the load. When the bar is empty, the DB instance is idle. As the load increases, the bar fills with blue. When the load passes the number of virtual CPUs (vCPUs) on the DB instance class, the bar turns red, indicating a potential bottleneck.
The following screenshot shows the dashboard for a DB instance. By default, the Performance Insights dashboard shows data for the last hour.

4. (Optional) Choose a different time interval by selecting a button in the upper right. For example, to change the interval to 5 hours, select 5h.

In the following screenshot, the DB load interval is 5 hours.

5. (Optional) To refresh your data automatically, enable Auto refresh.
The Performance Insight dashboard automatically refreshes with new data. The refresh rate depends on the amount of data displayed:

- 5 minutes refreshes every 5 seconds.
- 1 hour refreshes every minute.
- 5 hours refreshes every minute.
- 24 hours refreshes every 5 minutes.
- 1 week refreshes every hour.

Performance Insights dashboard components

The dashboard is divided into three parts:

1. **Counter Metrics** – Shows data for specific performance counter metrics.
2. **DB Load Chart** – Shows how the DB load compares to DB instance capacity as represented by the Max vCPU line.
3. **Top items** – Shows the top waits, SQL, hosts, and users contributing to DB load.

**Counter Metrics chart**

The **Counter Metrics** chart displays data for performance counters. The default metrics depend on the DB engine.

- Aurora MySQL – `db.SQL.Innodb_rows_read.avg`
- Aurora PostgreSQL – `db.Transactions.xact_commit.avg`

Change the performance counters by choosing **Manage Metrics**. You can select multiple **OS metrics** or **Database metrics**, as shown in the following screenshot. To see details for any metric, hover over the metric name.
For more information, see Customizing the Performance Insights dashboard (p. 542).

**Average Active Sessions chart**

The **Database Load** chart shows how the database load compares to DB instance capacity as represented by the **Max vCPU** line. By default, load is shown as active sessions grouped by wait states in a bar graph.
You can choose to display load as active sessions grouped by waits, SQL, users, or hosts. You can also choose a line graph.

To see details about a DB load item such as a SQL statement, hover over the item name.
To see details for any item for the selected time period in the legend, hover over that item.

**DB Load Chart**

Current Activity Measured in Average Active Sessions (AAS)

- **Show max vCPU**

Sessions

<table>
<thead>
<tr>
<th>Activity</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>0.89</td>
</tr>
<tr>
<td>IO:WALWrite</td>
<td>0</td>
</tr>
<tr>
<td>LWLock:ProcArrayLock</td>
<td>0</td>
</tr>
<tr>
<td>IO:XactSync</td>
<td>0.12</td>
</tr>
<tr>
<td>CPU</td>
<td>0.77</td>
</tr>
</tbody>
</table>

Max vCPU: 2
Top load table

The Top load table shows the top items contributing to database load. You can choose any of the following dimension tabs:

- Top SQL – The SQL statements that are currently running
- Top waits – The event for which the database backend is waiting
- Top hosts – The host name of the connected client
- Top users – The user logged in to the database
- Top databases – The name of the database to which the client is connected
- Top applications (Aurora PostgreSQL only) – The name of the application that is connected to the database
- Top session types (Aurora PostgreSQL only) – The type of the current session

By default, the console displays top SQL queries that are contributing to the database load. Every line in the table shows relevant statistics for the SQL statement:

To see the components of a query, select the query, and then choose the +. A SQL digest is a composite of multiple actual queries that are structurally similar but that possibly have different literal values. In the following screenshot, the selected query is a digest.

In Top sql, the Load by waits (AAS) column illustrates the percentage of the database load associated with each top load item. This column reflects the load for that item by whatever grouping is currently
selected in the **DB Load Chart**. For example, you might group the **DB Load Chart** chart by wait states. You examine SQL queries in the top load items table. In this case, the **DB Load by Waits** bar is sized, segmented, and color-coded to show how much of a given wait state that query is contributing to. It also shows which wait states are affecting the selected query.

In the **Top sql** table, you can open a statement to view its information. The information appears in the bottom pane.
In the **Top sql** tab, you can view the following types of identifiers (IDs) that are associated with SQL statements:

- **Support SQL ID** – A hash value of the SQL ID. This value is only for referencing a SQL ID when you are working with AWS Support. AWS Support doesn't have access to your actual SQL IDs and SQL text.
- **Support Digest ID** – A hash value of the digest ID. This value is only for referencing a digest ID when you are working with AWS Support. AWS Support doesn't have access to your actual digest IDs and SQL text.

You can control the statistics displayed in the **Top sql** tab by choosing the **Preferences** icon.
When you choose the Preferences icon, the Preferences window opens.

Enable the statistics that you want to have visible in the Top sql tab, use your mouse to scroll to the bottom of the window, and then choose Continue.
Analyzing DB load using the Performance Insights dashboard

If the **Average Active Sessions** chart shows a bottleneck, you can find out where the load is coming from. To do so, look at the top load items table below the **Average Active Sessions** chart. Choose a particular item, like a SQL query or a user, to drill down into that item and see details about it.

DB load grouped by waits and top SQL queries is the default Performance Insights dashboard view. This combination typically provides the most insight into performance issues. DB load grouped by waits shows if there are any resource or concurrency bottlenecks in the database. In this case, the **SQL** tab of the top load items table shows which queries are driving that load.

Your typical workflow for diagnosing performance issues is as follows:

1. Review the **Average Active Sessions** chart and see if there are any incidents of database load exceeding the **Max CPU** line.
2. If there is, look at the **Average Active Sessions** chart and identify which wait state or states are primarily responsible.
3. Identify the digest queries causing the load by seeing which of the queries the **SQL** tab on the top load items table are contributing most to those wait states. You can identify these by the **DB Load by Wait** column.
4. Choose one of these digest queries in the **SQL** tab to expand it and see the child queries that it is composed of.

For example, in the dashboard following, **log file sync** waits account for most of the DB load. The **LGWR all worker groups** wait is also high. The **Top sql** chart shows what is causing the **log file sync** waits: frequent **COMMIT** statements. In this case, committing less frequently will reduce DB load.
Analyzing statistics for running queries

In Amazon RDS Performance Insights, you can find statistics on running queries in the Top SQL section. Performance Insights collects statistics only for the most common queries. Typically, these match the top queries by load shown in the Performance Insights dashboard.

Topics
- Statistics for Aurora MySQL (p. 533)
- Statistics for Aurora PostgreSQL (p. 536)

Statistics for Aurora MySQL

Performance Insights collects SQL digest statistics from the events_statements_summary_by_digest table. This table is managed by the database and doesn't have an eviction policy. If the table becomes full, new SQL queries aren't tracked. To address this issue, Performance Insights automatically truncates the table when it's nearly full.

Performance Insights automatically truncates the table only if your parameter group doesn't have an explicitly set value for the performance_schema parameter. You can examine the performance_schema parameter, and if the value of source is user, then you set a value. If you want Performance Insights to truncate the table automatically, then reset the value for the performance_schema parameter. You can view the source of a parameter value by viewing the parameter in the AWS Management Console or by running the AWS CLI describe-db-parameters command. The following message is shown in the AWS Management Console when the table is full:

```
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.
```

The following SQL statistics are available for Aurora MySQL DB clusters.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>db.sql_tokenized.stats.count_star_per_sec</code></td>
<td>Calls per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_timer_wait_per_sec</code></td>
<td>Average active executions per second (AAE)</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_select_full_join_per_sec</code></td>
<td>Select full join per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_select_range_check_per_sec</code></td>
<td>Select range check per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_select_scan_per_sec</code></td>
<td>Select scan per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_sort_merge_passes_per_sort</code></td>
<td>Merge passes per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_sort_scan_per_sec</code></td>
<td>Sort scans per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_sort_range_per_sec</code></td>
<td>Sort ranges per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_sort_rows_per_sec</code></td>
<td>Sort rows per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_rows_affected_per_sec</code></td>
<td>Rows affected per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.sum_rows_examined_per_sec</code></td>
<td>Rows examined per second</td>
</tr>
</tbody>
</table>
Analyzing Aurora MySQL Metrics for running SQL statements

Using the AWS Management Console, you can view the metrics for a running SQL query by choosing the SQL tab and expanding the query.
Choose which statistics to display by choosing the gear icon in the upper-right corner of the chart.

The following screenshot shows the preferences for Aurora MySQL DB instances.
Statistics for Aurora PostgreSQL

To view SQL Digest statistics, the `pg_stat_statements` library must be loaded. For Aurora PostgreSQL DB clusters that are compatible with PostgreSQL 10, this library is loaded by default. For Aurora PostgreSQL DB clusters that are compatible with PostgreSQL 9.6, you enable this library manually. To enable it manually, add `pg_stat_statements` to `shared_preload_libraries` in the DB parameter group associated with the DB instance. Then reboot your DB instance. For more information, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

**Note**

Performance Insights can only collect statistics for queries in `pg_stat_activity` that aren't truncated. By default, PostgreSQL databases truncate queries longer than 1,024 bytes. To increase the query size, change the `track_activity_query_size` parameter in the DB parameter group associated with your DB instance. When you change this parameter, a DB instance reboot is required.

The following SQL Digest statistics are available for Aurora PostgreSQL DB instances.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>db.sql_tokenized.stats.calls_per_sec</code></td>
<td>Calls per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.rows_per_sec</code></td>
<td>Rows per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.total_time_per_sec</code></td>
<td>Average active executions per second (AAE)</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.shared_blks_hit_per_sec</code></td>
<td>Block hits per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.shared_blks_read_per_sec</code></td>
<td>Block reads per second</td>
</tr>
</tbody>
</table>
### Metric and Unit

<table>
<thead>
<tr>
<th>Metric</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>db.sql_tokenized.stats.shared_blks_dirtied_per_sec</code></td>
<td>Blocks dirtied per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.shared_blks_written_per_sec</code></td>
<td>Block writes per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.local_blks_hit_per_sec</code></td>
<td>Local block hits per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.local_blks_read_per_sec</code></td>
<td>Local block reads per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.local_blks_dirtied_per_sec</code></td>
<td>Local block dirty per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.local_blks_written_per_sec</code></td>
<td>Local block writes per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.temp_blks_written_per_sec</code></td>
<td>Temporary writes per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.temp_blks_read_per_sec</code></td>
<td>Temporary reads per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.blk_read_time_per_sec</code></td>
<td>Average concurrent reads per second</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.blk_write_time_per_sec</code></td>
<td>Average concurrent writes per second</td>
</tr>
</tbody>
</table>

The following metrics provide per call statistics for a SQL statement.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>db.sql_tokenized.stats.rows_per_call</code></td>
<td>Rows per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.avg_latency_per_call</code></td>
<td>Average latency per call (in ms)</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.shared_blks_hit_per_call</code></td>
<td>Block hits per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.shared_blks_read_per_call</code></td>
<td>Block reads per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.shared_blks_written_per_call</code></td>
<td>Block writes per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.shared_blks_dirtied_per_call</code></td>
<td>Blocks dirtied per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.local_blks_hit_per_call</code></td>
<td>Local block hits per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.local_blks_read_per_call</code></td>
<td>Local block reads per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.local_blks_dirtied_per_call</code></td>
<td>Local block dirty per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.local_blks_written_per_call</code></td>
<td>Local block writes per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.temp_blks_written_per_call</code></td>
<td>Temporary block writes per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.temp_blks_read_per_call</code></td>
<td>Temporary block reads per call</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.blk_read_time_per_call</code></td>
<td>Read time per call (in ms)</td>
</tr>
<tr>
<td><code>db.sql_tokenized.stats.blk_write_time_per_call</code></td>
<td>Write time per call (in ms)</td>
</tr>
</tbody>
</table>

For more information about these metrics, see [pg_stat_statements](https://www.postgresql.org/docs/current/static/views-pgstat-statements.html) in the PostgreSQL documentation.

**Analyzing Aurora PostgreSQL metrics for running SQL statements**

Using the AWS Management Console, you can view the metrics for a running SQL query by choosing the **SQL** tab.
Choose which statistics to display by choosing the gear icon in the upper-right corner of the chart.

The following screenshot shows the preferences for Aurora PostgreSQL.
Viewing more SQL text in the Performance Insights dashboard

By default, each row in the Top sql table shows 500 bytes of SQL text for each SQL statement. When a SQL statement is larger than 500 bytes, you can view more of the SQL statement by opening the statement in the Performance Insights dashboard. The dashboard displays text up to the following per-engine limits:

- Aurora MySQL 5.7 — 4,096 bytes
- Aurora MySQL 5.6 — 1,024 bytes

You can copy the text that is displayed on the dashboard, or choose Download.

Aurora PostgreSQL handles text differently. Using the Performance Insights dashboard, you can view and download up to 500 bytes. To access more than 500 bytes, set the size limit with the DB instance parameter track_activity_query_size. The maximum value is 102,400 bytes. To view or download text over 500 bytes, use the AWS Management Console, not the Performance Insights CLI or API. For more information, see Setting the SQL text limit for Aurora PostgreSQL DB instances (p. 540).
To view more SQL text in the Performance Insights dashboard

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Performance Insights**.
3. Choose a DB instance. The Performance Insights dashboard is displayed for that DB instance.

   SQL statements with text larger than 500 bytes look similar to the following image.

   ![Performance Insights dashboard](image)

4. Examine the SQL information section to view more of the SQL text.

   ![SQL information](image)

   The Performance Insights dashboard can display up to 4,096 bytes for each SQL statement.

5. (Optional) Choose **Copy** to copy the displayed SQL statement, or choose **Download** to download the SQL statement to view the SQL text up to the DB engine limit.

   **Note**
   
   To copy or download the SQL statement, disable pop-up blockers.

### Setting the SQL text limit for Aurora PostgreSQL DB instances

For Aurora PostgreSQL DB instances, you can control the limit for the SQL text that can be shown on the Performance Insights dashboard.

To do so, modify the `track_activity_query_size` DB instance parameter. On Aurora PostgreSQL version 9.6, the default setting for the `track_activity_query_size` parameter is 1,024 bytes. On Aurora PostgreSQL version 10 or higher, the default setting for the `track_activity_query_size` parameter is 4,096 bytes.

You can increase the number of bytes to increase the SQL text size visible in the Performance Insights dashboard. The limit for the parameter is 102,400 bytes. For more information about the
track_activity_query_size DB instance parameter, see Run-time Statistics in the PostgreSQL documentation.

To modify the parameter, change the parameter setting in the parameter group that is associated with the Aurora PostgreSQL DB instance.

If the Aurora PostgreSQL DB instance is using the default parameter group, complete the following steps:

1. Create a new DB instance parameter group for the appropriate DB engine and DB engine version.
2. Set the parameter in the new parameter group.
3. Associate the new parameter group with the DB instance.

For information about setting a DB instance parameter, see Modifying parameters in a DB parameter group (p. 303).

**Zooming In on the DB Load chart**

You can use other features of the Performance Insights user interface to help analyze performance data.

**Click-and-Drag Zoom In**

In the Performance Insights interface, you can choose a small portion of the load chart and zoom in on the detail.

To zoom in on a portion of the load chart, choose the start time and drag to the end of the time period you want. When you do this, the selected area is highlighted. When you release the mouse, the load chart zooms in on the selected AWS Region, and the Top items table is recalculated.
Customizing the Performance Insights dashboard

With counter metrics, you can customize the Performance Insights dashboard to include up to 10 additional graphs. These graphs that show a selection of dozens of operating system and database performance metrics. This information can be correlated with database load to help identify and analyze performance problems.

Topics

- Performance Insights operating system counters (p. 542)
- Performance Insights counters for Aurora MySQL (p. 545)
- Performance Insights counters for Aurora PostgreSQL (p. 547)

Performance Insights operating system counters

The following operating system counters are available with Performance Insights for Aurora PostgreSQL. You can find definitions for these metrics in Viewing Enhanced Monitoring by using CloudWatch Logs (p. 509).
<table>
<thead>
<tr>
<th>Counter</th>
<th>Type</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>memory</td>
<td>os.memory.active</td>
</tr>
<tr>
<td>buffers</td>
<td>memory</td>
<td>os.memory.buffers</td>
</tr>
<tr>
<td>cached</td>
<td>memory</td>
<td>os.memory.cached</td>
</tr>
<tr>
<td>dirty</td>
<td>memory</td>
<td>os.memory.dirty</td>
</tr>
<tr>
<td>free</td>
<td>memory</td>
<td>os.memory.free</td>
</tr>
<tr>
<td>hugePagesFree</td>
<td>memory</td>
<td>os.memory.hugePagesFree</td>
</tr>
<tr>
<td>hugePagesRsvd</td>
<td>memory</td>
<td>os.memory.hugePagesRsvd</td>
</tr>
<tr>
<td>hugePagesSize</td>
<td>memory</td>
<td>os.memory.hugePagesSize</td>
</tr>
<tr>
<td>hugePagesSurp</td>
<td>memory</td>
<td>os.memory.hugePagesSurp</td>
</tr>
<tr>
<td>hugePagesTotal</td>
<td>memory</td>
<td>os.memory.hugePagesTotal</td>
</tr>
<tr>
<td>inactive</td>
<td>memory</td>
<td>os.memory.inactive</td>
</tr>
<tr>
<td>mapped</td>
<td>memory</td>
<td>os.memory.mapped</td>
</tr>
<tr>
<td>pageTables</td>
<td>memory</td>
<td>os.memory.pageTables</td>
</tr>
<tr>
<td>slab</td>
<td>memory</td>
<td>os.memory.slab</td>
</tr>
<tr>
<td>total</td>
<td>memory</td>
<td>os.memory.total</td>
</tr>
<tr>
<td>writeback</td>
<td>memory</td>
<td>os.memory.writeback</td>
</tr>
<tr>
<td>guest</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.guest</td>
</tr>
<tr>
<td>idle</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.idle</td>
</tr>
<tr>
<td>irq</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.irq</td>
</tr>
<tr>
<td>nice</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.nice</td>
</tr>
<tr>
<td>steal</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.steal</td>
</tr>
<tr>
<td>system</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.system</td>
</tr>
<tr>
<td>total</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.total</td>
</tr>
<tr>
<td>user</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.user</td>
</tr>
<tr>
<td>wait</td>
<td>cpuUtilization</td>
<td>os.cpuUtilization.wait</td>
</tr>
<tr>
<td>avgQueueLen</td>
<td>diskIO</td>
<td>os.diskIO.avgQueueLen</td>
</tr>
<tr>
<td>avgReqSz</td>
<td>diskIO</td>
<td>os.diskIO.avgReqSz</td>
</tr>
<tr>
<td>await</td>
<td>diskIO</td>
<td>os.diskIO.await</td>
</tr>
<tr>
<td>readIOsPS</td>
<td>diskIO</td>
<td>os.diskIO.readIOsPS</td>
</tr>
<tr>
<td>readKb</td>
<td>diskIO</td>
<td>os.diskIO.readKb</td>
</tr>
<tr>
<td>readKbPS</td>
<td>diskIO</td>
<td>os.diskIO.readKbPS</td>
</tr>
<tr>
<td>Counter</td>
<td>Type</td>
<td>Metric</td>
</tr>
<tr>
<td>----------------</td>
<td>-------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>rrqmPS</td>
<td>diskIO</td>
<td>os.diskIO.rrqmPS</td>
</tr>
<tr>
<td>tps</td>
<td>diskIO</td>
<td>os.diskIO.tps</td>
</tr>
<tr>
<td>util</td>
<td>diskIO</td>
<td>os.diskIO.util</td>
</tr>
<tr>
<td>writeIosPS</td>
<td>diskIO</td>
<td>os.diskIO.writeIosPS</td>
</tr>
<tr>
<td>writeKb</td>
<td>diskIO</td>
<td>os.diskIO.writeKb</td>
</tr>
<tr>
<td>writeKbps</td>
<td>diskIO</td>
<td>os.diskIO.writeKbps</td>
</tr>
<tr>
<td>wrqmPS</td>
<td>diskIO</td>
<td>os.diskIO.wrqmPS</td>
</tr>
<tr>
<td>blocked</td>
<td>tasks</td>
<td>os.tasks.blocked</td>
</tr>
<tr>
<td>running</td>
<td>tasks</td>
<td>os.tasks.running</td>
</tr>
<tr>
<td>sleeping</td>
<td>tasks</td>
<td>os.tasks.sleeping</td>
</tr>
<tr>
<td>stopped</td>
<td>tasks</td>
<td>os.tasks.stopped</td>
</tr>
<tr>
<td>total</td>
<td>tasks</td>
<td>os.tasks.total</td>
</tr>
<tr>
<td>zombie</td>
<td>tasks</td>
<td>os.tasks.zombie</td>
</tr>
<tr>
<td>one</td>
<td>loadAverageMinute</td>
<td>os.loadAverageMinute.one</td>
</tr>
<tr>
<td>fifteen</td>
<td>loadAverageMinute</td>
<td>os.loadAverageMinute.fifteen</td>
</tr>
<tr>
<td>five</td>
<td>loadAverageMinute</td>
<td>os.loadAverageMinute.five</td>
</tr>
<tr>
<td>cached</td>
<td>swap</td>
<td>os.swap.cached</td>
</tr>
<tr>
<td>free</td>
<td>swap</td>
<td>os.swap.free</td>
</tr>
<tr>
<td>in</td>
<td>swap</td>
<td>os.swap.in</td>
</tr>
<tr>
<td>out</td>
<td>swap</td>
<td>os.swap.out</td>
</tr>
<tr>
<td>total</td>
<td>swap</td>
<td>os.swap.total</td>
</tr>
<tr>
<td>maxFiles</td>
<td>fileSys</td>
<td>os.fileSys.maxFiles</td>
</tr>
<tr>
<td>usedFiles</td>
<td>fileSys</td>
<td>os.fileSys.usedFiles</td>
</tr>
<tr>
<td>usedFilePercent</td>
<td>fileSys</td>
<td>os.fileSys.usedFilePercent</td>
</tr>
<tr>
<td>usedPercent</td>
<td>fileSys</td>
<td>os.fileSys.usedPercent</td>
</tr>
<tr>
<td>used</td>
<td>fileSys</td>
<td>os.fileSys.used</td>
</tr>
<tr>
<td>total</td>
<td>fileSys</td>
<td>os.fileSys.total</td>
</tr>
<tr>
<td>rx</td>
<td>network</td>
<td>os.network.rx</td>
</tr>
<tr>
<td>tx</td>
<td>network</td>
<td>os.network.tx</td>
</tr>
<tr>
<td>numVCPUs</td>
<td>general</td>
<td>os.general.numVCPUs</td>
</tr>
</tbody>
</table>
Performance Insights counters for Aurora MySQL

The following database counters are available with Performance Insights for Aurora MySQL.

**Topics**
- Native counters for Aurora MySQL (p. 545)
- Non-native counters for Aurora MySQL (p. 546)

Native counters for Aurora MySQL

You can find definitions for these native metrics in Server Status Variables in the MySQL documentation.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Type</th>
<th>Unit</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Com_analyze</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Com_analyze</td>
</tr>
<tr>
<td>Com_optimize</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Com_optimize</td>
</tr>
<tr>
<td>Com_select</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Com_select</td>
</tr>
<tr>
<td>Innodb_rows_deleted</td>
<td>SQL</td>
<td>Rows per second</td>
<td>db.SQL.Innodb_rows_deleted</td>
</tr>
<tr>
<td>Innodb_rows_inserted</td>
<td>SQL</td>
<td>Rows per second</td>
<td>db.SQL.Innodb_rows_inserted</td>
</tr>
<tr>
<td>Innodb_rows_read</td>
<td>SQL</td>
<td>Rows per second</td>
<td>db.SQL.Innodb_rows_read</td>
</tr>
<tr>
<td>Innodb_rows_updated</td>
<td>SQL</td>
<td>Rows per second</td>
<td>db.SQL.Innodb_rows_updated</td>
</tr>
<tr>
<td>Questions</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Questions</td>
</tr>
<tr>
<td>Select_full_join</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Select_full_join</td>
</tr>
<tr>
<td>Select_full_range_join</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Select_full_range_join</td>
</tr>
<tr>
<td>Select_range</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Select_range</td>
</tr>
<tr>
<td>Select_range_check</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Select_range_check</td>
</tr>
<tr>
<td>Select_scan</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Select_scan</td>
</tr>
<tr>
<td>Slow_queries</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Slow_queries</td>
</tr>
<tr>
<td>Sort_merge_passes</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Sort_merge_passes</td>
</tr>
<tr>
<td>Sort_range</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Sort_range</td>
</tr>
<tr>
<td>Sort_rows</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Sort_rows</td>
</tr>
<tr>
<td>Sort_scan</td>
<td>SQL</td>
<td>Queries per second</td>
<td>db.SQL.Sort_scan</td>
</tr>
<tr>
<td>Table_locks_immediate</td>
<td>Locks</td>
<td>Requests per second</td>
<td>db.Locks.Table_locks_immediate</td>
</tr>
<tr>
<td>Table_locks_waited</td>
<td>Locks</td>
<td>Requests per second</td>
<td>db.Locks.Table_locks_waited</td>
</tr>
<tr>
<td>Innodb_row_lock_time</td>
<td>Locks</td>
<td>Milliseconds (average)</td>
<td>db.Locks.Innodb_row_lock_time</td>
</tr>
<tr>
<td>Aborted_clients</td>
<td>Users</td>
<td>Connections</td>
<td>db.Users.Aborted_clients</td>
</tr>
<tr>
<td>Aborted_connects</td>
<td>Users</td>
<td>Connections</td>
<td>db.Users.Aborted_connects</td>
</tr>
<tr>
<td>Counter</td>
<td>Type</td>
<td>Unit</td>
<td>Metric</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Threads_created</td>
<td>Users</td>
<td>Connections</td>
<td>db.Users.Threads_created</td>
</tr>
<tr>
<td>Threads_running</td>
<td>Users</td>
<td>Connections</td>
<td>db.Users.Threads_running</td>
</tr>
<tr>
<td>Created_tmp_disk_tables</td>
<td>Temp</td>
<td>Tables per second</td>
<td>db.Temp.Created_tmp_disk_tables</td>
</tr>
<tr>
<td>Created_tmp_tables</td>
<td>Temp</td>
<td>Tables per second</td>
<td>db.Temp.Created_tmp_tables</td>
</tr>
<tr>
<td>Innodb_buffer_pool_page_data</td>
<td>Cache</td>
<td>Pages</td>
<td>db.Cache.Innodb_buffer_pool_pages_data</td>
</tr>
<tr>
<td>Innodb_buffer_pool_page_cache</td>
<td>Cache</td>
<td>Pages</td>
<td>db.Cache.Innodb_buffer_pool_pages_cache</td>
</tr>
<tr>
<td>Innodb_buffer_pool_read_cache</td>
<td>Cache</td>
<td>Pages per second</td>
<td>db.Cache.Innodb_buffer_pool_read_cache</td>
</tr>
<tr>
<td>Innodb_buffer_pool_reads_cache</td>
<td>Cache</td>
<td>Pages per second</td>
<td>db.Cache.Innodb_buffer_pool_reads_cache</td>
</tr>
<tr>
<td>Opened_tables</td>
<td>Cache</td>
<td>Tables</td>
<td>db.Cache.Opened_tables</td>
</tr>
<tr>
<td>Opened_table_definitions</td>
<td>Cache</td>
<td>Tables</td>
<td>db.Cache.Opened_table_definitions</td>
</tr>
<tr>
<td>Qcache_hits</td>
<td>Cache</td>
<td>Queries</td>
<td>db.Cache.Qcache_hits</td>
</tr>
</tbody>
</table>

**Non-native counters for Aurora MySQL**

Non-native counter metrics are counters defined by Amazon RDS. A non-native metric can be a metric that you get with a specific query. A non-native metric also can be a derived metric, where two or more native counters are used in calculations for ratios, hit rates, or latencies.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Type</th>
<th>Metric</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>innodb_buffer_pool_hits</td>
<td>Cache</td>
<td>db.Cache.innodb_buffer_pool_read_requests</td>
<td>The number of reads that InnoDB could satisfy from the buffer pool.</td>
<td>innodb_buffer_pool_read_requests - innodb_buffer_pool_reads</td>
</tr>
<tr>
<td>innodb_buffer_pool_hit_rate</td>
<td>Cache</td>
<td>db.Cache.innodb_buffer_pool_read_requests</td>
<td>The percentage of reads that InnoDB could satisfy from the buffer pool.</td>
<td>100 * (innodb_buffer_pool_read_requests / (innodb_buffer_pool_read_requests + innodb_buffer_pool_reads))</td>
</tr>
</tbody>
</table>

**Note**
When using compressed tables, this value can vary. For more information, see the information about `Innodb_buffer_pool_pages_data` and `Innodb_buffer_pool_pages_total` in Server Status Variables.
### Performance Insights counters for Aurora PostgreSQL

The following database counters are available with Performance Insights for Aurora PostgreSQL.

**Topics**
- Native Counters for Aurora PostgreSQL (p. 547)
- Non-native counters for Aurora PostgreSQL (p. 549)

### Native Counters for Aurora PostgreSQL

You can find definitions for these native metrics in *Viewing Statistics* in the PostgreSQL documentation.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Type</th>
<th>Unit</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>tup_deleted</td>
<td>SQL</td>
<td>Tuples per second</td>
<td>db.SQL.tup_deleted</td>
</tr>
</tbody>
</table>

---

Performance Insights counters for Aurora PostgreSQL

The following database counters are available with Performance Insights for Aurora PostgreSQL.

**Topics**
- Native Counters for Aurora PostgreSQL (p. 547)
- Non-native counters for Aurora PostgreSQL (p. 549)

### Native Counters for Aurora PostgreSQL

You can find definitions for these native metrics in *Viewing Statistics* in the PostgreSQL documentation.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Type</th>
<th>Unit</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>tup_deleted</td>
<td>SQL</td>
<td>Tuples per second</td>
<td>db.SQL.tup_deleted</td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th>Counter</th>
<th>Type</th>
<th>Unit</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>tup_fetched</td>
<td>SQL</td>
<td>Tuples per second</td>
<td>db.SQL.tup_fetched</td>
</tr>
<tr>
<td>tup_inserted</td>
<td>SQL</td>
<td>Tuples per second</td>
<td>db.SQL.tup_inserted</td>
</tr>
<tr>
<td>tup_returned</td>
<td>SQL</td>
<td>Tuples per second</td>
<td>db.SQL.tup_returned</td>
</tr>
<tr>
<td>tup_updated</td>
<td>SQL</td>
<td>Tuples per second</td>
<td>db.SQL.tup_updated</td>
</tr>
<tr>
<td>buffers_checkpoint</td>
<td>Checkpoint</td>
<td>Blocks per second</td>
<td>db.Checkpoint.buffers_checkpoint</td>
</tr>
<tr>
<td>checkpoints_req</td>
<td>Checkpoint</td>
<td>Checkpoints per minute</td>
<td>db.Checkpoint.checkpoints_req</td>
</tr>
<tr>
<td>checkpoint_sync_time</td>
<td>Checkpoint</td>
<td>Milliseconds per checkpoint</td>
<td>db.Checkpoint.checkpoint_sync_time</td>
</tr>
<tr>
<td>checkpoints_timed</td>
<td>Checkpoint</td>
<td>Checkpoints per minute</td>
<td>db.Checkpoint.checkpoints_timed</td>
</tr>
<tr>
<td>checkpoint_write_time</td>
<td>Checkpoint</td>
<td>Milliseconds per checkpoint</td>
<td>db.Checkpoint.checkpoint_write_time</td>
</tr>
<tr>
<td>maxwritten_clean</td>
<td>Checkpoint</td>
<td>Bgwriter clean stops per minute</td>
<td>db.Checkpoint.maxwritten_clean</td>
</tr>
<tr>
<td>active_transactions</td>
<td>Transactions</td>
<td>Transactions</td>
<td>db.Transactions.active_transactions</td>
</tr>
<tr>
<td>blocked_transactions</td>
<td>Transactions</td>
<td>Transactions</td>
<td>db.Transactions.blocked_transactions</td>
</tr>
<tr>
<td>max_used_xact_ids</td>
<td>Transactions</td>
<td>Transactions</td>
<td>db.Transactions.max_used_xact_ids</td>
</tr>
<tr>
<td>xact_commit</td>
<td>Transactions</td>
<td>Commits per second</td>
<td>db.Transactions.xact_commit</td>
</tr>
<tr>
<td>xact_rollback</td>
<td>Transactions</td>
<td>Rollbacks per second</td>
<td>db.Transactions.xact_rollback</td>
</tr>
<tr>
<td>blk_read_time</td>
<td>I/O</td>
<td>Milliseconds</td>
<td>db.IO.blk_read_time</td>
</tr>
<tr>
<td>blks_read</td>
<td>I/O</td>
<td>Blocks per second</td>
<td>db.IO.blks_read</td>
</tr>
<tr>
<td>buffers_backend</td>
<td>I/O</td>
<td>Blocks per second</td>
<td>db.IO.buffers_backend</td>
</tr>
<tr>
<td>buffers_backend_fsync</td>
<td>I/O</td>
<td>Blocks per second</td>
<td>db.IO.buffers_backend_fsync</td>
</tr>
<tr>
<td>buffers_clean</td>
<td>I/O</td>
<td>Blocks per second</td>
<td>db.IO.buffers_clean</td>
</tr>
<tr>
<td>blks_hit</td>
<td>Cache</td>
<td>Blocks per second</td>
<td>db.Cache.blks_hit</td>
</tr>
<tr>
<td>buffers_alloc</td>
<td>Cache</td>
<td>Blocks per second</td>
<td>db.Cache.buffers_alloc</td>
</tr>
<tr>
<td>temp_files</td>
<td>Temp</td>
<td>Files per minute</td>
<td>db.Temp.temp_files</td>
</tr>
<tr>
<td>numbackends</td>
<td>User</td>
<td>Connections</td>
<td>db.User.numbackends</td>
</tr>
<tr>
<td>deadlocks</td>
<td>Concurrency</td>
<td>Deadlocks per minute</td>
<td>db.Concurrency.deadlocks</td>
</tr>
<tr>
<td>archived_count</td>
<td>WAL</td>
<td>Files per minute</td>
<td>db.WAL.archived_count</td>
</tr>
<tr>
<td>archive_failed_count</td>
<td>WAL</td>
<td>Files per minute</td>
<td>db.WAL.archive_failed_count</td>
</tr>
</tbody>
</table>
Non-native counters for Aurora PostgreSQL

Non-native counter metrics are counters defined by Amazon RDS. A non-native metric can be a metric that you get with a specific query. A non-native metric also can be a derived metric, where two or more native counters are used in calculations for ratios, hit rates, or latencies.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Type</th>
<th>Metric</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkpoint_sync_latency</td>
<td>Checkpoint</td>
<td>db.Checkpoint.checkpoint_sync_latency</td>
<td>The total amount of time that has been spent in the portion of checkpoint processing where files are synchronized to disk.</td>
<td>checkpoint_sync_time / (checkpoints_timed + checkpoints_reg)</td>
</tr>
<tr>
<td>checkpoint_write_latency</td>
<td>Checkpoint</td>
<td>db.Checkpoint.checkpoint_write_latency</td>
<td>The total amount of time that has been spent in the portion of checkpoint processing where files are written to disk.</td>
<td>checkpoint_write_time / (checkpoints_timed + checkpoints_reg)</td>
</tr>
<tr>
<td>read_latency</td>
<td>I/O</td>
<td>db.IO.read_latency</td>
<td>The time spent reading data file blocks by backends in this instance.</td>
<td>blk_read_time / blks_read</td>
</tr>
</tbody>
</table>

Retrieving data with the Performance Insights API

When Performance Insights is enabled for supported engine types, the API provides visibility into instance performance. Amazon CloudWatch Logs provides the authoritative source for vended monitoring metrics for AWS services.

Performance Insights offers a domain-specific view of database load measured as average active sessions (AAS). This metric appears to API consumers as a two-dimensional time-series dataset. The time dimension of the data provides DB load data for each time point in the queried time range. Each time point decomposes overall load in relation to the requested dimensions, such as SQL, Wait-event, User, or Host, measured at that time point.

Amazon RDS Performance Insights monitors your Amazon RDS DB instance so that you can analyze and troubleshoot database performance. One way to view Performance Insights data is in the AWS Management Console. Performance Insights also provides a public API so that you can query your own data. You can use the API to offload data into a database, add Performance Insights data to existing monitoring dashboards, or to build monitoring tools. To use the Performance Insights API, enable Performance Insights on one of your Amazon RDS DB instances. For information about enabling Performance Insights, see Enabling and disabling Performance Insights (p. 517).

The Performance Insights API provides the following operations.

<table>
<thead>
<tr>
<th>Performance Insights Operation</th>
<th>AWS CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeDimensionKeys</td>
<td>aws pi describe-dimension-keys</td>
<td>Retrieves the top N dimension keys for a metric for a specific time period.</td>
</tr>
<tr>
<td>GetResourceMetrics</td>
<td>aws pi get-resource-metrics</td>
<td>Retrieves Performance Insights metrics for a set of data sources, over a time period. You can</td>
</tr>
</tbody>
</table>
For more information about the Performance Insights API, see the Amazon RDS Performance Insights API Reference.

**AWS CLI for Performance Insights**

You can view Performance Insights data using the AWS CLI. You can view help for the AWS CLI commands for Performance Insights by entering the following on the command line.

```
aws pi help
```

If you don't have the AWS CLI installed, see Installing the AWS Command Line Interface in the AWS CLI User Guide for information about installing it.

**Retrieving time-series metrics**

The `GetResourceMetrics` operation retrieves one or more time-series metrics from the Performance Insights data. `GetResourceMetrics` requires a metric and time period, and returns a response with a list of data points.

For example, the AWS Management Console uses `GetResourceMetrics` in two places in the Performance Insights dashboard. `GetResourceMetrics` is used to populate the Counter Metrics chart and in the Database Load chart, as seen in the following image.

![Counter Metrics](image1.png)

![Database Load](image2.png)

All the metrics returned by `GetResourceMetrics` are standard time-series metrics with one exception. The exception is `db.load`, which is the core metric in Performance Insights. This metric is displayed in the Database Load chart. The `db.load` metric is different from the other time-series metrics because you can break it into subcomponents called dimensions. In the previous image, `db.load` is broken down and grouped by the waits states that make up the `db.load`.
Note
GetResourceMetrics can also return the db.sampleload metric, but the db.load metric is appropriate in most cases.

For information about the counter metrics returned by GetResourceMetrics, see Customizing the Performance Insights dashboard (p. 542).

The following calculations are supported for the metrics:

- Average – The average value for the metric over a period of time. Append .avg to the metric name.
- Minimum – The minimum value for the metric over a period of time. Append .min to the metric name.
- Maximum – The maximum value for the metric over a period of time. Append .max to the metric name.
- Sum – The sum of the metric values over a period of time. Append .sum to the metric name.
- Sample count – The number of times the metric was collected over a period of time. Append .sample_count to the metric name.

For example, assume that a metric is collected for 300 seconds (5 minutes), and that the metric is collected one time each minute. The values for each minute are 1, 2, 3, 4, and 5. In this case, the following calculations are returned:

- Average – 3
- Minimum – 1
- Maximum – 5
- Sum – 15
- Sample count – 5

For information about using the get-resource-metrics AWS CLI command, see get-resource-metrics.

For the --metric-queries option, specify one or more queries that you want to get results for. Each query consists of a mandatory Metric and optional GroupBy and Filter parameters. The following is an example of a --metric-queries option specification.

```
{
  "Metric": "string",
  "GroupBy": {
    "Group": "string",
    "Dimensions": ["string", ...],
    "Limit": integer
  },
  "Filter": {"string": "string"
...
}
```

AWS CLI examples for Performance Insights

The following are several examples that use the AWS CLI for Performance Insights.

Topics
- Retrieving counter metrics (p. 552)
- Retrieving the DB load average for top wait events (p. 554)
- Retrieving the DB load average for top SQL (p. 556)
• Retrieving the DB Load Average Filtered by SQL (p. 558)

Retrieving counter metrics

The following screenshot shows two counter metrics charts in the AWS Management Console.

![Counter Metrics Chart]

The following example shows how to gather the same data that the AWS Management Console uses to generate the two counter metric charts.

For Linux, macOS, or Unix:

```
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"]
```

For 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"]
```

You can also make a command easier to read by specifying a file for the --metrics-query option. The following example uses a file called query.json for the option. The file has the following contents.

```
[
  {
    "Metric": "os.cpuUtilization.user.avg",
    "Metric": "os.cpuUtilization.idle.avg"
  }
]```
Run the following command to use the file.

For Linux, macOS, or Unix:

```
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
```

For 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
```

The preceding example specifies the following values for the options:

- `--service-type` – RDS for Amazon RDS
- `--identifier` – The resource ID for the DB instance
- `--start-time` and `--end-time` – The ISO 8601 DateTime values for the period to query, with multiple supported formats

It queries for a one-hour time range:

- `--period-in-seconds` – 60 for a per-minute query
- `--metric-queries` – An array of two queries, each just for one metric.

The metric name uses dots to classify the metric in a useful category, with the final element being a function. In the example, the function is `avg` for each query. As with Amazon CloudWatch, the supported functions are `min`, `max`, `total`, and `avg`.

The response looks similar to the following.

```
{
  "Identifier": "db-XXX",
  "AlignedStartTime": 1540857600.0,
  "AlignedEndTime": 1540861200.0,
  "MetricList": [ //A list of key/datapoints
    {
      "Metric": "os.cpuUtilization.user.avg"
    },
    {
      "Metric": "os.cpuUtilization.idle.avg"
    }
  ]
}
```
The response has an Identifier, AlignedStartTime, and AlignedEndTime. By the --period-in-seconds value was 60, the start and end times have been aligned to the minute. If the --period-in-seconds was 3600, the start and end times would have been aligned to the hour.

The MetricList in the response has a number of entries, each with a Key and a DataPoints entry. Each DataPoint has a Timestamp and a Value. Each Datapoints list has 60 data points because the queries are for per-minute data over an hour, with Timestamp1/Minute1, Timestamp2/Minute2, and so on, up to Timestamp60/Minute60.

Because the query is for two different counter metrics, there are two elements in the response MetricList.

**Retrieving the DB load average for top wait events**

The following example is the same query that the AWS Management Console uses to generate a stacked area line graph. This example retrieves the db.load.avg for the last hour with load divided according to the top seven wait events. The command is the same as the command in Retrieving counter metrics (p. 552). However, the query.json file has the following contents.

```json
[
  {
    "Metric": "db.load.avg",
    "GroupBy": { "Group": "db.wait_event", "Limit": 7 }
  }
] // end of MetricList
} // end of response
```
Run the following command.

For Linux, macOS, or Unix:

```
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
```

For 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
```

The example specifies the metric of `db.load.avg` and a `GroupBy` of the top seven wait events. For details about valid values for this example, see `DimensionGroup` in the Performance Insights API Reference.

The response looks similar to the following.

```
{
    "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": 0.3833333333333336
                },
                { "Timestamp": 1540857780.0, //Minute 3
                    "Value": 0.2666666666666666
                }
            ]
        },
        //... 60 datapoints for the total db.load.avg key
    ]
}
```
In this response, there are eight entries in the MetricList. There is one entry for the total `db.load.avg`, and seven entries each for the `db.load.avg` divided according to one of the top seven wait events. Unlike in the first example, because there was a grouping dimension, there must be one key for each grouping of the metric. There can't be only one key for each metric, as in the basic counter metric use case.

**Retrieving the DB load average for top SQL**

The following example groups `db.wait_events` by the top 10 SQL statements. There are two different groups for SQL statements:

- `db.sql` - The full SQL statement, such as `select * from customers where customer_id = 123`
- `db.sql_tokenized` - The tokenized SQL statement, such as `select * from customers where customer_id = ?`

When analyzing database performance, it can be useful to consider SQL statements that only differ by their parameters as one logic item. So, you can use `db.sql_tokenized` when querying. However, especially when you are interested in explain plans, sometimes it's more useful to examine full SQL statements with parameters, and query grouping by `db.sql`. There is a parent-child relationship between tokenized and full SQL, with multiple full SQL (children) grouped under the same tokenized SQL (parent).

The command in this example is similar to the command in **Retrieving the DB load average for top wait events** (p. 554). However, the query.json file has the following contents.

```json
[
  {
    "Metric": "db.load.avg",
    "GroupBy": {
      "Group": "db.sql_tokenized",
      "Limit": 10
    }
  }
]
```

The following example uses `db.sql_tokenized`. 

556
For Linux, macOS, or Unix:

```bash
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
```

For Windows:

```bash
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
```

This example queries over 24 hours, with a one hour period-in-seconds.

The example specifies the metric of `db.load.avg` and a GroupBy of the top seven wait events. For details about valid values for this example, see DimensionGroup in the Performance Insights API Reference.

The response looks similar to the following.

```json
{
  "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
```
This response has 11 entries in the MetricList (1 total, 10 top tokenized SQL), with each entry having 24 per-hour DataPoints.

For tokenized SQL, there are three entries in each dimensions list:

- db.sql_tokenized.statement – The tokenized SQL statement.
- db.sql_tokenized.db_id – Either the native database ID used to refer to the SQL, or a synthetic ID that Performance Insights generates for you if the native database ID isn't available. This example returns the pi-2372568224 synthetic ID.
- db.sql_tokenized.id – The ID of the query inside Performance Insights.

In the AWS Management Console, this ID is called the Support ID. It's named this because the ID is data that AWS Support can examine to help you troubleshoot an issue with your database. AWS takes the security and privacy of your data extremely seriously, and almost all data is stored encrypted with your AWS KMS customer master key (CMK). Therefore, nobody inside AWS can look at this data. In the example preceding, both the tokenized.statement and the tokenized.db_id are stored encrypted. If you have an issue with your database, AWS Support can help you by referencing the Support ID.

When querying, it might be convenient to specify a Group in GroupBy. However, for finer-grained control over the data that's returned, specify the list of dimensions. For example, if all that is needed is the db.sql_tokenized.statement, then a Dimensions attribute can be added to the query.json file.

```
[
  {
    "Metric": "db.load.avg",
    "GroupBy": {
      "Group": "db.sql_tokenized",
      "Dimensions": ["db.sql_tokenized.statement"],
      "Limit": 10
    }
  }
]
```

Retrieving the DB Load Average Filtered by SQL
The preceding image shows that a particular query is selected, and the top average active sessions stacked area line graph is scoped to that query. Although the query is still for the top seven overall wait events, the value of the response is filtered. The filter causes it to take into account only sessions that are a match for the particular filter.

The corresponding API query in this example is similar to the command in Retrieving the DB load average for top SQL (p. 556). However, the query.json file has the following contents.

```json
[
   {
      "Metric": "db.load.avg",
      "GroupBy": { "Group": "db.wait_event", "Limit": 5 },
      "Filter": { "db.sql_tokenized.id": "AKIAIOSFODNN7EXAMPLE" }
   }
]
```

For Linux, macOS, or Unix:

```
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
```

For 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
```

The response looks similar to the following.

```json
{
   "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": [
In this response, all values are filtered according to the contribution of tokenized SQL
AKIAIOSFODNN7EXAMPLE specified in the query.json file. The keys also might follow a different order
than a query without a filter, because it's the top five wait events that affected the filtered SQL.

Performance Insights metrics published to Amazon CloudWatch

Performance Insights automatically publishes metrics to Amazon CloudWatch. The same data can
be queried from Performance Insights, but having the metrics in CloudWatch makes it easy to add
CloudWatch alarms. It also makes it easy to add the metrics to existing CloudWatch Dashboards.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBLoad</td>
<td>The number of active sessions for the DB engine. Typically, you want the data for the average number of active sessions. In Performance Insights, this data is queried as db.load.avg.</td>
</tr>
<tr>
<td>DBLoadCPU</td>
<td>The number of active sessions where the wait event type is CPU. In Performance Insights, this data is queried as db.load.avg, filtered by the wait event type CPU.</td>
</tr>
<tr>
<td>DBLoadNonCPU</td>
<td>The number of active sessions where the wait event type is not CPU.</td>
</tr>
</tbody>
</table>
Note
These metrics are published to CloudWatch only if there is load on the DB instance.

You can examine these metrics using the CloudWatch console, the AWS CLI, or the CloudWatch API.

For example, you can get the statistics for the `DBLoad` metric by running the `get-metric-statistics` command.

```
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
```

This example generates output similar to the following.

```
{
  "Datapoints": [
    {
      "Timestamp": "2018-07-19T21:30:00Z",
      "Unit": "None",
      "Average": 2.1,
    },
    {
      "Timestamp": "2018-07-19T21:34:00Z",
      "Unit": "None",
      "Average": 1.7,
    },
    {
      "Timestamp": "2018-07-19T21:35:00Z",
      "Unit": "None",
      "Average": 2.8,
    },
    {
      "Timestamp": "2018-07-19T21:31:00Z",
      "Unit": "None",
      "Average": 1.5,
    },
    {
      "Timestamp": "2018-07-19T21:32:00Z",
      "Unit": "None",
      "Average": 1.8,
    },
    {
      "Timestamp": "2018-07-19T21:29:00Z",
      "Unit": "None",
      "Average": 3.0,
    },
    {
      "Timestamp": "2018-07-19T21:33:00Z",
      "Unit": "None",
      "Average": 2.4,
    }
  ],
  "Label": "DBLoad"
}
```

For more information about CloudWatch, see What is Amazon CloudWatch? in the Amazon CloudWatch User Guide.
Logging Performance Insights calls by using AWS CloudTrail

Performance Insights runs with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Performance Insights. CloudTrail captures all API calls for Performance Insights as events. This capture includes calls from the Amazon RDS console and from code calls to the Performance Insights API operations.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Performance Insights. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the data collected by CloudTrail, you can determine certain information. This information includes the request that was made to Performance Insights, the IP address the request was made from, who made the request, and when it was made. It also includes additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Working with Performance Insights information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Performance Insights, that activity is recorded in a CloudTrail event along with other AWS service events in the CloudTrail console in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History in AWS CloudTrail User Guide.

For an ongoing record of events in your AWS account, including events for Performance Insights, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all AWS Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following topics in AWS CloudTrail User Guide:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All Performance Insights operations are logged by CloudTrail and are documented in the Performance Insights API Reference. For example, calls to the DescribeDimensionKeys and GetResourceMetrics operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.
Performance Insights log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source. Each event includes information about the requested operation, the date and time of the operation, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the GetResourceMetrics operation.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/johndoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHEXAMPLE",
        "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"
}
```
Using Database Activity Streams with Amazon Aurora

Monitoring your database activity can help you provide safeguards for your database and help to meet compliance and regulatory requirements. To monitor database activity with Amazon Aurora, you can use the Database Activity Streams feature. Database activity streams provide a near real-time stream of the activity in your relational database. When you integrate database activity streams with monitoring tools, you can monitor and audit database activity.

Beyond external security threats, managed databases need to provide protection against insider risks from database administrators (DBAs). Database activity streams help protect your databases from internal threats by controlling DBA access to the database activity streams. Thus, the collection, transmission, storage, and subsequent processing of the stream of database activity is beyond the access of the DBAs that manage the database.

A stream of database activity is pushed from Aurora to an Amazon Kinesis data stream that is created on behalf of your Aurora DB cluster. From Kinesis, the activity stream can then be consumed by AWS services such as Amazon Kinesis Data Firehose and AWS Lambda, or by applications for compliance management. For database activity streams with Aurora PostgreSQL, these compliance applications include IBM's Security Guardium, McAfee's Data Center Security Suite, and Imperva's SecureSphere Database Audit and Protection. Such applications can use the activity stream information to generate alerts and provide auditing of all activity on your Aurora DB clusters.

**Tip**
Check the website for the particular application that you want to use with database activity streams. Confirm support for the specific Aurora DB engine and engine version that you intend to use.

Database activity streams have the following limits and requirements:

- For Aurora PostgreSQL, database activity streams are supported for version 2.3 or higher and versions 3.0 or higher. For PostgreSQL version compatibility, see [Engine versions for Amazon Aurora PostgreSQL](p. 1148).
- For Aurora MySQL, database activity streams are supported for version 2.08 or higher, which is compatible with MySQL version 5.7.
- You can start a database activity stream on the primary or secondary cluster of an Aurora global database. For DB engine version requirements, see [Limitations of Amazon Aurora global databases](p. 207).
- Database activity streams support the DB instance classes listed for Aurora in [Supported DB engines for DB instance classes](p. 47), with some exceptions:
  - For Aurora PostgreSQL, you can't use streams with the db.t3.medium instance class.
  - For Aurora MySQL, you can't use streams with any of the db.t2 or db.t3 instance classes.
- Database activity streams aren't supported in the following AWS Regions:
  - China (Beijing) Region, cn-north-1
  - China (Ningxia) Region, cn-northwest-1
  - Asia Pacific (Osaka-Local), ap-northeast-3
  - AWS GovCloud (US-East), us-gov-east-1
  - AWS GovCloud (US-West), us-gov-west-1
- Database activity streams require use of AWS Key Management Service (AWS KMS). AWS KMS is required because the activity streams are always encrypted.
- Database activity streams aren't supported in Aurora Serverless.

**Topics**
Network prerequisites for Aurora MySQL Database Activity Streams

To use Database Activity Streams with Aurora MySQL, all the DB instances that use database activity streams within a VPC must be able to access AWS KMS endpoints. Make sure this requirement is satisfied before enabling database activity streams for your Aurora MySQL cluster.

Important
If the Aurora MySQL DB cluster can't access the AWS KMS endpoint, the activity stream stops functioning. In that case, Aurora notifies you about this issue using RDS Events.

Important
If the Aurora cluster is publicly available, this requirement is satisfied automatically.

If you receive a notification that your Aurora MySQL cluster can't use database activity streams because it can't access a AWS KMS endpoint, check if your Aurora DB cluster is public or private. If your Aurora DB cluster is private, you must configure it to enable connections.

For an Aurora DB cluster to be public, it must be marked as publicly accessible. If you look at the details for the DB cluster in the AWS Management Console, Publicly Accessible is Yes if this is the case. The DB cluster must also be in an Amazon VPC public subnet. For more information about publicly accessible DB instances, see Working with a DB instance in a VPC (p. 1291). For more information about public Amazon VPC subnets, see Your VPC and subnets.

For more information about configuring VPC endpoints, see VPC endpoints.

Starting a database activity stream

You start an activity stream at the DB cluster level to monitor database activity for all DB instances of the cluster. Any DB instances added to the cluster are also automatically monitored.

When you start an activity stream, each database activity event, such as a change or access, generates an activity stream event. Access events are generated from SQL commands such as CONNECT and SELECT. Change events are generated from SQL commands such as CREATE and INSERT. To make each activity stream event durable, Aurora encrypts and stores it.

You can choose to have the database session handle database activity events either asynchronously or synchronously:

- **Asynchronous mode** – In asynchronous mode, when a database session generates an activity stream event, the session returns to normal activities immediately. In the background, the activity stream event is made a durable record. If an error occurs in the background task, an RDS event is sent. This
event indicates the beginning and end of any time windows where activity stream event records might have been lost.

Asynchronous mode favors database performance over the accuracy of the activity stream.

**Note**
Asynchronous mode is available for both Aurora PostgreSQL and Aurora MySQL.

- **Synchronous mode** – In synchronous mode, when a database session generates an activity stream event, the session blocks other activities until the event is made durable. If the event can't be made durable for some reason, the database session returns to normal activities. However, an RDS event is sent indicating that activity stream records might be lost for some time. A second RDS event is sent after the system is back to a healthy state.

The synchronous mode favors the accuracy of the activity stream over database performance.

**Note**
Synchronous mode is available for Aurora PostgreSQL. You can't use synchronous mode with Aurora MySQL.

**Console**

**To start an activity stream**

1. Open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Databases**.
3. Choose the DB cluster that you want to use.
4. For **Actions**, choose **Start activity stream**. The **Database Activity Stream** window appears.
5. Enter the following settings in the **Database Activity Stream** window:
   - For **Master key**, choose a key from the list of AWS KMS customer master keys (CMKs).
     **Note**
     If your Aurora MySQL cluster can't access AWS KMS CMKs, follow the instructions in [Network prerequisites for Aurora MySQL Database Activity Streams](p. 566) to enable such access first.

     The master key is used to encrypt the key that in turn encrypts the database activity logged. You must choose a master key other than the default key. For more information about encryption keys and AWS KMS, see [What is AWS Key Management Service?](in the [AWS Key Management Service Developer Guide](p. 566).

   - For **Database activity stream mode**, choose **Asynchronous** or **Synchronous**.
     **Note**
     Currently, this choice only applies to Aurora PostgreSQL. For Aurora MySQL, you can use only asynchronous mode.

   - Choose **Apply immediately**.

     If you choose **Schedule for the next maintenance window**, the database doesn't restart right away. Instead, it remains in the **PENDING REBOOT** state. In this case, the database activity stream doesn't start until the next maintenance window.

When you're done entering settings, choose **Continue**.

The cluster's DB instance status shows that the database activity stream is being configured.
AWS CLI

To start database activity streams for a DB cluster, configure the DB cluster using the `start-activity-stream` AWS CLI command. Identify the AWS Region for the DB cluster with the `--region` parameter. The `--apply-immediately` parameter is optional.

For Linux, macOS, or Unix:

```bash
aws rds --region MY_REGION
   start-activity-stream
   --mode [sync | async]
   --kms-key-id MY_KMS_KEY_ARN
   --resource-arn MY_CLUSTER_ARN
   --apply-immediately
```

For Windows:

```bash
aws rds --region MY_REGION
   start-activity-stream
   --mode [sync | async]
   --kms-key-id MY_KMS_KEY_ARN
   --resource-arn MY_CLUSTER_ARN
   --apply-immediately
```

**Note**
The `--mode` parameter is required. For Aurora PostgreSQL, you can choose either value. For Aurora MySQL, you must always specify `async`.

Getting the status of an activity stream

You can get the status of an activity stream using the console or AWS CLI.

**Console**

**To get the status of a DB cluster's activity stream**

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases, and then choose the DB cluster.
3. Choose the Configuration tab, and check Database activity stream for status.

**AWS CLI**

You can get a DB cluster's activity stream configuration as the response to a `describe-db-clusters` CLI request. In the following example, see the values for `ActivityStreamKinesisStreamName`, `ActivityStreamStatus`, `ActivityStreamKmsKeyId`, and `ActivityStreamMode`.

The request is as follows.

```bash
aws rds --region MY_REGION describe-db-clusters --db-cluster-identifier my-cluster
```

The response includes the following items for a database activity stream.

The following example shows a JSON response. These fields are the same for Aurora PostgreSQL and Aurora MySQL, except that `ActivityStreamMode` is always `async` for Aurora MySQL, while for Aurora PostgreSQL it might be `sync` or `async`.
Stopping an activity stream

You can stop an activity stream using the console or AWS CLI.

If you delete a DB cluster, the activity stream is stopped and the underlying Amazon Kinesis stream is deleted automatically.

**Console**

**To turn off an activity stream**

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/
2. In the navigation pane, choose Databases.
3. Choose the DB cluster that you want to stop the database activity stream for.
4. For Actions, choose Stop activity stream. The Database Activity Stream window appears.
   a. Choose Apply immediately.
      
      If you choose Schedule for the next maintenance window, the database doesn’t restart right away. Instead, it remains in the PENDING REBOOT state. In this case, the data activity stream isn’t disabled until the next maintenance window.
   b. Choose Continue.

**AWS CLI**

To stop database activity streams for a DB cluster, configure the DB cluster using the AWS CLI command stop-activity-stream. Identify the AWS Region for the DB cluster using the --region parameter. The --apply-immediately parameter is optional.

For Linux, macOS, or Unix:

```bash
aws rds --region MY_REGION \ stop-activity-stream \ --resource-arn MY_CLUSTER_ARN \ --apply-immediately
```

For Windows:

```bash
aws rds --region MY_REGION ^
stop-activity-stream ^
--resource-arn MY_CLUSTER_ARN ^
```
Monitoring database activity streams

Database activity streams monitor and report activities on the database as described following.

The stream of activity is collected and transmitted to Amazon Kinesis. From Kinesis, you can monitor the activity stream, or other services and applications can consume the activity stream for further analysis. You can find the underlying Kinesis stream name by using the AWS CLI command `describe-db-clusters` or the RDS API `DescribeDBClusters` operation.

Aurora manages the Kinesis stream for you.

- You don’t use an existing Kinesis stream. Aurora creates the Kinesis stream automatically with a 24-hour retention period.
- Aurora scales the Kinesis stream if necessary.
- Aurora recreates the Kinesis stream if you delete it.
- If you stop the database activity stream or delete the DB cluster, Aurora deletes the Kinesis stream.

The following categories of activity are monitored and put in the activity stream audit log:

- **SQL commands** – All SQL commands are audited, and also prepared statements, built-in functions, and functions in Procedural Language for SQL (PL/SQL). Calls to stored procedures are audited. Any SQL statements issued inside stored procedures or functions are also audited.
- **Other database information** – Activity monitored includes the full SQL statement, the row count of affected rows from DML commands, accessed objects, and the unique database name. For Aurora PostgreSQL, database activity streams also monitor the bind variables and stored procedure parameters.

  **Important**
  The full SQL text of each statement is visible in the activity stream audit log, including any sensitive data. However, database user passwords are redacted if Aurora can determine them from the context, such as in the following SQL statement.

  ```sql
  ALTER ROLE role-name WITH password
  ```

- **Connection information** – Activity monitored includes session and network information, the server process ID, and exit codes.

If an activity stream has a failure while monitoring a DB instance, you are notified by using RDS events. If a failure occurs, you can shut down the DB instance or let it continue.

**Topics**

- Accessing an activity stream from Kinesis (p. 570)
- Audit log contents and examples (p. 571)
- Processing an activity stream using the AWS SDK (p. 585)

**Accessing an activity stream from Kinesis**

When you enable an activity stream for a DB cluster, a Kinesis stream is created for you. From Kinesis, you can monitor your database activity in real time. To further analyze database activity, you can connect your Kinesis stream to consumer applications. You can also connect it to compliance management applications.
To access an activity stream from Kinesis

2. Choose your activity stream from the list of Kinesis streams.

   An activity stream's name includes the prefix `aws-rds-das-` followed by the DB cluster's resource ID. The following is an example.

   ```
   aws-rds-das-cluster-NHVOV4PCLWHGF52NP
   ```

   To use the Amazon RDS console to find your DB cluster's resource ID, choose your DB cluster from the list of databases, and then choose the **Configuration** tab.

   To use the AWS CLI to find the full Kinesis stream name for an activity stream, use a `describe-db-clusters` CLI request and note the value of `ActivityStreamKinesisStreamName` in the response.
3. Choose **Monitoring** to begin observing the database activity.

For more information about using Amazon Kinesis, see [What is Amazon Kinesis Data Streams?](https://aws.amazon.com/kinesis/).

Audit log contents and examples

The database activity events that are monitored are represented in the Kinesis activity stream as JSON strings. The structure consists of a JSON object containing a `DatabaseActivityMonitoringRecord`, which in turn contains a `databaseActivityEventList` array of activity events.

**Topics**
- Examples of database activity streams audit log (p. 571)
- Database activity monitoring records JSON object (p. 577)
- `databaseActivityEvents` JSON object (p. 577)
- `databaseActivityEventList` JSON array (p. 579)

Examples of database activity streams audit log

Following are sample decrypted JSON audit logs of activity event records.

**Example Activity event record of an Aurora PostgreSQL CONNECT SQL statement**

Following is an activity event record of a logon with the use of a `CONNECT SQL statement` (`command`) by a `psql client` (`clientApplication`).

```json
{
  "type":"DatabaseActivityMonitoringRecords",
  "version":"1.1",
  "databaseActivityEvents":
  {
    "type":"DatabaseActivityMonitoringRecord",
    "clusterId":"cluster-4HNYSV4RRNKKYB71CFE5JBQQ",
    "instanceId":"db-FZTMYKQBUU26VLU7NW3ITCM",
    "databaseActivityEventList":
    {
      "startTime": "2019-10-30 00:39:49.940668+00",
      "logTime": "2019-10-30 00:39:49.990579+00",
      "statementId": 1,
      "substatementId": 1,
    }
  }
}
```
Monitoring activity streams

```
"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
}
```

Example Activity event record of an Aurora MySQL CONNECT SQL statement

Following is an activity event record of a logon with the use of a CONNECT SQL statement (command) by a 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,
            "serverHostname": "master",
            "serverName": "Amazon Aurora MySQL",
            "serverType": "MySQL",
            "serviceVersion": "MySQL 5.7.12",
            "startTime": "2020-05-22 18:07:13.267207+00",
            "endTime": "2020-05-22 18:07:13.267213+00",
        }
    ]
}
```
Example Activity event record of an Aurora PostgreSQL CREATE TABLE statement

Following is an example of a CREATE TABLE event for Aurora PostgreSQL.

```
{
    "type": "DatabaseActivityMonitoringRecords",
    "version": "1.1",
    "databaseActivityEvents": {
        "type": "DatabaseActivityMonitoringRecord",
        "clusterId": "cluster-4HNY5V4RRNPPKRYB71CFKE5JBBQ",
        "instanceId": "db-FZJTMYRCXQBUZ6VL07NW31ITCM",
        "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
            }
        ]
    }
}
```

Example Activity event record of an Aurora MySQL CREATE TABLE statement

Following is an example of a CREATE TABLE statement for Aurora MySQL. The operation is represented as two separate event records. One event has "class": "MAIN". The other event has "class": "AUX". The messages might arrive in any order. The logTime field of the MAIN event is always earlier than the logTime fields of any corresponding AUX events.

```
{
    "type": "DatabaseActivityMonitoringRecords",
    "version": "1.1",
    "databaseActivityEvents": {
        "type": "DatabaseActivityMonitoringRecord",
        "clusterId": "cluster-4HNY5V4RRNPPKRYB71CFKE5JBBQ",
        "instanceId": "db-FZJTMYRCXQBUZ6VL07NW31ITCM",
        "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
            }
        ]
    }
}
```
The following example shows the event with a class value of MAIN.

```
{
  "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"
    }
  ]
}
```

The following example shows the corresponding event with a class value of AUX.

```
{
  "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,
```

574
Example Activity event record of an Aurora PostgreSQL SELECT statement

Following is an example of a SELECT event.

```json
{
  "type": "DatabaseActivityMonitoringRecords",
  "version": "1.1",
  "databaseActivityEvents": {
    "type": "DatabaseActivityMonitoringRecord",
    "clusterId": "cluster-4HNY5V4RRP6K5BF4REX4EY71CPKKE5JBQQ",
    "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
      }
    ]
  }
}
```
Example Activity event record of an Aurora MySQL SELECT statement

Following is an example of a SELECT event.

The following example shows the event with a class value of MAIN.

```json
{
  "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":12830,
      "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"
  }
}
```

The following example shows the corresponding event with a class value of AUX.

```json
{
  "type":"DatabaseActivityMonitoringRecord",
  "clusterId":"cluster-some_id",
  "instanceId":"db-some_id",
  "databaseActivityEventList": [
    {
      "logTime":"2020-05-22 18:29:57.986399+00",
      "type":"record",
      "clientApplication":null,
      "pid":12830,
      "dbUserName":"master",
      "databaseName":"test",
      "remoteHost":"localhost",
      "remotePort":"11054",
      "command":"READ",
      "commandText":"test1",
      "paramList":null,
      "class":"AUX"
  }
}
```
Database activity monitoring records JSON object

The database activity event records are in a JSON object that contains the following information.

<table>
<thead>
<tr>
<th>JSON field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>string</td>
<td>The type of JSON record. The value is <code>DatabaseActivityMonitoringRecords</code>.</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>The version of the database activity monitoring records. The version of the generated database activity records depends on the engine version of the DB cluster.</td>
</tr>
<tr>
<td>databaseActivityEvents</td>
<td>string</td>
<td>A JSON object containing the activity events.</td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>An encryption key you use to decrypt the <code>databaseActivityEventList (p. 579)</code> databaseActivityEventList JSON array.</td>
</tr>
</tbody>
</table>

**databaseActivityEvents JSON object**

The `databaseActivityEvents` JSON object contains the following information.

**Top-level fields in JSON record**

Each event in the audit log is wrapped inside a record in JSON format. This record contains the following fields.
**type**

This field always has the value `DatabaseActivityMonitoringRecords`.

**version**

This field represents the version of the database activity stream data protocol or contract. It defines what fields are available. Version 1.0 represents the original data activity streams support for Aurora PostgreSQL versions 10.7 and 11.4. Version 1.1 represents the data activity streams support for Aurora PostgreSQL versions 10.10 and higher and Aurora PostgreSQL 11.5 and higher. Version 1.1 includes the additional fields `errorMessage` and `startTime`. Version 1.2 represents the data activity streams support for Aurora MySQL 2.08 and higher. Version 1.2 includes the additional fields `endTime` and `transactionId`.

**databaseActivityEvents**

An encrypted string representing one or more activity events. It’s represented as a base64 byte array. When you decrypt the string, the result is a record in JSON format with fields as shown in the examples in this section.

**key**

The encrypted data key used to encrypt the `databaseActivityEvents` string. This is the same AWS KMS customer master key (CMK) that you provided when you started the database activity stream.

The following example shows the format of this record.

```
{
  "type":"DatabaseActivityMonitoringRecords",
  "version":"1.1",
  "databaseActivityEvents":"encrypted audit records",
  "key":"encrypted key"
}
```

Take the following steps to decrypt the contents of the `databaseActivityEvents` field:

1. Decrypt the value in the `key` JSON field using the AWS KMS CMK you provided when starting database activity stream. Doing so returns the data encryption key in clear text.
2. Base64-decode the value in the `databaseActivityEvents` JSON field to obtain the ciphertext, in binary format, of the audit payload.
3. Decrypt the binary ciphertext with the data encryption key that you decoded in the first step.
4. Decompress the decrypted payload.
   - The encrypted payload is in the `databaseActivityEvents` field.
   - The `databaseActivityEventList` field contains an array of audit records. The `type` fields in the array can be `record` or `heartbeat`.

The audit log activity event record is a JSON object that contains the following information.

<table>
<thead>
<tr>
<th>JSON field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>string</td>
<td>The type of JSON record. The value is <code>DatabaseActivityMonitoringRecord</code>.</td>
</tr>
<tr>
<td>clusterId</td>
<td>string</td>
<td>The DB cluster resource identifier. It corresponds to the DB cluster attribute <code>DbClusterResourceId</code>.</td>
</tr>
</tbody>
</table>
databaseActivityEventList JSON array

The audit log payload is an encrypted `databaseActivityEventList` JSON array. The following table lists alphabetically the fields for each activity event in the decrypted `DatabaseActivityEventList` array of an audit log. The fields are different depending on whether you use Aurora PostgreSQL or Aurora MySQL. Consult the table that applies to your database engine.

**Important**
The event structure is subject to change. Aurora might add new fields to activity events in the future. In applications that parse the JSON data, make sure that your code can ignore or take appropriate actions for unknown field names.

### databaseActivityEventList fields for Aurora PostgreSQL

<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>class</strong></td>
<td>string</td>
<td>The class of activity event. Valid values for Aurora PostgreSQL are the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ALL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CONNECT – A connect or disconnect event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- DDL – A DDL statement that is not included in the list of statements for the ROLE class.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- FUNCTION – A function call or a DO block.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- MISC – A miscellaneous command such as DISCARD, FETCH, CHECKPOINT, or VACUUM.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- READ – A SELECT or COPY statement when the source is a relation or a query.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ROLE – A statement related to roles and privileges including GRANT, REVOKE, and CREATE/ALTER/DROP ROLE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- WRITE – An INSERT, UPDATE, DELETE, TRUNCATE, or COPY statement when the destination is a relation.</td>
</tr>
<tr>
<td><strong>clientApplication</strong></td>
<td>string</td>
<td>The application the client used to connect as reported by the client. The client doesn't have to provide this information, so the value can be null.</td>
</tr>
<tr>
<td><strong>command</strong></td>
<td>string</td>
<td>The name of the SQL command without any command details.</td>
</tr>
<tr>
<td><strong>commandText</strong></td>
<td>string</td>
<td>The actual SQL statement passed in by the user. For Aurora PostgreSQL, the value is identical to the original SQL statement. This field is used for all types of records except for connect or disconnect records, in which case the value is null. <strong>Important</strong> The full SQL text of each statement is visible in the activity stream audit log, including any sensitive data. However, database user passwords are redacted if</td>
</tr>
</tbody>
</table>
### Field | Data type | Description
---|---|---
| [Aurora can determine them from the context, such as in the following SQL statement.](#)
|ALTER ROLE role-name WITH password| | 

databaseName | string | The database to which the user connected. 

dbProtocol | string | The database protocol, for example `Postgres 3.0`. 

dbUserName | string | The database user with which the client authenticated. 

**errorMessage** 
*(version 1.1 database activity records only)*

| string | If there was any error, this field is populated with the error message that would've been generated by the DB server. The `errorMessage` value is null for normal statements that didn't result in an error. 

An error is defined as any activity that would produce a client-visible PostgreSQL error log event at a severity level of `ERROR` or greater. For more information, see [PostgreSQL message severity levels](#). For example, syntax errors and query cancellations generate an error message. 

Internal PostgreSQL server errors such as background checkpointer process errors do not generate an error message. However, records for such events are still emitted regardless of the setting of the log severity level. This prevents attackers from turning off logging to attempt avoiding detection. 

See also the `exitCode` field. |

exitCode | int | A value used for a session exit record. On a clean exit, this contains the exit code. An exit code can't always be obtained in some failure scenarios. Examples are if PostgreSQL does an `exit()` or if an operator performs a command such as `kill -9`. 

If there was any error, the `exitCode` field shows the SQL error code, `SQLSTATE`, as listed in [PostgreSQL error codes](#). 

See also the `errorMessage` field. |

logTime | string | A timestamp as recorded in the auditing code path. This represents the SQL statement execution end time. See also the `startTime` field. |

netProtocol | string | The network communication protocol. |

objectName | string | The name of the database object if the SQL statement is operating on one. This field is used only where the SQL statement operates on a database object. If the SQL statement is not operating on an object, this value is null. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>objectType</td>
<td>string</td>
<td>The database object type such as table, index, view, and so on. This field is used only where the SQL statement operates on a database object. If the SQL statement is not operating on an object, this value is null. Valid values include the following:</td>
</tr>
</tbody>
</table>
|                     |           | • COMPOSITE TYPE  
|                     |           | • FOREIGN TABLE  
|                     |           | • FUNCTION  
|                     |           | • INDEX  
|                     |           | • MATERIALIZED VIEW  
|                     |           | • SEQUENCE  
|                     |           | • TABLE  
|                     |           | • TOAST TABLE  
|                     |           | • VIEW  
|                     |           | • UNKNOWN  |
| paramList           | string    | An array of comma-separated parameters passed to the SQL statement. If the SQL statement has no parameters, this value is an empty array. |
| pid                 | int       | The process ID of the backend process that is allocated for serving the client connection.                                                 |
| remoteHost          | string    | Either the client IP address or hostname. For Aurora PostgreSQL, which one is used depends on the database's log_hostname parameter setting.   |
| remotePort          | string    | The client port number.                                                                                                                   |
| rowCount            | int       | The number of rows returned by the SQL statement. For example, if a SELECT statement returns 10 rows, rowCount is 10. For INSERT or UPDATE statements, rowCount is 0. |
| serverHost          | string    | The database server host IP address.                                                                                                         |
| serverType          | string    | The database server type, for example PostgreSQL.                                                                                             |
| serverVersion       | string    | The database server version, for example 2.3.1 for Aurora PostgreSQL.                                                                           |
| serviceName         | string    | The name of the service, for example Amazon Aurora PostgreSQL-Compatible edition.                                                           |
| sessionId           | int       | A pseudo-unique session identifier.                                                                                                           |
| startTime           | int       | The time when execution began for the SQL statement.                                                                                           |
|                     |           | (version 1.1 database activity records only)                                                                                                  |
|                     |           | To calculate the approximate execution time of the SQL statement, use logTime - startTime. See also the logTime field.                          |
| statementId         | int       | An identifier for the client's SQL statement. The counter is at the session level and increments with each SQL statement entered by the client. |
### Field | Data type | Description
--- | --- | ---
substatementId | int | An identifier for a SQL substatement. This value counts the contained substatements for each SQL statement identified by the `statementId` field.
type | string | The event type. Valid values are `record` or `heartbeat`.

**databaseActivityEventList fields for Aurora MySQL**

<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
</table>
class | string | The class of activity event. Valid values for Aurora MySQL are the following:
- **MAIN** – The primary event representing a SQL statement.
- **AUX** – A supplemental event containing additional details. For example, a statement that renames an object might have an event with class `AUX` that reflects the new name.

To find **MAIN** and **AUX** events corresponding to the same statement, check for different events that have the same values for the `pid` field and for the `statementId` field.

clientApplication | string | The application the client used to connect as reported by the client. The client doesn't have to provide this information, so the value can be null.

command | string | The general category of the SQL statement. The values for this field depend on the value of `class`.

The values when `class` is **MAIN** include the following:
- **CONNECT** – When a client session is connected.
- **QUERY** – A SQL statement. Accompanied by one or more events with a `class` value of **AUX**.
- **DISCONNECT** – When a client session is disconnected.
- **FAILED_CONNECT** – When a client attempts to connect but isn't able to.
- **CHANGEUSER** – A state change that's part of the MySQL network protocol, not from a statement that you issue.

The values when `class` is **AUX** include the following:
- **READ** – A `SELECT` or `COPY` statement when the source is a relation or a query.
- **WRITE** – An `INSERT`, `UPDATE`, `DELETE`, `TRUNCATE`, or `COPY` statement when the destination is a relation.
- **DROP** – Deleting an object.
- **CREATE** – Creating an object.
- **RENAME** – Renaming an object.
- **ALTER** – Changing the properties of an object.
<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commandText</td>
<td>string</td>
<td>For events with a class value of MAIN, this field represents the actual SQL statement passed in by the user. This field is used for all types of records except for connect or disconnect records, in which case the value is null. For events with a class value of AUX, this field contains supplemental information about the objects involved in the event. For Aurora MySQL, characters such as quotation marks are preceded by a backslash, representing an escape character. <strong>Important</strong> The full SQL text of each statement is visible in the audit log, including any sensitive data. However, database user passwords are redacted if Aurora can determine them from the context, such as in the following SQL statement.</td>
</tr>
<tr>
<td>databaseName</td>
<td>string</td>
<td>The database to which the user connected.</td>
</tr>
<tr>
<td>dbProtocol</td>
<td>string</td>
<td>The database protocol. Currently, this value is always MySQL for Aurora MySQL.</td>
</tr>
<tr>
<td>dbUserName</td>
<td>string</td>
<td>The database user with which the client authenticated.</td>
</tr>
<tr>
<td>endTime</td>
<td>string</td>
<td>The time when execution ended for the SQL statement. It is represented in Coordinated Universal Time (UTC) format. To calculate the execution time of the SQL statement, use endTime - startTime. See also the startTime field.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>string</td>
<td>If there was any error, this field is populated with the error message that would've been generated by the DB server. The errorMessage value is null for normal statements that didn't result in an error. An error is defined as any activity that would produce a client-visible MySQL error log event at a severity level of ERROR or greater. For more information, see The error log in the MySQL Reference Manual. For example, syntax errors and query cancellations generate an error message. Internal MySQL server errors such as background checkpoint process errors do not generate an error message. However, records for such events are still emitted regardless of the setting of the log severity level. This prevents attackers from turning off logging to attempt avoiding detection. See also the exitCode field.</td>
</tr>
<tr>
<td>startTime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Data type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exitCode</td>
<td>int</td>
<td>A value used for a session exit record. On a clean exit, this contains the exit code. An exit code can't always be obtained in some failure scenarios. In such cases, this value might be zero or might be blank.</td>
</tr>
<tr>
<td>logTime</td>
<td>string</td>
<td>A timestamp as recorded in the auditing code path. It is represented in Coordinated Universal Time (UTC) format. For the most accurate way to calculate statement duration, see the startTime and endTime fields.</td>
</tr>
<tr>
<td>netProtocol</td>
<td>string</td>
<td>The network communication protocol. Currently, this value is always TCP for Aurora MySQL.</td>
</tr>
<tr>
<td>objectName</td>
<td>string</td>
<td>The name of the database object if the SQL statement is operating on one. This field is used only where the SQL statement operates on a database object. If the SQL statement isn't operating on an object, this value is blank. To construct the fully qualified name of the object, combine databaseName and objectName. If the query involves multiple objects, this field can be a comma-separated list of names.</td>
</tr>
<tr>
<td>objectType</td>
<td>string</td>
<td>The database object type such as table, index, and so on. This field is used only where the SQL statement operates on a database object. If the SQL statement is not operating on an object, this value is null. Valid values for Aurora MySQL include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• INDEX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TABLE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UNKNOWN</td>
</tr>
<tr>
<td>paramList</td>
<td>string</td>
<td>This field isn't used for Aurora MySQL and is always null.</td>
</tr>
<tr>
<td>pid</td>
<td>int</td>
<td>The process ID of the backend process that is allocated for serving the client connection. When the database server is restarted, the pid changes and the counter for the statementId field starts over.</td>
</tr>
<tr>
<td>remoteHost</td>
<td>string</td>
<td>Either the IP address or hostname of the client that issued the SQL statement. For Aurora MySQL, which one is used depends on the database's skip_name_resolve parameter setting. The value localhost indicates activity from the rdsadmin special user.</td>
</tr>
<tr>
<td>remotePort</td>
<td>string</td>
<td>The client port number.</td>
</tr>
<tr>
<td>rowCount</td>
<td>int</td>
<td>The number of table rows affected or retrieved by the SQL statement. This field is used only for SQL statements that are data manipulation language (DML) statements. If the SQL statement is not a DML statement, this value is null.</td>
</tr>
<tr>
<td>serverHost</td>
<td>string</td>
<td>The database server instance identifier. This value is represented differently for Aurora MySQL than for Aurora PostgreSQL. Aurora PostgreSQL uses an IP address instead of an identifier.</td>
</tr>
<tr>
<td>serverType</td>
<td>string</td>
<td>The database server type, for example MySQL.</td>
</tr>
</tbody>
</table>
### Field Data type Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>serverVersion</td>
<td>string</td>
<td>The database server version. Currently, this value is always MySQL 5.7.12 for Aurora MySQL.</td>
</tr>
<tr>
<td>serviceName</td>
<td>string</td>
<td>The name of the service. Currently, this value is always Amazon Aurora MySQL for Aurora MySQL.</td>
</tr>
<tr>
<td>sessionId</td>
<td>int</td>
<td>A pseudo-unique session identifier.</td>
</tr>
<tr>
<td>startTime</td>
<td>string</td>
<td>The time when execution began for the SQL statement. It is represented in Coordinated Universal Time (UTC) format. To calculate the execution time of the SQL statement, use endTime - startTime. See also the endTime field.</td>
</tr>
<tr>
<td>statementId</td>
<td>int</td>
<td>An identifier for the client's SQL statement. The counter increments with each SQL statement entered by the client. The counter is reset when the DB instance is restarted.</td>
</tr>
<tr>
<td>substatementId</td>
<td>int</td>
<td>An identifier for a SQL substatement. This value is 1 for events with class MAIN and 2 for events with class AUX. Use the statementId field to identify all the events generated by the same statement.</td>
</tr>
<tr>
<td>transactionId</td>
<td>int</td>
<td>An identifier for a transaction.</td>
</tr>
<tr>
<td>type</td>
<td>string</td>
<td>The event type. Valid values are record or heartbeat.</td>
</tr>
</tbody>
</table>

### Processing an activity stream using the AWS SDK

You can programmatically process an activity stream by using the AWS SDK. The following are fully functioning Java and Python examples of how you might process the Kinesis data stream.

#### Java

```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;
```

---

585
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.interfaces.IRecordProcessorCheckpointer;
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 {
    checkpoint.checkpoint();
    break;
} catch (ShutdownException se) {
    // Ignore checkpoint if the processor instance has been shutdown
    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);
} catch (Exception e) {
    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.REQUIRE_ENCRYPT_ALLOW_DECRYPT)

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.DefaultCryptoMaterialsManager(master_key_provider=my_key_provider))
        return decrypted_plaintext
Managing access to database activity streams

Any user with appropriate AWS Identity and Access Management (IAM) role privileges for database activity streams can create, start, stop, and modify the activity stream settings for a DB cluster. These actions are included in the audit log of the stream. For best compliance practices, we recommend that you don't provide these privileges to DBAs.

You set access to database activity streams using IAM policies. For more information about Aurora authentication, see Identity and access management in Amazon Aurora (p. 1222). For more information about creating IAM policies, see Creating and using an IAM policy for IAM database access (p. 1241).

Example Policy to allow configuring database activity streams

To give users fine-grained access to modify activity streams, use the service-specific operation context keys rds:StartActivityStream and rds:StopActivityStream in an IAM policy. The following IAM policy example allows a user or role to configure activity streams.

```json
{
    "Version":"2012-10-17",
    "Statement":[
        
```
Example Policy to allow starting database activity streams

The following IAM policy example allows a user or role to start activity streams.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowStartActivityStreams",
            "Effect": "Allow",
            "Action": "rds:StartActivityStream",
            "Resource": "*"
        }
    ]
}
```

Example Policy to allow stopping database activity streams

The following IAM policy example allows a user or role to stop activity streams.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowStopActivityStreams",
            "Effect": "Allow",
            "Action": "rds:StopActivityStream",
            "Resource": "*"
        }
    ]
}
```

Example Policy to deny starting database activity streams

The following IAM policy example prevents a user or role from starting activity streams.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyStartActivityStreams",
            "Effect": "Deny",
            "Action": "rds:StartActivityStream",
            "Resource": "*"
        }
    ]
}
```
Example Policy to deny stopping database activity streams

The following IAM policy example prevents a user or role from stopping activity streams.

```json
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyStopActivityStreams",
         "Effect":"Deny",
         "Action":"rds:StopActivityStream",
         "Resource":"*"
      }
   ]
}
```
Using Amazon RDS event notification

Topics
- Amazon RDS event categories and event messages (p. 595)
- Subscribing to Amazon RDS event notification (p. 602)
- Listing Amazon RDS event notification subscriptions (p. 604)
- Modifying an Amazon RDS event notification subscription (p. 606)
- Adding a source identifier to an Amazon RDS event notification subscription (p. 608)
- Removing a source identifier from an Amazon RDS event notification subscription (p. 609)
- Listing the Amazon RDS event notification categories (p. 610)
- Deleting an Amazon RDS event notification subscription (p. 611)

Amazon RDS uses the Amazon Simple Notification Service (Amazon SNS) to provide notification when an Amazon RDS event occurs. These notifications can be in any notification form supported by Amazon SNS for an AWS Region, such as an email, a text message, or a call to an HTTP endpoint.

Amazon RDS groups these events into categories that you can subscribe to so that you can be notified when an event in that category occurs. You can subscribe to an event category for a DB instance, DB cluster, DB cluster snapshot, DB parameter group, or DB security group. For example, if you subscribe to the Backup category for a given DB instance, you are notified whenever a backup-related event occurs that affects the DB instance. If you subscribe to a configuration change category for a DB security group, you are notified when the DB security group is changed. You also receive notification when an event notification subscription changes.

For Amazon Aurora, events occur at both the DB cluster and the DB instance level, so you can receive events if you subscribe to an Aurora DB cluster or an Aurora DB instance.

Event notifications are sent to the addresses that you provide when you create the subscription. You might want to create several different subscriptions, such as one subscription receiving all event notifications and another subscription that includes only critical events for your production DB instances. You can easily turn off notification without deleting a subscription by choosing No for Enabled in the Amazon RDS console or by setting the Enabled parameter to false using the AWS CLI or Amazon RDS API.

**Important**
Amazon RDS doesn't guarantee the order of events sent in an event stream. The event order is subject to change.

**Note**
For more information on using text messages with SNS, see Mobile text messaging (SMS) in the Amazon Simple Notification Service Developer Guide.

Amazon RDS uses the ARN of an Amazon SNS topic to identify each subscription. The Amazon RDS console creates the ARN for you when you create the subscription. If you use the CLI or API, you create the ARN by using the Amazon SNS console or the Amazon SNS API when you create a subscription.

Billing for Amazon RDS event notification is through the Amazon Simple Notification Service (Amazon SNS). Amazon SNS fees apply when using event notification. For more information on Amazon SNS billing, see Amazon Simple Notification Service pricing.

The process for subscribing to Amazon RDS event notification is as follows:

1. Create an Amazon RDS event notification subscription by using the Amazon RDS console, AWS CLI, or API.
2. Amazon RDS sends an approval email or SMS message to the addresses you submitted with your subscription. To confirm your subscription, choose the link in the notification you were sent.
3. When you have confirmed the subscription, the status of your subscription is updated in the Amazon RDS console’s **My Event Subscriptions** section.
4. You then begin to receive event notifications.

**Note**

When Amazon SNS sends a notification to a subscribed HTTP or HTTPS endpoint, the POST message sent to the endpoint has a message body that contains a JSON document. For more information, see [Amazon SNS message and JSON formats](https://docs.aws.amazon.com/AmazonSNS/latest/dg/sms-messaging.html) in the Amazon Simple Notification Service Developer Guide.

You can use AWS Lambda to process event notifications from a DB instance. For more information, see [Using AWS Lambda with Amazon RDS](https://docs.aws.amazon.com/lambda/latest/dg/lambda-rds.html) in the AWS Lambda Developer Guide.

The following section lists all categories and events that you can be notified of. It also provides information about subscribing to and working with Amazon RDS event subscriptions.

### Amazon RDS event categories and event messages

Amazon RDS generates a significant number of events in categories that you can subscribe to using the Amazon RDS Console, AWS CLI, or the API. Each category applies to a source type, which can be a DB instance, DB snapshot, DB security group, or DB parameter group.

The following table shows the event category and a list of events when a DB instance is the source type.

<table>
<thead>
<tr>
<th>Category</th>
<th>Amazon RDS event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>availability</td>
<td>RDS-EVENT-0006</td>
<td>The DB instance restarted.</td>
</tr>
<tr>
<td>availability</td>
<td>RDS-EVENT-0004</td>
<td>DB instance shutdown.</td>
</tr>
<tr>
<td>availability</td>
<td>RDS-EVENT-0022</td>
<td>An error has occurred while restarting MySQL or MariaDB.</td>
</tr>
<tr>
<td>backtrack</td>
<td>RDS-EVENT-0131</td>
<td>The actual Backtrack window is smaller than the target Backtrack window you specified. Consider reducing the number of hours in your target Backtrack window. For more information about backtracking, see Backtracking an Aurora DB cluster (p. 677).</td>
</tr>
<tr>
<td>backtrack</td>
<td>RDS-EVENT-0132</td>
<td>The actual Backtrack window is the same as the target Backtrack window.</td>
</tr>
<tr>
<td>backup</td>
<td>RDS-EVENT-0001</td>
<td>Backing up DB instance.</td>
</tr>
<tr>
<td>backup</td>
<td>RDS-EVENT-0002</td>
<td>Finished DB Instance backup.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0009</td>
<td>The DB instance has been added to a security group.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0024</td>
<td>The DB instance is being converted to a Multi-AZ DB instance.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0030</td>
<td>The DB instance is being converted to a Single-AZ DB instance.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0012</td>
<td>Applying modification to database instance class.</td>
</tr>
<tr>
<td>Category</td>
<td>Amazon RDS event ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0018</td>
<td>The current storage settings for this DB instance are being changed.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0011</td>
<td>A parameter group for this DB instance has changed.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0092</td>
<td>A parameter group for this DB instance has finished updating.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0028</td>
<td>Automatic backups for this DB instance have been disabled.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0032</td>
<td>Automatic backups for this DB instance have been enabled.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0033</td>
<td>There are [count] users that match the master user name. Users not tied to a specific host have been reset.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0025</td>
<td>The DB instance has been converted to a Multi-AZ DB instance.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0029</td>
<td>The DB instance has been converted to a Single-AZ DB instance.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0014</td>
<td>The DB instance class for this DB instance has changed.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0017</td>
<td>The storage settings for this DB instance have changed.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0010</td>
<td>The DB instance has been removed from a security group.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0016</td>
<td>The master password for the DB instance has been reset.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0067</td>
<td>An attempt to reset the master password for the DB instance has failed.</td>
</tr>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0078</td>
<td>The Enhanced Monitoring configuration has been changed.</td>
</tr>
<tr>
<td>creation</td>
<td>RDS-EVENT-0005</td>
<td>DB instance created.</td>
</tr>
<tr>
<td>deletion</td>
<td>RDS-EVENT-0003</td>
<td>The DB instance has been deleted.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0034</td>
<td>Amazon RDS is not attempting a requested failover because a failover recently occurred on the DB instance.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0013</td>
<td>A Multi-AZ failover that resulted in the promotion of a standby instance has started.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0015</td>
<td>A Multi-AZ failover that resulted in the promotion of a standby instance is complete. It may take several minutes for the DNS to transfer to the new primary DB instance.</td>
</tr>
<tr>
<td>Category</td>
<td>Amazon RDS event ID</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0065</td>
<td>The instance has recovered from a partial failover.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0049</td>
<td>A Multi-AZ failover has completed.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0050</td>
<td>A Multi-AZ activation has started after a successful instance recovery.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0051</td>
<td>A Multi-AZ activation is complete. Your database should be accessible now.</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0031</td>
<td>The DB instance has failed due to an incompatible configuration or an underlying storage issue. Begin a point-in-time-restore for the DB instance.</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0036</td>
<td>The DB instance is in an incompatible network. Some of the specified subnet IDs are invalid or do not exist.</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0035</td>
<td>The DB instance has invalid parameters. For example, if the DB instance could not start because a memory-related parameter is set too high for this instance class, the customer action would be to modify the memory parameter and reboot the DB instance.</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0058</td>
<td>Error while creating Statspack user account PERFSTAT. Please drop the account before adding the Statspack option.</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0079</td>
<td>Enhanced Monitoring cannot be enabled without the enhanced monitoring IAM role. For information on creating the enhanced monitoring IAM role, see To create an IAM role for Amazon RDS enhanced monitoring (p. 505).</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0080</td>
<td>Enhanced Monitoring was disabled due to an error making the configuration change. It is likely that the enhanced monitoring IAM role is configured incorrectly. For information on creating the enhanced monitoring IAM role, see To create an IAM role for Amazon RDS enhanced monitoring (p. 505).</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0082</td>
<td>Aurora was unable to copy backup data from an Amazon S3 bucket. It is likely that the permissions for Aurora to access the Amazon S3 bucket are configured incorrectly. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).</td>
</tr>
<tr>
<td>low storage</td>
<td>RDS-EVENT-0089</td>
<td>The DB instance has consumed more than 90% of its allocated storage. You can monitor the storage space for a DB instance using the Free Storage Space metric. For more information, see Viewing DB instance metrics (p. 470).</td>
</tr>
<tr>
<td>Category</td>
<td>Amazon RDS event ID</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>low storage</td>
<td>RDS-EVENT-0007</td>
<td>The allocated storage for the DB instance has been exhausted. To resolve this issue, you should allocate additional storage for the DB instance. For more information, see the RDS FAQ. You can monitor the storage space for a DB instance using the Free Storage Space metric. For more information, see Viewing DB instance metrics (p. 470).</td>
</tr>
<tr>
<td>maintenance</td>
<td>RDS-EVENT-0026</td>
<td>Offline maintenance of the DB instance is taking place. The DB instance is currently unavailable.</td>
</tr>
<tr>
<td>maintenance</td>
<td>RDS-EVENT-0027</td>
<td>Offline maintenance of the DB instance is complete. The DB instance is now available.</td>
</tr>
<tr>
<td>maintenance</td>
<td>RDS-EVENT-0047</td>
<td>Patching of the DB instance has completed.</td>
</tr>
<tr>
<td>maintenance</td>
<td>RDS-EVENT-0155</td>
<td>The DB instance has a DB engine minor version upgrade available.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0044</td>
<td>Operator-issued notification. For more information, see the event message.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0048</td>
<td>Patching of the DB instance has been delayed.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0054</td>
<td>The MySQL storage engine you are using is not InnoDB, which is the recommended MySQL storage engine for Amazon RDS. For information about MySQL storage engines, see Supported storage engines for MySQL on Amazon RDS.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0055</td>
<td>The number of tables you have for your DB instance exceeds the recommended best practices for Amazon RDS. Please reduce the number of tables on your DB instance. For information about recommended best practices, see Best practices with Amazon Aurora (p. 1191).</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0056</td>
<td>The number of databases you have for your DB instance exceeds the recommended best practices for Amazon RDS. Please reduce the number of databases on your DB instance. For information about recommended best practices, see Best practices with Amazon Aurora (p. 1191).</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0087</td>
<td>The DB instance has been stopped.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0088</td>
<td>The DB instance has been started.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0154</td>
<td>The DB instance is being started due to it exceeding the maximum allowed time being stopped.</td>
</tr>
<tr>
<td>Category</td>
<td>Amazon RDS event ID</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| notification | RDS-EVENT-0157       | RDS can't modify the DB instance class because the target instance class can't support the number of databases that exist on the source DB instance. The error message appears as: “The instance has N databases, but after conversion it would only support N”.

notification | RDS-EVENT-0158       | DB instance is in a state that can't be upgraded.                                                                                                                                                     |

read replica | RDS-EVENT-0045       | An error has occurred in the read replication process. For more information, see the event message. For information on troubleshooting read replica errors, see Troubleshooting a MySQL read replica problem. |

read replica | RDS-EVENT-0046       | The read replica has resumed replication. This message appears when you first create a read replica, or as a monitoring message confirming that replication is functioning properly. If this message follows an RDS-EVENT-0045 notification, then replication has resumed following an error or after replication was stopped. |

read replica | RDS-EVENT-0057       | Replication on the read replica was terminated.                                                                                                                                                       |

read replica | RDS-EVENT-0062       | Replication on the read replica was manually stopped.                                                                                                                                                  |

read replica | RDS-EVENT-0063       | Replication on the read replica was reset.                                                                                                                                                            |

recovery    | RDS-EVENT-0020       | Recovery of the DB instance has started. Recovery time will vary with the amount of data to be recovered.                                                                                              |

recovery    | RDS-EVENT-0021       | Recovery of the DB instance is complete.                                                                                                                                                              |

recovery    | RDS-EVENT-0023       | A manual backup has been requested but Amazon RDS is currently in the process of creating a DB snapshot. Submit the request again after Amazon RDS has completed the DB snapshot.           |

recovery    | RDS-EVENT-0052       | Recovery of the Multi-AZ instance has started. Recovery time will vary with the amount of data to be recovered.                                                                                     |

recovery    | RDS-EVENT-0053       | Recovery of the Multi-AZ instance is complete.                                                                                                                                                        |

restoration | RDS-EVENT-0008       | The DB instance has been restored from a DB snapshot.                                                                                                                                                    |

restoration | RDS-EVENT-0019       | The DB instance has been restored from a point-in-time backup.                                                                                                                                          |

The following table shows the event category and a list of events when a DB parameter group is the source type.
The following table shows the event category and a list of events when a DB security group is the source type.

<table>
<thead>
<tr>
<th>Category</th>
<th>RDS event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration change</td>
<td>RDS-EVENT-0038</td>
<td>The security group has been modified.</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0039</td>
<td>The security group owned by [user] does not exist; authorization for the security group has been revoked.</td>
</tr>
</tbody>
</table>

The following table shows the event category and a list of events when an Aurora DB cluster is the source type.

<table>
<thead>
<tr>
<th>Category</th>
<th>RDS event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>failover</td>
<td>RDS-EVENT-0069</td>
<td>A failover for the DB cluster has failed.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0070</td>
<td>A failover for the DB cluster has restarted.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0071</td>
<td>A failover for the DB cluster has finished.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0072</td>
<td>A failover for the DB cluster has begun within the same Availability Zone.</td>
</tr>
<tr>
<td>failover</td>
<td>RDS-EVENT-0073</td>
<td>A failover for the DB cluster has begun across Availability Zones.</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0083</td>
<td>Aurora was unable to copy backup data from an Amazon S3 bucket. It is likely that the permissions for Aurora to access the Amazon S3 bucket are configured incorrectly. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).</td>
</tr>
<tr>
<td>failure</td>
<td>RDS-EVENT-0143</td>
<td>Scaling failed for the Aurora Serverless DB cluster.</td>
</tr>
<tr>
<td>maintenance</td>
<td>RDS-EVENT-0156</td>
<td>The DB cluster has a DB engine minor version upgrade available.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0076</td>
<td>Migration to an Aurora DB cluster failed.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0077</td>
<td>An attempt to convert a table from the source database to InnoDB failed during the migration to an Aurora DB cluster.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0141</td>
<td>Scaling initiated for the Aurora Serverless DB cluster.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0142</td>
<td>Scaling completed for the Aurora Serverless DB cluster.</td>
</tr>
</tbody>
</table>
### Amazon RDS event categories and event messages

<table>
<thead>
<tr>
<th>Category</th>
<th>RDS event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notification</td>
<td>RDS-EVENT-0144</td>
<td>Automatic pause initiated for the Aurora Serverless DB cluster.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0145</td>
<td>The Aurora Serverless DB cluster paused.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0146</td>
<td>Pause cancelled for the Aurora Serverless DB cluster.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0147</td>
<td>Resume initiated for the Aurora Serverless DB cluster.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0148</td>
<td>Resume completed for the Aurora Serverless DB cluster.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0149</td>
<td>Seamless scaling completed with the force option for the Aurora Serverless DB cluster. Connections might have been interrupted as required.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0150</td>
<td>The DB cluster stopped.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0151</td>
<td>The DB cluster started.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0152</td>
<td>The DB cluster stop failed.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0153</td>
<td>The DB cluster is being started due to it exceeding the maximum allowed time being stopped.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0173</td>
<td>Patching of the DB cluster has completed.</td>
</tr>
</tbody>
</table>

The following table shows the event category and a list of events when an Aurora DB cluster snapshot is the source type.

<table>
<thead>
<tr>
<th>Category</th>
<th>RDS event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>RDS-EVENT-0074</td>
<td>Creation of a manual DB cluster snapshot has started.</td>
</tr>
<tr>
<td>backup</td>
<td>RDS-EVENT-0075</td>
<td>A manual DB cluster snapshot has been created.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0162</td>
<td>DB cluster snapshot export task failed.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0163</td>
<td>DB cluster snapshot export task canceled.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0164</td>
<td>DB cluster snapshot export task completed.</td>
</tr>
<tr>
<td>backup</td>
<td>RDS-EVENT-0168</td>
<td>Creating automated cluster snapshot.</td>
</tr>
<tr>
<td>backup</td>
<td>RDS-EVENT-0169</td>
<td>Automated cluster snapshot created.</td>
</tr>
<tr>
<td>creation</td>
<td>RDS-EVENT-0170</td>
<td>DB cluster created.</td>
</tr>
<tr>
<td>deletion</td>
<td>RDS-EVENT-0171</td>
<td>DB cluster deleted.</td>
</tr>
<tr>
<td>notification</td>
<td>RDS-EVENT-0172</td>
<td>Renamed DB cluster from [old DB cluster name] to [new DB cluster name].</td>
</tr>
</tbody>
</table>
Subscribing to Amazon RDS event notification

You can create an Amazon RDS event notification subscription so you can be notified when an event occurs for a given DB instance, DB snapshot, DB security group, or DB parameter group. The simplest way to create a subscription is with the RDS console. If you choose to create event notification subscriptions using the CLI or API, you must create an Amazon Simple Notification Service topic and subscribe to that topic with the Amazon SNS console or Amazon SNS API. You will also need to retain the Amazon Resource Name (ARN) of the topic because it is used when submitting CLI commands or API operations. For information on creating an SNS topic and subscribing to it, see Getting started with Amazon SNS in the Amazon Simple Notification Service Developer Guide.

You can specify the type of source you want to be notified of and the Amazon RDS source that triggers the event. These are defined by the **SourceType** (type of source) and the **SourceIdentifier** (the Amazon RDS source generating the event). If you specify both the **SourceType** and **SourceIdentifier**, such as `SourceType = db-instance` and `SourceIdentifier = myDBInstance1`, you receive all the DB instance events for the specified source. If you specify a **SourceType** but don't specify a **SourceIdentifier**, you receive notice of the events for that source type for all your Amazon RDS sources. If you don't specify either the **SourceType** or the **SourceIdentifier**, you are notified of events generated from all Amazon RDS sources belonging to your customer account.

**Note**

Event notifications might take up to five minutes to be delivered.
Amazon RDS event notification is only available for unencrypted SNS topics. If you specify an encrypted SNS topic, event notifications aren’t sent for the topic.

**Console**

**To subscribe to RDS event notification**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In navigation pane, choose **Event subscriptions**.
3. In the **Event subscriptions** pane, choose **Create event subscription**.
4. In the **Create event subscription** dialog box, do the following:
   a. For **Name**, enter a name for the event notification subscription.
   b. For **Send notifications to**, choose an existing Amazon SNS ARN for an Amazon SNS topic, or choose **create topic** to enter the name of a topic and a list of recipients.
   c. For **Source type**, choose a source type.
   d. Choose **Yes** to enable the subscription. If you want to create the subscription but to not have notifications sent yet, choose **No**.
   e. Depending on the source type you selected, choose the event categories and sources that you want to receive event notifications for.
   f. Choose **Create**.

The Amazon RDS console indicates that the subscription is being created.
AWS CLI

To subscribe to RDS event notification, use the AWS CLI `create-event-subscription` command. Include the following required parameters:

- `--subscription-name`
- `--sns-topic-arn`

**Example**

For Linux, macOS, or Unix:

```
aws rds create-event-subscription \
  --subscription-name myeventsubscription \
  --sns-topic-arn arn:aws:sns:us-east-1:802#########:myawsuser-RDS \
  --enabled
```

For Windows:

```
aws rds create-event-subscription ^
  --subscription-name myeventsubscription ^
  --sns-topic-arn arn:aws:sns:us-east-1:802#########:myawsuser-RDS ^
  --enabled
```

API

To subscribe to Amazon RDS event notification, call the Amazon RDS API function `CreateEventSubscription`. Include the following required parameters:

- `SubscriptionName`
- `SnsTopicArn`
Listing Amazon RDS event notification subscriptions

You can list your current Amazon RDS event notification subscriptions.

**Console**

**To list your current Amazon RDS event notification subscriptions**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Event subscriptions**. The **Event subscriptions** pane shows all your event notification subscriptions.

**AWS CLI**

To list your current Amazon RDS event notification subscriptions, use the AWS CLI `describe-event-subscriptions` command.

**Example**

The following example describes all event subscriptions.

```
aws rds describe-event-subscriptions
```

The following example describes the `myfirsteventsubscription`.

```
aws rds describe-event-subscriptions --subscription-name myfirsteventsubscription
```

**API**

To list your current Amazon RDS event notification subscriptions, call the Amazon RDS API **DescribeEventSubscriptions** action.

**Example**

The following code example lists up to 100 event subscriptions.

```
https://rds.us-east-1.amazonaws.com/
?Action=DescribeEventSubscriptions
&MaxRecords=100
```
The following example describes the `myfirsteventsubscription`.

```plaintext
https://rds.us-east-1.amazonaws.com/
?Action=DescribeEventSubscriptions
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&SubscriptionName=myfirsteventsubscription
&Version=2014-10-31
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140428/us-east-1/rds/aws4_request
&X-Amz-Date=20140428T161907Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=4208679fe967783a1a149c826199080a066085d5a88227a80c6c0cadb3e8c0d4
```
Modifying an Amazon RDS event notification subscription

After you have created a subscription, you can change the subscription name, source identifier, categories, or topic ARN.

Console

To modify an Amazon RDS event notification subscription

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Event subscriptions.
3. In the Event subscriptions pane, choose the subscription that you want to modify and choose Edit.
4. Make your changes to the subscription in either the Target or Source section.
5. Choose Edit. The Amazon RDS console indicates that the subscription is being modified.

AWS CLI

To modify an Amazon RDS event notification subscription, use the AWS CLI modify-event-subscription command. Include the following required parameter:

• --subscription-name

Example

The following code enables myeventsubscription.

For Linux, macOS, or Unix:

```bash
aws rds modify-event-subscription \
    --subscription-name myeventsubscription \
    --enabled
```

For Windows:

```bash
aws rds modify-event-subscription ^
    --subscription-name myeventsubscription ^
    --enabled
```

API

To modify an Amazon RDS event, call the Amazon RDS API operation ModifyEventSubscription. Include the following required parameter:
• SubscriptionName
Adding a source identifier to an Amazon RDS event notification subscription

You can add a source identifier (the Amazon RDS source generating the event) to an existing subscription.

Console

You can easily add or remove source identifiers using the Amazon RDS console by selecting or deselecting them when modifying a subscription. For more information, see Modifying an Amazon RDS event notification subscription (p. 606).

AWS CLI

To add a source identifier to an Amazon RDS event notification subscription, use the AWS CLI add-source-identifier-to-subscription command. Include the following required parameters:

- --subscription-name
- --source-identifier

Example

The following example adds the source identifier mysqldb to the myrdeventsubscription subscription.

For Linux, macOS, or Unix:

```
aws rds add-source-identifier-to-subscription \
  --subscription-name myrdeventsubscription \
  --source-identifier mysqldb
```

For Windows:

```
aws rds add-source-identifier-to-subscription ^
  --subscription-name myrdeventsubscription ^
  --source-identifier mysqldb
```

API

To add a source identifier to an Amazon RDS event notification subscription, call the Amazon RDS API AddSourceIdentifierToSubscription. Include the following required parameters:

- SubscriptionName
- SourceIdentifier
Removing a source identifier from an Amazon RDS event notification subscription

You can remove a source identifier (the Amazon RDS source generating the event) from a subscription if you no longer want to be notified of events for that source.

Console

You can easily add or remove source identifiers using the Amazon RDS console by selecting or deselecting them when modifying a subscription. For more information, see Modifying an Amazon RDS event notification subscription (p. 606).

AWS CLI

To remove a source identifier from an Amazon RDS event notification subscription, use the AWS CLI remove-source-identifier-from-subscription command. Include the following required parameters:

- --subscription-name
- --source-identifier

Example

The following example removes the source identifier mysql from the myrsdeventsubscription subscription.

For Linux, macOS, or Unix:

```
aws rds remove-source-identifier-from-subscription \
    --subscription-name myrsdeventsubscription \
    --source-identifier mysql
```

For Windows:

```
aws rds remove-source-identifier-from-subscription ^
    --subscription-name myrsdeventsubscription ^
    --source-identifier mysql
```

API

To remove a source identifier from an Amazon RDS event notification subscription, use the Amazon RDS API `RemoveSourceIdentifierFromSubscription` command. Include the following required parameters:

- SubscriptionName
- SourceIdentifier
Listing the Amazon RDS event notification categories

All events for a resource type are grouped into categories. To view the list of categories available, use the following procedures.

Console

When you create or modify an event notification subscription, the event categories are displayed in the Amazon RDS console. For more information, see Modifying an Amazon RDS event notification subscription (p. 606).

AWS CLI

To list the Amazon RDS event notification categories, use the AWS CLI describe-event-categories command. This command has no required parameters.

Example

```
aws rds describe-event-categories
```

API

To list the Amazon RDS event notification categories, use the Amazon RDS API DescribeEventCategories command. This command has no required parameters.
Deleting an Amazon RDS event notification subscription

You can delete a subscription when you no longer need it. All subscribers to the topic will no longer receive event notifications specified by the subscription.

Console

To delete an Amazon RDS event notification subscription

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose DB Event Subscriptions.
3. In the My DB Event Subscriptions pane, choose the subscription that you want to delete.
4. Choose Delete.
5. The Amazon RDS console indicates that the subscription is being deleted.

AWS CLI

To delete an Amazon RDS event notification subscription, use the AWS CLI delete-event-subscription command. Include the following required parameter:

- --subscription-name

Example

The following example deletes the subscription myrdssubscription.

```
aws rds delete-event-subscription --subscription-name myrdssubscription
```

API

To delete an Amazon RDS event notification subscription, use the RDS API DeleteEventSubscription command. Include the following required parameter:

- SubscriptionName
Viewing Amazon RDS events

Amazon RDS keeps a record of events that relate to your DB instances, DB snapshots, DB security groups, and DB parameter groups. This information includes the date and time of the event, the source name and source type of the event, and a message associated with the event.

You can retrieve events for your RDS resources through the AWS Management Console, which shows events from the past 24 hours. You can also retrieve events for your RDS resources by using the `describe-events` AWS CLI command, or the `DescribeEvents` RDS API operation. If you use the AWS CLI or the RDS API to view events, you can retrieve events for up to the past 14 days.

**Note**

If you need to store events for longer periods of time, you can send Amazon RDS events to CloudWatch Events. For more information, see Getting CloudWatch Events and Amazon EventBridge events for Amazon Aurora (p. 614)

**Console**

**To view all Amazon RDS instance events for the past 24 hours**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Events**. The available events appear in a list.
3. Use the **Filter** list to filter the events by type, and use the text box to the right of the **Filter** list to further filter your results. For example, the following screenshot shows a list of events filtered by the DB instance event type and containing the characters **1318**.

![Events Filter](image)

**AWS CLI**

**To view all Amazon RDS instance events for the past 7 days**

You can view all Amazon RDS instance events for the past 7 days by calling the `describe-events` AWS CLI command and setting the `--duration` parameter to **10080**.

```
aws rds describe-events --duration 10080
```

**API**

**To view all Amazon RDS instance events for the past 14 days**

You can view all Amazon RDS instance events for the past 14 days by calling the `DescribeEvents` RDS API operation and setting the `Duration` parameter to **20160**.

---

612
https://rds.us-west-2.amazonaws.com/
    ?Action=DescribeEvents
    &Duration=20160
    &MaxRecords=100
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20140421/us-west-2/rds/aws4_request
    &X-Amz-Date=20140421T194733Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=8e313cabcdbd9766c56a2886b5b298fd944e0b7cfa248953c82705fdd0374f27
Getting CloudWatch Events and Amazon EventBridge events for Amazon Aurora

Amazon CloudWatch Events and Amazon EventBridge both enable you to automate AWS services and respond to system events such as application availability issues or resource changes. Events from AWS services are delivered to CloudWatch Events and EventBridge nearly in real time. You can write simple rules to indicate which events interest you and what automated actions to take when an event matches a rule.

You can set a variety of targets—such as an AWS Lambda function or an Amazon SNS topic—which receive events in JSON format. For more information, see the Amazon CloudWatch Events User Guide and the Amazon EventBridge User Guide.

For example, you can configure Amazon Aurora to send events to CloudWatch Events or Amazon EventBridge whenever a DB instance is created or deleted.

Topics

- Sending Amazon RDS events to CloudWatch Events (p. 614)
- DB cluster events (p. 615)
- DB instance events (p. 615)
- DB parameter group events (p. 616)
- DB security group events (p. 616)
- DB cluster snapshot events (p. 617)
- DB snapshot events (p. 617)

Sending Amazon RDS events to CloudWatch Events

You can create CloudWatch Events rules to send Amazon RDS events to CloudWatch Events.

Use the following steps to create a CloudWatch Events rule that triggers on an event emitted by an AWS service.

To create a rule that triggers on an event:

2. Under Events in the navigation pane, choose Rules.
3. Choose Create rule.
4. For Event Source, do the following:
   a. Choose Event Pattern.
   b. For Service Name, choose Relational Database Service (RDS).
   c. For Event Type, choose the type of Amazon RDS resource that triggers the event. For example, if a DB instance triggers the event, choose RDS DB Instance Event.
5. For Targets, choose Add Target, then choose the CloudWatch log group.
6. For Log Group, enter a name for the log group to store the events.
7. Choose Configure details. For Rule definition, type a name and description for the rule.
8. Choose Create rule.
DB cluster events

The following is an example of a DB cluster event.

```
{
  "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",
    "SourceIdentifier": "rds:my-db-cluster",
    "Message": "Database cluster has been patched"
  }
}
```

DB instance events

The following is an example of a DB instance event.

```
{
  "version": "0",
  "id": "68f6e973-1a0c-d37b-f2f2-94a7f62ff4e",
  "detail-type": "RDS DB Instance 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:my-db-instance"
  }],
  "detail": {
    "EventCategories": ["failover"],
    "SourceType": "DB_INSTANCE",
    "Date": "2018-09-27T22:36:43.882Z",
    "SourceIdentifier": "rds:my-db-instance",
    "Message": "A Multi-AZ failover has completed."
  }
}
```
DB parameter group events

The following is an example of a DB parameter group event.

```
{
    "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",
        "Date": "2018-10-06T12:26:13.882Z",
        "SourceIdentifier": "rds:my-db-param-group",
        "Message": "Updated parameter time_zone to UTC with apply method immediate"
    }
}
```

DB security group events

The following is an example of a DB security group event.

```
{
    "version": "0",
    "id": "844e2571-85d4-695f-b930-0153b71dcb42",
    "detail-type": "RDS DB Security Group Event",
    "source": "aws.rds",
    "account": "123456789012",
    "time": "2018-10-06T12:26:13Z",
    "region": "us-east-1",
    "resources": [
    ],
    "detail": {
        "EventCategories": ["configuration change"],
        "SourceType": "SECURITY_GROUP",
        "Date": "2018-10-06T12:26:13.882Z",
        "SourceIdentifier": "rds:my-security-group",
        "Message": "Applied change to security group"
    }
}
```
DB cluster snapshot events

The following is an example of a DB cluster snapshot event.

```
{
  "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": [
  ],
  "detail": {
    "EventCategories": [
      "backup"
    ],
    "SourceType": "CLUSTER_SNAPSHOT",
    "Date": "2018-10-06T12:26:13.882Z",
    "SourceIdentifier": "rds:my-db-cluster-snapshot",
    "Message": "Creating manual cluster snapshot"
  }
}
```

DB snapshot events

The following is an example of a DB snapshot event.

```
{
  "version": "0",
  "id": "844e2571-85d4-695f-b930-0153b71dcb42",
  "detail-type": "RDS DB Snapshot Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-10-06T12:26:13Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "EventCategories": [
      "deletion"
    ],
    "SourceType": "SNAPSHOT",
    "Date": "2018-10-06T12:26:13.882Z",
    "SourceIdentifier": "rds:my-db-snapshot",
    "Message": "Deleted manual snapshot"
  }
}
```
Amazon Aurora database log files

You can view, download, and watch database logs using the AWS Management Console, the AWS Command Line Interface (AWS CLI), or the Amazon RDS API. Viewing, downloading, or watching transaction logs isn't supported.

For engine-specific information, see the following:

- MySQL database log files (p. 622)
- PostgreSQL database log files (p. 627)

**Note**

In some cases, logs contain hidden data. Therefore, the AWS Management Console might show content in a log file, but the log file might be empty when you download it.

Viewing and listing database log files

You can view database log files for your DB engine by using the AWS Management Console. You can list what log files are available for download or monitoring by using the AWS CLI or Amazon RDS API.

**Console**

To view a database log file

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that has the log file that you want to view.
4. Choose the **Logs & events** tab.
5. Scroll down to the **Logs** section.
6. In the **Logs** section, choose the log that you want to view, and then choose **View**.

**AWS CLI**

To list the available database log files for a DB instance, use the AWS CLI `describe-db-log-files` command.

The following example returns a list of log files for a DB instance named `my-db-instance`.

**Example**

```
aws rds describe-db-log-files --db-instance-identifier my-db-instance
```

**RDS API**

To list the available database log files for a DB instance, use the Amazon RDS API `DescribeDBLogFiles` action.

**Downloading a database log file**

You can use the AWS Management Console, AWS CLI or API to download a database log file.
Console

To download a database log file

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the name of the DB instance that has the log file that you want to view.
4. Choose the Logs & events tab.
5. Scroll down to the Logs section.
6. In the Logs section, choose the button next to the log that you want to download, and then choose Download.
7. Open the context (right-click) menu for the link provided, and then choose Save Link As. Enter the location where you want the log file to be saved, and then choose Save.

AWS CLI

To download a database log file, use the AWS CLI command download-db-log-file-portion. By default, this command downloads only the latest portion of a log file. However, you can download an entire file by specifying the parameter --starting-token 0.

The following example shows how to download the entire contents of a log file called log/ERROR.4 and store it in a local file called errorlog.txt.

Example

For Linux, macOS, or Unix:

```bash
aws rds download-db-log-file-portion \
  --db-instance-identifier myexampledb \
  --starting-token 0 --output text \
  --log-file-name log/ERROR.4 > errorlog.txt
```

For Windows:

```bash
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

To download a database log file, use the Amazon RDS API DownloadDBLogFilePortion action.
Watching a database log file

You can monitor the contents of a log file by using the AWS Management Console.

Console

To watch a database log file

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the name of the DB instance that has the log file that you want to view.
4. Choose the Logs & events tab.
5. In the Logs section, choose a log file, and then choose Watch.

Publishing database logs to Amazon CloudWatch Logs

In addition to viewing and downloading DB instance logs, you can publish logs to Amazon CloudWatch Logs. With CloudWatch Logs, you can perform real-time analysis of the log data, store the data in highly durable storage, and manage the data with the CloudWatch Logs Agent. AWS retains log data published to CloudWatch Logs for an indefinite time period unless you specify a retention period. For more information, see Change log data retention in CloudWatch Logs.

For engine-specific information, see the following:

- the section called “Publishing Aurora MySQL logs to CloudWatch Logs” (p. 824)
- the section called “Publishing Aurora PostgreSQL logs to CloudWatch Logs” (p. 1075)

Reading log file contents using REST

Amazon RDS provides a REST endpoint that allows access to DB instance log files. This is useful if you need to write an application to stream Amazon RDS log file contents.

The syntax is:

```
GET /v13/downloadCompleteLogFile/DBInstanceIdentifier/LogFileName HTTP/1.1
Content-type: application/json
host: rds.region.amazonaws.com
```

The following parameters are required:

- `DBInstanceIdentifier`—the name of the DB instance that contains the log file you want to download.
- `LogFileName`—the name of the log file to be downloaded.

The response contains the contents of the requested log file, as a stream.

The following example downloads the log file named `log/ERROR.6` for the DB instance named `sample-sql` in the `us-west-2` region.

```
GET /v13/downloadCompleteLogFile/sample-sql/log/ERROR.6 HTTP/1.1
```
If you specify a nonexistent DB instance, the response consists of the following error:

- **DBInstanceNotFound**—**DBInstanceIdentifier** does not refer to an existing DB instance. (HTTP status code: 404)
MySQL database log files

You can monitor the MySQL error log, slow query log, and the general log. The MySQL error log is generated by default; you can generate the slow query and general logs by setting parameters in your DB parameter group. Amazon RDS rotates all of the MySQL log files; the intervals for each type are given following.

You can monitor the MySQL logs directly through the Amazon RDS console, Amazon RDS API, AWS CLI, or AWS SDKs. You can also access MySQL logs by directing the logs to a database table in the main database and querying that table. You can use the mysqlbinlog utility to download a binary log.

For more information about viewing, downloading, and watching file-based database logs, see Amazon Aurora database log files (p. 618).

Topics

- Accessing MySQL error logs (p. 622)
- Accessing the MySQL slow query and general logs (p. 622)
- Publishing Aurora MySQL logs to Amazon CloudWatch Logs (p. 624)
- Log file size (p. 624)
- Managing table-based MySQL logs (p. 624)
- Binary logging format (p. 624)
- Accessing MySQL binary logs (p. 625)

Accessing MySQL error logs

The MySQL error log is written to the mysql-error.log file. You can view mysql-error.log by using the Amazon RDS console or by retrieving the log using the Amazon RDS API, Amazon RDS CLI, or AWS SDKs. mysql-error.log is flushed every 5 minutes, and its contents are appended to mysql-error-running.log. The mysql-error-running.log file is then rotated every hour and the hourly files generated during the last 30 days are retained. Note that the retention period is different between Amazon RDS and Aurora.

Each log file has the hour it was generated (in UTC) appended to its name. The log files also have a timestamp that helps you determine when the log entries were written.

MySQL writes to the error log only on startup, shutdown, and when it encounters errors. A DB instance can go hours or days without new entries being written to the error log. If you see no recent entries, it's because the server did not encounter an error that would result in a log entry.

Accessing the MySQL slow query and general logs

The MySQL slow query log and the general log can be written to a file or a database table by setting parameters in your DB parameter group. For information about creating and modifying a DB parameter group, see Working with DB parameter groups and DB cluster parameter groups (p. 298). You must set these parameters before you can view the slow query log or general log in the Amazon RDS console or by using the Amazon RDS API, Amazon RDS CLI, or AWS SDKs.

You can control MySQL logging by using the parameters in this list:

- **slow_query_log**: To create the slow query log, set to 1. The default is 0.
- **general_log**: To create the general log, set to 1. The default is 0.
- **long_query_time**: To prevent fast-running queries from being logged in the slow query log, specify a value for the shortest query run time to be logged, in seconds. The default is 10 seconds; the minimum is 0. If log_output = FILE, you can specify a floating point value that goes to microsecond
resolution. If log_output = TABLE, you must specify an integer value with second resolution. Only queries whose run time exceeds the long_query_time value are logged. For example, setting long_query_time to 0.1 prevents any query that runs for less than 100 milliseconds from being logged.

- log_queries_not_using_indexes: To log all queries that do not use an index to the slow query log, set to 1. The default is 0. Queries that do not use an index are logged even if their run time is less than the value of the long_query_time parameter.

- log_output option: You can specify one of the following options for the log_output parameter.
  - TABLE – Write general queries to the mysql.general_log table, and slow queries to the mysql.slow_log table.
  - FILE – Write both general and slow query logs to the file system. Log files are rotated hourly.
  - NONE – Disable logging.

For Aurora MySQL 5.6, the default for log_output is TABLE. For Aurora MySQL 5.7, the default for log_output is FILE.

When logging is enabled, Amazon RDS rotates table logs or deletes log files at regular intervals. This measure is a precaution to reduce the possibility of a large log file either blocking database use or affecting performance. FILE and TABLE logging approach rotation and deletion as follows:

- When FILE logging is enabled, log files are examined every hour and log files older than 24 hours are deleted. In some cases, the remaining combined log file size after the deletion might exceed the threshold of 2 percent of a DB instance's allocated space. In these cases, the largest log files are deleted until the log file size no longer exceeds the threshold.

- When TABLE logging is enabled, in some cases log tables are rotated every 24 hours. This rotation occurs if the space used by the table logs is more than 20 percent of the allocated storage space or the size of all logs combined is greater than 10 GB. If the amount of space used for a DB instance is greater than 90 percent of the DB instance's allocated storage space, then the thresholds for log rotation are reduced. Log tables are then rotated if the space used by the table logs is more than 10 percent of the allocated storage space or the size of all logs combined is greater than 5 GB. You can subscribe to the low_free_storage event to be notified when log tables are rotated to free up space. For more information, see Using Amazon RDS event notification (p. 594).

When log tables are rotated, the current log table is copied to a backup log table and the entries in the current log table are removed. If the backup log table already exists, then it is deleted before the current log table is copied to the backup. You can query the backup log table if needed. The backup log table for the mysql.general_log table is named mysql.general_log_backup. The backup log table for the mysql.slow_log table is named mysql.slow_log_backup.

You can rotate the mysql.general_log table by calling the mysql.rds_rotate_general_log procedure. You can rotate the mysql.slow_log table by calling the mysql.rds_rotate_slow_log procedure.

Table logs are rotated during a database version upgrade.

To work with the logs from the Amazon RDS console, Amazon RDS API, Amazon RDS CLI, or AWS SDKs, set the log_output parameter to FILE. Like the MySQL error log, these log files are rotated hourly. The log files that were generated during the previous 72 hours are retained. Note that the retention period is different between Amazon RDS and Aurora.

For more information about the slow query and general logs, go to the following topics in the MySQL documentation:

- The slow query log
- The general query log
Publishing Aurora MySQL logs to Amazon CloudWatch Logs

You can configure your Aurora MySQL DB cluster to publish log data to a log group in Amazon CloudWatch Logs. With CloudWatch Logs, you can perform real-time analysis of the log data, and use CloudWatch to create alarms and view metrics. You can use CloudWatch Logs to store your log records in highly durable storage. For more information, see Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs (p. 824).

Log file size

The MySQL slow query log, error log, and the general log file sizes are constrained to no more than 2 percent of the allocated storage space for a DB instance. To maintain this threshold, logs are automatically rotated every hour and log files older than 24 hours are removed. If the combined log file size exceeds the threshold after removing old log files, then the largest log files are deleted until the log file size no longer exceeds the threshold.

For MySQL, there is a size limit on BLOBs written to the redo log. To account for this limit, ensure that the innodb_log_file_size parameter for your MySQL DB instance is 10 times larger than the largest BLOB data size found in your tables, plus the length of other variable length fields (VARCHAR, VARBINARY, TEXT) in the same tables. For information on how to set parameter values, see Working with DB parameter groups and DB cluster parameter groups (p. 298). For information on the redo log BLOB size limit, go to Changes in MySQL 5.6.20.

Managing table-based MySQL logs

You can direct the general and slow query logs to tables on the DB instance by creating a DB parameter group and setting the log_output server parameter to TABLE. General queries are then logged to the mysql.general_log table, and slow queries are logged to the mysql.slow_log table. You can query the tables to access the log information. Enabling this logging increases the amount of data written to the database, which can degrade performance.

Both the general log and the slow query logs are disabled by default. In order to enable logging to tables, you must also set the general_log and slow_query_log server parameters to 1.

Log tables keep growing until the respective logging activities are turned off by resetting the appropriate parameter to 0. A large amount of data often accumulates over time, which can use up a considerable percentage of your allocated storage space. Amazon RDS does not allow you to truncate the log tables, but you can move their contents. Rotating a table saves its contents to a backup table and then creates a new empty log table. You can manually rotate the log tables with the following command line procedures, where the command prompt is indicated by PROMPT>:

```
PROMPT> CALL mysql.rds_rotate_slow_log;
PROMPT> CALL mysql.rds_rotate_general_log;
```

To completely remove the old data and reclaim the disk space, call the appropriate procedure twice in succession.

Binary logging format

MySQL on Amazon Aurora supports the row-based, statement-based, and mixed binary logging formats for MySQL version 5.6 and later. The default binary logging format is mixed. For details on the different MySQL binary log formats, see Binary logging formats in the MySQL documentation.

If you plan to use replication, the binary logging format is important because it determines the record of data changes that is recorded in the source and sent to the replication targets. For information about the
advantages and disadvantages of different binary logging formats for replication, see Advantages and disadvantages of statement-based and row-based replication in the MySQL documentation.

**Important**

Setting the binary logging format to row-based can result in very large binary log files. Large binary log files reduce the amount of storage available for a DB cluster and can increase the amount of time to perform a restore operation of a DB cluster. Statement-based replication can cause inconsistencies between the source DB cluster and a read replica. For more information, see Determination of safe and unsafe statements in binary logging in the MySQL documentation.

### To set the MySQL binary logging format

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Parameter groups**.
3. Choose the parameter group used by the DB cluster you want to modify.
   
   You can’t modify a default parameter group. If the DB cluster is using a default parameter group, create a new parameter group and associate it with the DB cluster.

   For more information on parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).
4. From **Parameter group actions**, choose **Edit**.
5. Set the **binlog_format** parameter to the binary logging format of your choice (**ROW**, **STATEMENT**, or **MIXED**).
6. Choose **Save changes** to save the updates to the DB cluster parameter group.

**Important**

Changing a DB cluster parameter group affects all DB clusters that use that parameter group. If you want to specify different binary logging formats for different Aurora MySQL DB clusters in an AWS Region, the DB clusters must use different DB cluster parameter groups. These parameter groups identify different logging formats. Assign the appropriate DB cluster parameter group to each DB clusters. For more information about Aurora MySQL parameters, see Aurora MySQL parameters (p. 848).

### Accessing MySQL binary logs

You can use the mysqlbinlog utility to download or stream binary logs from Amazon RDS instances running MySQL 5.6 or later. The binary log is downloaded to your local computer, where you can perform actions such as replaying the log using the mysql utility. For more information about using the mysqlbinlog utility, go to Using mysqlbinlog to back up binary log files.

To run the mysqlbinlog utility against an Amazon RDS instance, use the following options:

- Specify the `--read-from-remote-server` option.
- `--host`: Specify the DNS name from the endpoint of the instance.
- `--port`: Specify the port used by the instance.
- `--user`: Specify a MySQL user that has been granted the replication slave permission.
- `--password`: Specify the password for the user, or omit a password value so that the utility prompts you for a password.
- To have the file downloaded in binary format, specify the `--raw` option.
- `-result-file`: Specify the local file to receive the raw output.
- Specify the names of one or more binary log files. To get a list of the available logs, use the SQL command `SHOW BINARY LOGS`. 

- To stream the binary log files, specify the `--stop-never` option.

For more information about `mysqlbinlog` options, go to `mysqlbinlog` - utility for processing binary log files.

For example, see the following.

For Linux, macOS, or Unix:

```bash
mysqlbinlog --read-from-remote-server --host=MySQL56Instance1.cg034hpkmjt.region.rds.amazonaws.com --port=3306 --user ReplUser --password --raw --result-file=/tmp/ binlog.00098
```

For Windows:

```bash
mysqlbinlog ^
 --read-from-remote-server ^
 --host=MySQL56Instance1.cg034hpkmjt.region.rds.amazonaws.com ^
 --port=3306 ^
 --user ReplUser ^
 --password ^
 --raw ^
 --result-file=/tmp/ ^
 binlog.00098
```

Amazon RDS normally purges a binary log as soon as possible, but the binary log must still be available on the instance to be accessed by mysqlbinlog. To specify the number of hours for RDS to retain binary logs, use the `mysql.rds_set_configuration` stored procedure and specify a period with enough time for you to download the logs. After you set the retention period, monitor storage usage for the DB instance to ensure that the retained binary logs don't take up too much storage.

**Note**

The `mysql.rds_set_configuration` stored procedure is only available for MySQL version 5.6 or later.

The following example sets the retention period to 1 day.

```sql
call mysql.rds_set_configuration('binlog retention hours', 24);
```

To display the current setting, use the `mysql.rds_show_configuration` stored procedure.

```sql
call mysql.rds_show_configuration;
```
PostgreSQL database log files

Amazon RDS for PostgreSQL generates query and error logs. RDS PostgreSQL writes autovacuum information and rds_admin actions to the error log. PostgreSQL also logs connections, disconnections, and checkpoints to the error log. For more information, see the Error reporting and logging in the PostgreSQL documentation.

To set logging parameters for a DB instance, set the parameters in a DB parameter group and associate that parameter group with the DB instance. For more information, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

Topics

- Setting the log retention period (p. 627)
- Setting log file rotation (p. 627)
- Setting the output format of the logs (p. 628)
- Enabling query logging (p. 628)

Setting the log retention period

To set the retention period for system logs, use the rds.log_retention_period parameter. You can find rds.log_retention_period in the DB parameter group associated with your DB instance. The unit for this parameter is minutes. For example, a setting of 1,440 retains logs for one day. The default value is 4,320 (three days). The maximum value is 10,080 (seven days). Your instance must have enough allocated storage to contain the retained log files.

Amazon Aurora compresses older PostgreSQL logs when storage for the DB instance reaches a threshold. Aurora compresses the files using the gzip compression utility; for information on gzip, see the gzip website. When storage for the DB instance is low and all available logs are compressed, you get a warning like the following.

Warning: local storage for PostgreSQL log files is critically low for this Aurora PostgreSQL instance, and could lead to a database outage.

Note

If storage gets too low, Aurora might delete compressed PostgreSQL logs before the retention period expires. If logs are deleted early, you get a message like the following.

The oldest PostgreSQL log files were deleted due to local storage constraints.

To retain older logs, publish them to Amazon CloudWatch Logs. For more information, see Publishing Aurora PostgreSQL logs to Amazon CloudWatch Logs (p. 1075). After you set up CloudWatch publishing, Aurora doesn't delete a log until it's published to CloudWatch Logs.

Setting log file rotation

To control PostgreSQL log file rotation, set two parameters in the DB parameter group associated with your DB instance: log_rotation_age and log_rotation_size. These two settings control when a new, distinct log file is created.

The log file names are based on the file name pattern of the log_filename parameter. For example, to provide log files names with a granularity of less than an hour, set log_filename to the minute format: postgresql.log.%Y-%m-%d-%H%M. Granularity of less than an hour is only supported for PostgreSQL version 10 and higher. To use a granularity in hours for log file names, set log_filename to the hour format: postgresql.log.%Y-%m-%d-%H.
To control log file rotation based on time, set the `log_rotation_age` parameter to anywhere from 1 minute to 1,440 minutes (24 hours). The `log_rotation_age` default is 60 minutes. If you set the `log_rotation_age` parameter to less than 60 minutes, also set the `log_filename` parameter to the minute format.

To control log file rotation based on file size, set the `log_rotation_size` parameter to anywhere from 50,000 to 1,000,000 KB. The default is 100,000 KB. We recommend that you also set the `log_filename` parameter to the minute format. Doing this makes sure that you can create a new log file in less than an hour if the `log_rotation_age` parameter is 60 minutes or greater.

### Setting the output format of the logs

By default, Aurora PostgreSQL generates logs in standard error (stderr) format. In this format, each log message is prefixed with the information specified by the parameter `log_line_prefix`. Aurora only allows the following value for `log_line_prefix`:

```
%t:%r:%u@%d:[%p]:t
```

The preceding value maps to the following code:

```
log-time : remote-host : user-name @ db-name : [ process-id ]
```

For example, the following error message results from querying a column using the wrong name.

```
2019-03-10 03:54:59 UTC:10.0.0.123(52834):postgres@tstdb:[20175]:ERROR: column "wrong" does not exist at character 8
```

To specify the format for output logs, use the parameter `log_destination`. To make the instance generate both standard and CSV output files, set `log_destination` to `csvlog` in your instance parameter group. For a discussion of PostgreSQL logs, see Working with RDS and Aurora PostgreSQL logs: Part 1.

### Enabling query logging

To enable query logging for your PostgreSQL DB instance, set two parameters in the DB parameter group associated with your DB instance: `log_statement` and `log_min_duration_statement`.

The `log_statement` parameter controls which SQL statements are logged. We recommend that you set this parameter to `all` to log all statements when you debug issues in your DB instance. The default value is `none`. To log all data definition language (DDL) statements (CREATE, ALTER, DROP, and so on), set this value to `ddl`. To log all DDL and data modification language (DML) statements (INSERT, UPDATE, DELETE, and so on), set this value to `mod`.

The `log_min_duration_statement` parameter sets the limit in milliseconds of a statement to be logged. All SQL statements that run longer than the parameter setting are logged. This parameter is disabled and set to `-1` by default. Enabling this parameter can help you find unoptimized queries.

To set up query logging, take the following steps:

1. Set the `log_statement` parameter to `all`. The following example shows the information that is written to the `postgres.log` file.

```
2013-11-05 16:48:56 UTC::@:::[2952]:LOG: received SIGHUP, reloading configuration files
2013-11-05 16:48:56 UTC::@:::[2952]:LOG: parameter "log_statement" changed to "all"
```
Additional information is written to the postgres.log file when you run a query. The following example shows the type of information written to the file after a query.

```
2013-11-05 16:41:07 UTC::@:[2955]:LOG: checkpoint starting: time
2013-11-05 16:41:07 UTC::@:[2955]:LOG: checkpoint complete: wrote 1 buffers (0.3%);
0 transaction log file(s) added, 0 removed, 1 recycled; write=0.000 s, sync=0.003 s,
total=0.012 s; sync files=1, longest=0.003 s, average=0.003 s
2013-11-05 16:45:14 UTC:[local]:master@postgres:[8839]:LOG: statement: SELECT d.datname
as "Name",
    pg_catalog.pg_get_userbyid(d.datdba) as "Owner",
    pg_catalog.pg_encoding_to_char(d.encoding) as "Encoding",
    d.datcollate as "Collate",
    d.datctype as "Ctype",
    pg_catalog.array_to_string(d.datacl, E'\n') AS "Access privileges"
FROM pg_catalog.pg_database d
ORDER BY 1;
```

2. Set the log_min_duration_statement parameter. The following example shows the information that is written to the postgres.log file when the parameter is set to 1.

```
2013-11-05 16:48:56 UTC::@:[2952]:LOG: received SIGHUP, reloading configuration files
2013-11-05 16:48:56 UTC::@:[2952]:LOG: parameter "log_min_duration_statement" changed to
"1"
```

Additional information is written to the postgres.log file when you run a query that exceeds the duration parameter setting. The following example shows the type of information written to the file after a query.

```
2013-11-05 16:51:10 UTC:[local]:master@postgres:[9193]:LOG: statement: SELECT
c2.relname, i.indisprimary, i.indisunique, i.indisclustered, i.indisvalid,
    pg_catalog.pg_get_indexdef(i.indexrelid, 0, true),
    pg_catalog.pg_get_constraintdef(con.oid, true), contype, condeferrable, condeferred,
c2.reltablespace
FROM pg_catalog.pg_class c, pg_catalog.pg_class c2, pg_catalog.pg_index i
    LEFT JOIN pg_catalog.pg_constraint con ON (conrelid = i.indexrelid AND conindid =
        i.indexrelid AND contype IN ('p','u','x'))
WHERE c.oid = '1255' AND c.oid = i.indrelid AND i.indexrelid = c2.oid
ORDER BY i.indisprimary DESC, i.indisunique DESC, c2.relname;
2013-11-05 16:51:10 UTC:[local]:master@postgres:[9193]:LOG: duration: 3.367 ms
2013-11-05 16:51:10 UTC:[local]:master@postgres:[9193]:LOG: statement: SELECT
c.oid::pg_catalog.regclass FROM pg_catalog.pg_class c,
    pg_catalog.pg_inherits i WHERE c.oid=i.inhparent AND i.inhrelid = '1255' ORDER BY
    inhseqno;
2013-11-05 16:51:18 UTC:[local]:master@postgres:[9193]:LOG: statement: select proname
```

from pg_proc;
2013-11-05 16:51:18 UTC:[local]:master@postgres:[9193]:LOG: duration: 3.469 ms
Working with AWS CloudTrail and Amazon RDS

AWS CloudTrail is an AWS service that helps you audit your AWS account. CloudTrail is enabled on your AWS account when you create it.

For complete information about CloudTrail, see the AWS CloudTrail User Guide.

CloudTrail integration with Amazon RDS

All Amazon RDS actions are logged by CloudTrail. CloudTrail provides a record of actions taken by a user, role, or an AWS service in Amazon RDS.

CloudTrail events

CloudTrail captures API calls for Amazon RDS as events. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. Events include calls from the Amazon RDS console and from code calls to the Amazon RDS APIs.

Amazon RDS activity is recorded in a CloudTrail event in Event history. You can use the CloudTrail console to view the last 90 days of recorded API activity and events in an AWS Region. For more information, see Viewing events with CloudTrail event history.

CloudTrail trails

For an ongoing record of events in your AWS account, including events for Amazon RDS, create a trail. A trail is a configuration that enables delivery of events to a specified Amazon S3 bucket. CloudTrail typically delivers log files within 15 minutes of account activity.

Note
If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history.

You can create two types of trails for an AWS account: a trail that applies to all regions, or a trail that applies to one region. By default, when you create a trail in the console, the trail applies to all regions.

Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions and Receiving CloudTrail log files from multiple accounts

Amazon RDS log file entries

CloudTrail log files contain one or more log entries. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the CreateDBInstance action.

```json
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
```
"principalId": "AKIAIOSFODNN7EXAMPLE",
"arn": "arn:aws:iam::123456789012:user/johndoe",
"accountId": "123456789012",
"accessKeyId": "AKIAI44QH8DHBEXAMPLE",
"userName": "johndoe"
},
"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",
   "storageDestroyed": false,
   "preferredBackupWindow": "10:27-10:57",
   "preferredMaintenanceWindow": "sat:05:47-sat:06:17",
   "backupRetentionPeriod": 1,
   "allocatedStorage": 20,
   "storageType": "standard",
   "engineVersion": "5.6.39",
   "dBInstancePort": 0,
   "optionGroupMemberships": [
      {
         "status": "in-sync",
         "optionGroupName": "default:mysql5.6"
      }
   ],
   "dBPParameterGroups": [
      {
         "dBPParameterGroupName": "default.mysql5.6",
         "parameterApplyStatus": "in-sync"
      }
   ],
   "monitoringInterval": 0,
   "dBInstanceClass": "db.m1.small",
   "readReplicaDBInstanceIdentifiers": [],
   "dBSubnetGroup": {
      "dBSubnetGroupName": "default",
      "dBSubnetGroupDescription": "default",
      "subnets": [
         {
            "subnetAvailabilityZone": {"name": "us-east-1b"},
            "subnetIdentifier": "subnet-cbfff289",
            "subnetStatus": "Active"
         },
         {
            "subnetAvailabilityZone": {"name": "us-east-1e"},
            "subnetIdentifier": "subnet-d7c825e8",
            "subnetStatus": "Active"
         }
      ]
   }
}
As shown in the `userIdentity` element in the preceding example, every event or log entry contains information about who generated the request. The identity information helps you determine the following:
• Whether the request was made with root or IAM user credentials.
• Whether the request was made with temporary security credentials for a role or federated user.
• Whether the request was made by another AWS service.

For more information about the `userIdentity`, see the [CloudTrail `userIdentity` element](https://docs.aws.amazon.com/AmazonCloudTrail/latest/APIReference/API_CreateTrail.html). For more information about `CreateDBInstance` and other Amazon RDS actions, see the [Amazon RDS API Reference](https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/).
Working with Amazon Aurora MySQL

Amazon Aurora MySQL is a fully managed, MySQL-compatible, relational database engine that combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. Aurora MySQL is a drop-in replacement for MySQL and makes it simple and cost-effective to set up, operate, and scale your new and existing MySQL deployments, thus freeing you to focus on your business and applications. Amazon RDS provides administration for Aurora by handling routine database tasks such as provisioning, patching, backup, recovery, failure detection, and repair. Amazon RDS also provides push-button migration tools to convert your existing Amazon RDS for MySQL applications to Aurora MySQL.

Topics
• Overview of Amazon Aurora MySQL (p. 634)
• Security with Amazon Aurora MySQL (p. 637)
• Updating applications to connect to Aurora MySQL DB clusters using new SSL/TLS certificates (p. 640)
• Migrating data to an Amazon Aurora MySQL DB cluster (p. 644)
• Managing Amazon Aurora MySQL (p. 675)
• Working with parallel query for Amazon Aurora MySQL (p. 697)
• Using advanced auditing with an Amazon Aurora MySQL DB cluster (p. 727)
• Single-master replication with Amazon Aurora MySQL (p. 730)
• Working with Aurora multi-master clusters (p. 766)
• Integrating Amazon Aurora MySQL with other AWS services (p. 792)
• Amazon Aurora MySQL lab mode (p. 839)
• Best practices with Amazon Aurora MySQL (p. 840)
• Amazon Aurora MySQL reference (p. 848)
• Database engine updates for Amazon Aurora MySQL (p. 874)

Overview of Amazon Aurora MySQL

The following sections provide an overview of Amazon Aurora MySQL.

Topics
• Amazon Aurora MySQL performance enhancements (p. 634)
• Amazon Aurora MySQL and spatial data (p. 635)
• Comparison of Aurora MySQL 5.6 and Aurora MySQL 5.7 (p. 636)
• Comparison of Aurora MySQL 5.7 and MySQL 5.7 (p. 636)

Amazon Aurora MySQL performance enhancements

Amazon Aurora includes performance enhancements to support the diverse needs of high-end commercial databases.

Fast insert

Fast insert accelerates parallel inserts sorted by primary key and applies specifically to LOAD DATA and INSERT INTO ... SELECT ... statements. Fast insert caches the position of a cursor in an index traversal while executing the statement. This avoids unnecessarily traversing the index again.
You can monitor the following metrics to determine the effectiveness of fast insert for your DB cluster:

- **aurora_fast_insert_cache_hits**: A counter that is incremented when the cached cursor is successfully retrieved and verified.
- **aurora_fast_insert_cache_misses**: A counter that is incremented when the cached cursor is no longer valid and Aurora performs a normal index traversal.

You can retrieve the current value of the fast insert metrics using the following command:

```sql
mysql> show global status like 'Aurora_fast_insert%';
```

You will get output similar to the following:

<table>
<thead>
<tr>
<th>Variable_name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora_fast_insert_cache_hits</td>
<td>3598300</td>
</tr>
<tr>
<td>Aurora_fast_insert_cache_misses</td>
<td>436401336</td>
</tr>
</tbody>
</table>

**Amazon Aurora MySQL and spatial data**

The following list summarizes the main Aurora MySQL spatial features and explains how they correspond to spatial features in MySQL:

- Aurora MySQL 1.x supports the same spatial data types and spatial relation functions as MySQL 5.6.
- Aurora MySQL 2.x supports the same spatial data types and spatial relation functions as MySQL 5.7.
- Aurora MySQL 1.x and 2.x both support spatial indexing on InnoDB tables. Spatial indexing improves query performance on large datasets for queries on spatial data. In MySQL, spatial indexing for InnoDB tables isn't available in MySQL 5.6, but is available in MySQL 5.7. Both Aurora MySQL 1.x and 2.x use a different spatial indexing strategy than MySQL for high performance with spatial queries. The Aurora spatial index implementation uses a space-filling curve on a B-tree, which is intended to provide higher performance for spatial range scans than an R-tree.

The following data definition language (DDL) statements are supported for creating indexes on columns that use spatial data types.

**CREATE TABLE**

You can use the `SPATIAL INDEX` keywords in a `CREATE TABLE` statement to add a spatial index to a column in a new table. Following is an example.

```sql
CREATE TABLE test (shape POLYGON NOT NULL, SPATIAL INDEX(shape));
```

**ALTER TABLE**

You can use the `SPATIAL INDEX` keywords in an `ALTER TABLE` statement to add a spatial index to a column in an existing table. Following is an example.

```sql
ALTER TABLE test ADD SPATIAL INDEX(shape);
```
CREATE INDEX

You can use the `SPATIAL` keyword in a `CREATE INDEX` statement to add a spatial index to a column in an existing table. Following is an example.

```
CREATE SPATIAL INDEX shape_index ON test (shape);
```

Comparison of Aurora MySQL 5.6 and Aurora MySQL 5.7

The following Amazon Aurora MySQL features are supported in Aurora MySQL 5.6, but these features are currently not supported in Aurora MySQL 5.7.

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. You can asynchronously invoke AWS Lambda functions from Aurora MySQL 5.7. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).

Currently, Aurora MySQL 5.7 does not support features added in Aurora MySQL version 1.16 and later. For information about Aurora MySQL version 1.16, see Aurora MySQL database engine updates 2017-12-11 (p. 955).

The performance schema isn't available for early release of Aurora MySQL 5.7. Upgrade to Aurora 2.03 or higher for performance schema support.

Comparison of Aurora MySQL 5.7 and MySQL 5.7

The following features are supported in MySQL 5.7.12 but are currently not supported in Aurora MySQL 5.7:

- Group replication plugin
- Increased page size
- InnoDB buffer pool loading at startup
- InnoDB full-text parser plugin
- Multisource replication
- Online buffer pool resizing
- Password validation plugin
- Query rewrite plugins
- Replication filtering
- The `CREATE TABLESPACE` SQL statement
- X Protocol

For more information about these features, see the MySQL 5.7 documentation.
Security with Amazon Aurora MySQL

Security for Amazon Aurora MySQL is managed at three levels:

- To control who can perform Amazon RDS management actions on Aurora MySQL DB clusters and DB instances, you use AWS Identity and Access Management (IAM). When you connect to AWS using IAM credentials, your AWS account must have IAM policies that grant the permissions required to perform Amazon RDS management operations. For more information, see Identity and access management in Amazon Aurora (p. 1222).

  If you are using IAM to access the Amazon RDS console, you must first sign on to the AWS Management Console with your IAM user credentials. Then go to the Amazon RDS console at https://console.aws.amazon.com/rds/.

- Aurora MySQL DB clusters must be created in an Amazon Virtual Private Cloud (VPC). To control which devices and Amazon EC2 instances can open connections to the endpoint and port of the DB instance for Aurora MySQL DB clusters in a VPC, you use a VPC security group. These endpoint and port connections can be made using Secure Sockets Layer (SSL). In addition, firewall rules at your company can control whether devices running at your company can open connections to a DB instance. For more information on VPCs, see Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281).

  The supported VPC tenancy depends on the instance class used by your Aurora MySQL DB clusters. With default VPC tenancy, the VPC runs on shared hardware. With dedicated VPC tenancy, the VPC runs on a dedicated hardware instance. Aurora MySQL supports the following VPC tenancy based on the instance class:

  - The db.r3 instance classes support both default and dedicated VPC tenancy.
  - The db.r4 instance classes support default and dedicated VPC tenancy only.
  - The db.t2 instance classes support default VPC tenancy only.

  For more information about instance classes, see DB instance classes (p. 46). For more information about default and dedicated VPC tenancy, see Dedicated instances in the Amazon Elastic Compute Cloud User Guide.

- To authenticate login and permissions for an Amazon Aurora MySQL DB cluster, you can take either of the following approaches, or a combination of them:

  - You can take the same approach as with a standalone instance of MySQL.

    Commands such as CREATE USER, RENAME USER, GRANT, REVOKE, and SET PASSWORD work just as they do in on-premises databases, as does directly modifying database schema tables. For more information, see Access control and account management in the MySQL documentation.

  - You can also use IAM database authentication.

    With IAM database authentication, you authenticate to your DB cluster by using an IAM user or IAM role and an authentication token. An authentication token is a unique value that is generated using the Signature Version 4 signing process. By using IAM database authentication, you can use the same credentials to control access to your AWS resources and your databases. For more information, see IAM database authentication (p. 1238).

Master user privileges with Amazon Aurora MySQL

When you create an Amazon Aurora MySQL DB instance, the master user has the following default privileges:

- ALTER
- ALTER ROUTINE
- CREATE
To provide management services for each DB cluster, the rdsadmin user is created when the DB cluster is created. Attempting to drop, rename, change the password, or change privileges for the rdsadmin account results in an error.

For management of the Aurora MySQL DB cluster, the standard kill and kill_query commands have been restricted. Instead, use the Amazon RDS commands rds_kill and rds_kill_query to terminate user sessions or queries on Aurora MySQL DB instances.

**Note**
Encryption of a database instance and snapshots is not supported for the China (Ningxia) region.

### Using SSL/TLS with Aurora MySQL DB clusters

Amazon Aurora MySQL DB clusters support Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections from applications using the same process and public key as Amazon RDS MySQL DB instances.

Amazon RDS creates an SSL/TLS certificate and installs the certificate on the DB instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The SSL/TLS certificate includes the DB instance endpoint as the Common Name (CN) for the SSL/TLS certificate to guard against spoofing attacks. As a result, you can only use the DB cluster endpoint to connect to a DB cluster using SSL/TLS if your client supports Subject Alternative Names (SAN). Otherwise, you must use the instance endpoint of a writer instance.
For information about downloading certificates, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).

We recommend the MariaDB Connector/J client as a client that supports SAN with SSL. For more information, see the MariaDB Connector/J download page.

**Topics**
- Requiring an SSL/TLS connection to an Aurora MySQL DB cluster (p. 639)
- TLS versions for Aurora MySQL (p. 639)
- Encrypting connections to an Aurora MySQL DB cluster (p. 640)

**Requiring an SSL/TLS connection to an Aurora MySQL DB cluster**

You can require that all user connections to your Aurora MySQL DB cluster use SSL/TLS by using the `require_secure_transport` DB cluster parameter. By default, the `require_secure_transport` parameter is set to `OFF`. You can set the `require_secure_transport` parameter to `ON` to require SSL/TLS for connections to your DB cluster.

You can set the `require_secure_transport` parameter value by updating the DB cluster parameter group for your DB cluster. You don't need to reboot your DB cluster for the change to take effect. For more information on parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

**Note**
The `require_secure_transport` parameter is only available for Aurora MySQL version 5.7.

When the `require_secure_transport` parameter is set to `ON` for a DB cluster, a database client can connect to it if it can establish an encrypted connection. Otherwise, an error message similar to the following is returned to the client:

```
MySQL Error 3159 (HY000): Connections using insecure transport are prohibited while --require_secure_transport=ON.
```

**TLS versions for Aurora MySQL**

Aurora MySQL supports Transport Layer Security (TLS) versions 1.0, 1.1, and 1.2. The following table shows the TLS support for Aurora MySQL versions.

<table>
<thead>
<tr>
<th>Aurora MySQL version</th>
<th>TLS 1.0</th>
<th>TLS 1.1</th>
<th>TLS 1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora MySQL 5.7</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Aurora MySQL 5.6</td>
<td>Supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

For an Aurora MySQL 5.7 DB cluster, you can use the `tls_version` DB cluster parameter to indicate the permitted protocol versions. Similar client parameters exist for most client tools or database drivers. Some older clients might not support newer TLS versions. By default, the DB cluster attempts to use the highest TLS protocol version allowed by both the server and client configuration.

Set the `tls_version` DB cluster parameter to one of the following values:

- **TLSv1.2** – Only the TLS version 1.2 protocol is permitted for encrypted connections.
• TLSv1.1 – TLS version 1.1 and 1.2 protocols are permitted for encrypted connections.
• TLSv1 – TLS version 1.0, 1.1, and 1.2 protocols are permitted for encrypted connections.

If the parameter isn't set, then TLS version 1.0, 1.1, and 1.2 protocols are permitted for encrypted connections.

**Note**
The `tls_version` DB cluster parameter isn't available for Aurora MySQL 5.6.

### Encrypting connections to an Aurora MySQL DB cluster

To encrypt connections using the default `mysql` client, launch the `mysql` client using the `--ssl-ca` parameter to reference the public key, for example:

**For MySQL 5.7 and later:**

```bash
mysql -h myinstance.c9akciq32.rds-us-east-1.amazonaws.com --ssl-ca=[full path]rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY
```

**For MySQL 5.6 and earlier:**

```bash
mysql -h myinstance.c9akciq32.rds-us-east-1.amazonaws.com --ssl-ca=[full path]rds-combined-ca-bundle.pem --ssl-verify-server-cert
```

You can require SSL/TLS connections for specific users accounts. For example, you can use one of the following statements, depending on your MySQL version, to require SSL/TLS connections on the user account `encrypted_user`.

**For MySQL 5.7 and later:**

```sql
ALTER USER 'encrypted_user'@'%' REQUIRE SSL;
```

**For MySQL 5.6 and earlier:**

```sql
GRANT USAGE ON *.* TO 'encrypted_user'@'%' REQUIRE SSL;
```

When you use an RDS proxy, you connect to the proxy endpoint instead of the usual cluster endpoint. You can make SSL/TLS required or optional for connections to the proxy, in the same way as for connections directly to the Aurora DB cluster. For information about using the RDS Proxy, see Managing connections with Amazon RDS Proxy (p. 260).

**Note**
For more information on SSL/TLS connections with MySQL, see the MySQL documentation.

### Updating applications to connect to Aurora MySQL DB clusters using new SSL/TLS certificates

As of September 19, 2019, Amazon RDS has published new Certificate Authority (CA) certificates for connecting to your Aurora DB clusters using Secure Socket Layer or Transport Layer Security (SSL/TLS). Following, you can find information about updating your applications to use the new certificates.
This topic can help you to determine whether any client applications use SSL/TLS to connect to your DB clusters. If they do, you can further check whether those applications require certificate verification to connect.

**Note**
Some applications are configured to connect to Aurora MySQL DB clusters only if they can successfully verify the certificate on the server. For such applications, you must update your client application trust stores to include the new CA certificates.

After you update your CA certificates in the client application trust stores, you can rotate the certificates on your DB clusters. We strongly recommend testing these procedures in a development or staging environment before implementing them in your production environments.

For more information about certificate rotation, see Rotating your SSL/TLS certificate (p. 1213). For more information about downloading certificates, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211). For information about using SSL/TLS with Aurora MySQL DB clusters, see Using SSL/TLS with Aurora MySQL DB clusters (p. 638).

**Topics**
- Determining whether any applications are connecting to your Aurora MySQL DB cluster using SSL (p. 641)
- Determining whether a client requires certificate verification to connect (p. 642)
- Updating your application trust store (p. 642)
- Example Java code for establishing SSL connections (p. 643)

### Determining whether any applications are connecting to your Aurora MySQL DB cluster using SSL

If you are using Aurora MySQL version 2 (compatible with MySQL 5.7) and the Performance Schema is enabled, run the following query to check if connections are using SSL/TLS. For information about enabling the Performance Schema, see Performance Schema quick start in the MySQL documentation.

```sql
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 this sample output, you can see both your own session (admin) and an application logged in as webapp1 are using SSL.

<table>
<thead>
<tr>
<th>id</th>
<th>user</th>
<th>host</th>
<th>connection_type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>admin</td>
<td>10.0.4.249:42590</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td>4</td>
<td>event_scheduler</td>
<td>localhost</td>
<td>NULL</td>
</tr>
<tr>
<td>10</td>
<td>webapp1</td>
<td>159.28.1.1:42189</td>
<td>SSL/TLS</td>
</tr>
</tbody>
</table>

3 rows in set (0.00 sec)

If you are using Aurora MySQL version 1 (compatible with MySQL 5.6), then you can't determine from the server side whether applications are connecting with or without SSL. For those versions, you can determine whether SSL is used by examining the application's connection method. You can find more information on examining the client connection configuration in the following section.
Determining whether a client requires certificate verification to connect

You can check whether JDBC clients and MySQL clients require certificate verification to connect.

**JDBC**

The following example with MySQL Connector/J 8.0 shows one way to check an application’s JDBC connection properties to determine whether successful connections require a valid certificate. For more information on all of the JDBC connection options for MySQL, see Configuration properties in the MySQL documentation.

When using the MySQL Connector/J 8.0, an SSL connection requires verification against the server CA certificate if your connection properties have `sslMode` set to `VERIFY_CA` or `VERIFY_IDENTITY`, as in the following example.

```java
Properties properties = new Properties();
properties.setProperty("sslMode", "VERIFY_IDENTITY");
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);
```

**Note**

If you use either the MySQL Java Connector v5.1.38 or later, or the MySQL Java Connector v8.0.9 or later to connect to your databases, even if you haven't explicitly configured your applications to use SSL/TLS when connecting to your databases, these client drivers default to using SSL/TLS. In addition, when using SSL/TLS, they perform partial certificate verification and fail to connect if the database server certificate is expired.

**MySQL**

The following examples with the MySQL Client show two ways to check a script's MySQL connection to determine whether successful connections require a valid certificate. For more information on all of the connection options with the MySQL Client, see Client-side configuration for encrypted connections in the MySQL documentation.

When using the MySQL 5.7 or MySQL 8.0 Client, an SSL connection requires verification against the server CA certificate if for the `--ssl-mode` option you specify `VERIFY_CA` or `VERIFY_IDENTITY`, as in the following example.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --ssl-mode=VERIFY_CA
```

When using the MySQL 5.6 Client, an SSL connection requires verification against the server CA certificate if you specify the `--ssl-verify-server-cert` option, as in the following example.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --ssl-verify-server-cert
```

**Updating your application trust store**

For information about updating the trust store for MySQL applications, see Installing SSL certificates in the MySQL documentation.

**Note**

When you update the trust store, you can retain older certificates in addition to adding the new certificates.
Updating your application trust store for JDBC

You can update the trust store for applications that use JDBC for SSL/TLS connections.

To update the trust store for JDBC applications

1. Download the 2019 root certificate that works for all AWS Regions and put the file in the trust store directory.

   For information about downloading the root certificate, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).

2. Convert the certificate to .der format using the following command.


   Replace the file name with the one that you downloaded.

3. Import the certificate into the key store using the following command.


4. Confirm that the key store was updated successfully.

   `keytool -list -v -keystore clientkeystore.jks`

   Enter the metastore password when you are prompted for it.

   Your output should contain the following.

   ```
   rds-root, date, trustedCertEntry,
   Certificate fingerprint (SHA1):
   # This fingerprint should match the output from the below command
   openssl x509 -fingerprint -in rds-ca-2019-root.pem -noout
   ```

If you are using the mysql JDBC driver in an application, set the following properties in the application.

```
System.setProperty("javax.net.ssl.trustStore", "certs");
System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

When you start the application, set the following properties.

```
java -Djavax.net.ssl.trustStore=/path_to_truststore/MyTruststore.jks -Djavax.net.ssl.trustStorePassword=my_truststore_password -Dcom.companyName.MyApplication
```

Example Java code for establishing SSL connections

The following code example shows how to set up the SSL connection that validates the server certificate using JDBC.

```java
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
After you have determined that your database connections use SSL/TLS and have updated your
application trust store, you can update your database to use the rds-ca-2019 certificates. For
instructions, see step 3 in Updating your CA certificate by modifying your DB instance (p. 1214).

Migrating data to an Amazon Aurora MySQL DB cluster

You have several options for migrating data from your existing database to an Amazon Aurora MySQL DB
cluster. Your migration options also depend on the database that you are migrating from and the size of
the data that you are migrating.

There are two different types of migration: physical and logical. Physical migration means that physical
copies of database files are used to migrate the database. Logical migration means that the migration is
accomplished by applying logical database changes, such as inserts, updates, and deletes.

Physical migration has the following advantages:

- Physical migration is faster than logical migration, especially for large databases.
- Database performance does not suffer when a backup is taken for physical migration.
- Physical migration can migrate everything in the source database, including complex database
  components.

Physical migration has the following limitations:

- The innodb_page_size parameter must be set to its default value (16KB).
- The innodb_data_file_path parameter must be configured with only one data file that uses the
default data file name "ibdata1:12M:autoextend". Databases with two data files, or with a data
  file with a different name, can't be migrated using this method.
The following are examples of file names that are not allowed: "innodb_data_file_path=ibdata1:50M; ibdata2:50M:autolead" and "innodb_data_file_path=ibdata01:50M:autolead".

- The `innodb_log_files_in_group` parameter must be set to its default value (2).

Logical migration has the following advantages:

- You can migrate subsets of the database, such as specific tables or parts of a table.
- The data can be migrated regardless of the physical storage structure.

Logical migration has the following limitations:

- Logical migration is usually slower than physical migration.
- Complex database components can slow down the logical migration process. In some cases, complex database components can even block logical migration.

The following table describes your options and the type of migration for each option.

<table>
<thead>
<tr>
<th>Migrating from</th>
<th>Migration type</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Amazon RDS MySQL DB instance</td>
<td>Physical</td>
<td>You can migrate from an RDS MySQL DB instance by first creating an Aurora MySQL read replica of a MySQL DB instance. When the replica lag between the MySQL DB instance and the Aurora MySQL read replica is 0, you can direct your client applications to read from the Aurora read replica and then stop replication to make the Aurora MySQL read replica a standalone Aurora MySQL DB cluster for reading and writing. For details, see [Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using an Aurora read replica](p. 666).</td>
</tr>
<tr>
<td>An RDS MySQL DB snapshot</td>
<td>Physical</td>
<td>You can migrate data directly from an Amazon RDS MySQL DB snapshot to an Amazon Aurora MySQL DB cluster. For details, see [Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using a DB snapshot](p. 659).</td>
</tr>
<tr>
<td>A MySQL database external to Amazon RDS</td>
<td>Logical</td>
<td>You can create a dump of your data using the <code>mysqldump</code> utility, and then import that data into an existing Amazon Aurora MySQL DB cluster. For details, see [Migrating from MySQL to Amazon Aurora by using mysqldump](p. 659).</td>
</tr>
<tr>
<td>A MySQL database external to Amazon RDS</td>
<td>Physical</td>
<td>You can copy the backup files from your database to an Amazon Simple Storage Service (Amazon S3) bucket, and then restore an Amazon Aurora MySQL DB</td>
</tr>
</tbody>
</table>
### Migrating from an external MySQL database to Aurora MySQL

<table>
<thead>
<tr>
<th>Migrating from</th>
<th>Migration type</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A MySQL database external to Amazon RDS</td>
<td>Logical</td>
<td>You can save data from your database as text files and copy those files to an Amazon S3 bucket. You can then load that data into an existing Aurora MySQL DB cluster using the <code>LOAD DATA FROM S3</code> MySQL command. For more information, see [Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket](p. 804).</td>
</tr>
<tr>
<td>A database that is not MySQL-compatible</td>
<td>Logical</td>
<td>You can use AWS Database Migration Service (AWS DMS) to migrate data from a database that is not MySQL-compatible. For more information on AWS DMS, see [What is AWS database migration service?](</td>
</tr>
</tbody>
</table>

**Note**

- If you are migrating a MySQL database external to Amazon RDS, the migration options described in the table are supported only if your database supports the InnoDB or MyISAM tablespaces.
- If the MySQL database you are migrating to Aurora MySQL uses `memcached`, remove `memcached` before migrating it.

### Migrating data from an external MySQL database to an Amazon Aurora MySQL DB cluster

If your database supports the InnoDB or MyISAM tablespaces, you have these options for migrating your data to an Amazon Aurora MySQL DB cluster:

- You can create a dump of your data using the `mysqldump` utility, and then import that data into an existing Amazon Aurora MySQL DB cluster. For more information, see [Migrating from MySQL to Amazon Aurora by using mysqldump](p. 659).
- You can copy the full and incremental backup files from your database to an Amazon S3 bucket, and then restore an Amazon Aurora MySQL DB cluster from those files. This option can be considerably faster than migrating data using `mysqldump`. For more information, see [Migrating data from MySQL by using an Amazon S3 bucket](p. 646).

### Migrating data from MySQL by using an Amazon S3 bucket

You can copy the full and incremental backup files from your source MySQL version 5.5, 5.6, or 5.7 database to an Amazon S3 bucket, and then restore an Amazon Aurora MySQL DB cluster from those files.
This option can be considerably faster than migrating data using `mysqldump`, because using `mysqldump` replays all of the commands to recreate the schema and data from your source database in your new Aurora MySQL DB cluster. By copying your source MySQL data files, Aurora MySQL can immediately use those files as the data for an Aurora MySQL DB cluster.

**Note**
The Amazon S3 bucket and the Amazon Aurora MySQL DB cluster must be in the same AWS Region.

Aurora MySQL doesn't restore everything from your database. You should save the database schema and values for the following items from your source MySQL database and add them to your restored Aurora MySQL DB cluster after it has been created:

- User accounts
- Functions
- Stored procedures
- Time zone information. Time zone information is loaded from the local operating system of your Amazon Aurora MySQL DB cluster. For more information, see Local time zone for Amazon Aurora DB clusters (p. 9).

You can't restore from an encrypted source database, but you can encrypt the data being migrated. You can also leave the data unencrypted during the migration process.

You can't migrate from a source database that has tables defined outside of the default MySQL data directory.

Also, decide whether you want to minimize downtime by using binary log replication during the migration process. If you use binary log replication, the external MySQL database remains open to transactions while the data is being migrated to the Aurora MySQL DB cluster. After the Aurora MySQL DB cluster has been created, you use binary log replication to synchronize the Aurora MySQL DB cluster with the transactions that happened after the backup. When the Aurora MySQL DB cluster is caught up with the MySQL database, you finish the migration by completely switching to the Aurora MySQL DB cluster for new transactions.

**Topics**
- Before you begin (p. 647)
- Backing up files to be restored as an Amazon Aurora MySQL DB cluster (p. 649)
- Restoring an Amazon Aurora MySQL DB cluster from an Amazon S3 bucket (p. 651)
- Synchronizing the Amazon Aurora MySQL DB cluster with the MySQL database using replication (p. 654)

**Before you begin**

Before you can copy your data to an Amazon S3 bucket and restore a DB cluster from those files, you must do the following:

- Install Percona XtraBackup on your local server.
- Permit Aurora MySQL to access your Amazon S3 bucket on your behalf.

**Installing Percona XtraBackup**

Amazon Aurora can restore a DB cluster from files that were created using Percona XtraBackup. You can install Percona XtraBackup from Download Percona XtraBackup.
Note
For MySQL 5.7 migration, you must use Percona XtraBackup 2.4. For earlier MySQL versions, use Percona XtraBackup 2.3 or 2.4.

Required permissions
To migrate your MySQL data to an Amazon Aurora MySQL DB cluster, several permissions are required:

- The user that is requesting that Aurora create a new cluster from an Amazon S3 bucket must have permission to list the buckets for your AWS account. You grant the user this permission using an AWS Identity and Access Management (IAM) policy.
- Aurora requires permission to act on your behalf to access the Amazon S3 bucket where you store the files used to create your Amazon Aurora MySQL DB cluster. You grant Aurora the required permissions using an IAM service role.
- The user making the request must also have permission to list the IAM roles for your AWS account.
- If the user making the request is to create the IAM service role or request that Aurora create the IAM service role (by using the console), then the user must have permission to create an IAM role for your AWS account.
- If you plan to encrypt the data during the migration process, update the IAM policy of the user who will perform the migration to grant RDS access to the AWS Key Management Service customer master keys (CMKs) used for encrypting the backups. For instructions, see Creating an IAM policy to access AWS KMS resources (p. 798).

For example, the following IAM policy grants a user the minimum required permissions to use the console to list IAM roles, create an IAM role, list the Amazon S3 buckets for your account, and list the AWS KMS CMKs.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles",
        "iam:CreateRole",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "s3:ListBucket",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Additionally, for a user to associate an IAM role with an Amazon S3 bucket, the IAM user must have the `iam:PassRole` permission for that IAM role. This permission allows an administrator to restrict which IAM roles a user can associate with Amazon S3 buckets.

For example, the following IAM policy allows a user to associate the role named `S3Access` with an Amazon S3 bucket.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3AccessRole",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::mybucket/*"
    }
  ]
}
```
For more information on IAM user permissions, see Managing access using policies (p. 1224).

Creating the IAM service role

You can have the AWS Management Console create a role for you by choosing the Create a New Role option (shown later in this topic). If you select this option and specify a name for the new role, then Aurora creates the IAM service role required for Aurora to access your Amazon S3 bucket with the name that you supply.

As an alternative, you can manually create the role using the following procedure.

To create an IAM role for Aurora to access Amazon S3

1. Complete the steps in Creating an IAM policy to access Amazon S3 resources (p. 794).
2. Complete the steps in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).
3. Complete the steps in Associating an IAM role with an Amazon Aurora MySQL DB cluster (p. 800).

Backing up files to be restored as an Amazon Aurora MySQL DB cluster

You can create a full backup of your MySQL database files using Percona XtraBackup and upload the backup files to an Amazon S3 bucket. Alternatively, if you already use Percona XtraBackup to back up your MySQL database files, you can upload your existing full and incremental backup directories and files to an Amazon S3 bucket.

Creating a full backup with Percona XtraBackup

To create a full backup of your MySQL database files that can be restored from Amazon S3 to create an Amazon Aurora MySQL DB cluster, use the Percona XtraBackup utility (xtrabackup) to back up your database.

For example, the following command creates a backup of a MySQL database and stores the files in the /on-premises/s3-restore/backup folder.

```
xtrabackup --backup --user=<myuser> --password=<password> --target-dir=/on-premises/s3-restore/backup
```

If you want to compress your backup into a single file (which can be split, if needed), you can use the --stream option to save your backup in one of the following formats:

- Gzip (.gz)
- tar (.tar)
- Percona xbstream (.xbstream)

The following command creates a backup of your MySQL database split into multiple Gzip files.

```
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/*.tar.gz
```

The following command creates a backup of your MySQL database split into multiple tar files.
The following command creates a backup of your MySQL database split into multiple xbstream files.

```
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
```

Once you have backed up your MySQL database using the Percona XtraBackup utility, you can copy your backup directories and files to an Amazon S3 bucket.

For information on creating and uploading a file to an Amazon S3 bucket, see Getting started with Amazon Simple Storage Service in the Amazon S3 Getting Started Guide.

Using incremental backups with Percona XtraBackup

Amazon Aurora MySQL supports both full and incremental backups created using Percona XtraBackup. If you already use Percona XtraBackup to perform full and incremental backups of your MySQL database files, you don't need to create a full backup and upload the backup files to Amazon S3. Instead, you can save a significant amount of time by copying your existing backup directories and files for your full and incremental backups to an Amazon S3 bucket. For more information about creating incremental backups using Percona XtraBackup, see Incremental backup.

When copying your existing full and incremental backup files to an Amazon S3 bucket, you must recursively copy the contents of the base directory. Those contents include the full backup and also all incremental backup directories and files. This copy must preserve the directory structure in the Amazon S3 bucket. Aurora iterates through all files and directories. Aurora uses the xtrabackup-checkpoints file included with each incremental backup to identify the base directory and to order incremental backups by log sequence number (LSN) range.

For information on creating and uploading a file to an Amazon S3 bucket, see Getting started with Amazon Simple Storage Service in the Amazon S3 Getting Started Guide.

Backup considerations

When you upload a file to an Amazon S3 bucket, you can use server-side encryption to encrypt the data. You can then restore an Amazon Aurora MySQL DB cluster from those encrypted files. Amazon Aurora MySQL can restore a DB cluster with files encrypted using the following types of server-side encryption:

- Server-side encryption with Amazon S3–managed keys (SSE-S3) – Each object is encrypted with a unique key employing strong multifactor encryption.
- Server-side encryption with AWS KMS–managed keys (SSE-KMS) – Similar to SSE-S3, but you have the option to create and manage encryption keys yourself, and also other differences.

For information about using server-side encryption when uploading files to an Amazon S3 bucket, see Protecting data using server-side encryption in the Amazon S3 Developer Guide.

Amazon S3 limits the size of a file uploaded to an Amazon S3 bucket to 5 TB. If the backup data for your database exceeds 5 TB, use the `split` command to split the backup files into multiple files that are each less than 5 TB.

Aurora limits the number of source files uploaded to an Amazon S3 bucket to 1 million files. In some cases, backup data for your database, including all full and incremental backups, can come to a large number of files. In these cases, use a tarball (.tar.gz) file to store full and incremental backup files in the Amazon S3 bucket.
Aurora consumes your backup files based on the file name. Be sure to name your backup files with the appropriate file extension based on the file format—for example, `.xbstream` for files stored using the Percona xbstream format.

Aurora consumes your backup files in alphabetical order and also in natural number order. Always use the `split` option when you issue the `xtrabackup` command to ensure that your backup files are written and named in the proper order.

Aurora doesn't support partial backups created using Percona XtraBackup. You can't use the following options to create a partial backup when you back up the source files for your database: `--tables`, `--tables-exclude`, `--tables-file`, `--databases`, `--databases-exclude`, or `--databases-file`.

For more information about backing up your database with Percona XtraBackup, see Percona XtraBackup documentation and The xtrabackup binary on the Percona website.

Aurora supports incremental backups created using Percona XtraBackup. For more information about creating incremental backups using Percona XtraBackup, see Incremental backup.

**Restoring an Amazon Aurora MySQL DB cluster from an Amazon S3 bucket**

You can restore your backup files from your Amazon S3 bucket to create a new Amazon Aurora MySQL DB cluster by using the Amazon RDS console.

**To restore an Amazon Aurora MySQL DB cluster from files on an Amazon S3 bucket**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the top right corner of the Amazon RDS console, choose the AWS Region in which to create your DB cluster. Choose the same AWS Region as the Amazon S3 bucket that contains your database backup.
3. In the navigation pane, choose Databases, and then choose Restore from S3.
4. Choose Restore from S3.

   The Create database by restoring from S3 page appears.
5. **Under S3 destination:**
   a. Choose the S3 bucket where to write audit logs.
   b. (Optional) For **S3 folder path prefix**, enter a file path prefix for the files stored in your Amazon S3 bucket.

   If you don’t specify a prefix, then RDS creates your DB instance using all of the files and folders in the root folder of the S3 bucket. If you do specify a prefix, then RDS creates your DB instance using the files and folders in the S3 bucket where the path for the file begins with the specified prefix.

   For example, suppose that you store your backup files on S3 in a subfolder named backups, and you have multiple sets of backup files, each in its own directory (gzip_backup1, gzip_backup2, and so on). In this case, you specify a prefix of backups/gzip_backup1 to restore from the files in the gzip_backup1 folder.

6. **Under Engine options:**
   a. For **Engine type**, choose Amazon Aurora.
   b. For **Version**, choose the Aurora MySQL engine version for your restored DB instance.

7. For **IAM role**, you can choose an existing IAM role.

8. (Optional) You can also have a new IAM role created for you by choosing **Create a new role**. If so:
   a. Enter the **IAM role name**.
   b. Choose whether to allow access to KMS key:
      - If you didn’t encrypt the backup files, choose No.
      - If you encrypted the backup files with AES-256 (SSE-S3) when you uploaded them to Amazon S3, choose No. In this case, the data is decrypted automatically.
      - If you encrypted the backup files with AWS-KMS (SSE-KMS) server-side encryption when you uploaded them to Amazon S3, choose Yes. Next, choose the correct master key for **Master key**.

      The AWS Management Console creates an IAM policy that enables Aurora to decrypt the data.

      For more information, see **Protecting data using server-side encryption** in the Amazon S3 Developer Guide.

9. Choose settings for your DB cluster, such as the DB cluster identifier and the login credentials. For information about each setting, see **Settings for Aurora DB clusters** (p. 128).

10. Customize additional settings for your Aurora MySQL DB cluster as needed.

11. Choose **Create database** to launch your Aurora DB instance.

On the Amazon RDS console, the new DB instance appears in the list of DB instances. The DB instance has a status of **creating** until the DB instance is created and ready for use. When the state changes to **available**, you can connect to the primary instance for your DB cluster. Depending on the DB instance class and store allocated, it can take several minutes for the new instance to be available.

To view the newly created cluster, choose the **Databases** view in the Amazon RDS console and choose the DB cluster. For more information, see **Viewing an Amazon Aurora DB cluster** (p. 473).
Note the port and the writer endpoint of the DB cluster. Use the writer endpoint and port of the DB cluster in your JDBC and ODBC connection strings for any application that performs write or read operations.

**Synchronizing the Amazon Aurora MySQL DB cluster with the MySQL database using replication**

To achieve little or no downtime during the migration, you can replicate transactions that were committed on your MySQL database to your Aurora MySQL DB cluster. Replication enables the DB cluster to catch up with the transactions on the MySQL database that happened during the migration. When the DB cluster is completely caught up, you can stop the replication and finish the migration to Aurora MySQL.

**Topics**
- Configuring your external MySQL database and your Aurora MySQL DB cluster for encrypted replication (p. 655)
• Synchronizing the Amazon Aurora MySQL DB cluster with the external MySQL database (p. 656)

Configuring your external MySQL database and your Aurora MySQL DB cluster for encrypted replication

To replicate data securely, you can use encrypted replication.

**Note**
If you don’t need to use encrypted replication, you can skip these steps and move on to the instructions in Synchronizing the Amazon Aurora MySQL DB cluster with the external MySQL database (p. 656).

The following are prerequisites for using encrypted replication:

- Secure Sockets Layer (SSL) must be enabled on the external MySQL primary database.
- A client key and client certificate must be prepared for the Aurora MySQL DB cluster.

During encrypted replication, the Aurora MySQL DB cluster acts a client to the MySQL database server. The certificates and keys for the Aurora MySQL client are in files in .pem format.

**To configure your external MySQL database and your Aurora MySQL DB cluster for encrypted replication**

1. Ensure that you are prepared for encrypted replication:
   - If you don’t have SSL enabled on the external MySQL primary database and don’t have a client key and client certificate prepared, enable SSL on the MySQL database server and generate the required client key and client certificate.
   - If SSL is enabled on the external primary, supply a client key and certificate for the Aurora MySQL DB cluster. If you don’t have these, generate a new key and certificate for the Aurora MySQL DB cluster. To sign the client certificate, you must have the certificate authority key that you used to configure SSL on the external MySQL primary database.
   - For more information, see Creating SSL certificates and keys using openssl in the MySQL documentation.
     You need the certificate authority certificate, the client key, and the client certificate.

2. Connect to the Aurora MySQL DB cluster as the primary user using SSL.
   - For information about connecting to an Aurora MySQL DB cluster with SSL, see Using SSL/TLS with Aurora MySQL DB clusters (p. 638).

3. Run the `mysql.rds_import_binlog_ssl_material` stored procedure to import the SSL information into the Aurora MySQL DB cluster.
   - For the `ssl_material_value` parameter, insert the information from the .pem format files for the Aurora MySQL DB cluster in the correct JSON payload.
     The following example imports SSL information into an Aurora MySQL DB cluster. In .pem format files, the body code typically is longer than the body code shown in the example.

```sql
CALL mysql.rds_import_binlog_ssl_material(
  '{"ssl_ca":"-----BEGIN CERTIFICATE-----
AAAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhcE53pcj9P3maAhDFcvB5706V
h2ZltxC1h-PnGUSuAw+WNQn/mZphTk/a/gU8jEzoGWbkn淤xayb/w86xbiFveSFjpQp/d6RJhJ0I0iBXr
la8nBfntctki37PbxJXrLvwwJryDUIlbMTY7twB+QhYUNXcze65ijb/186eJtjnV3iAoG/cQk+0FoZ
qaeJIAHco+CY/5WrbkrNhFzrHcKxwJhWPKyQS5xzqC+PwUIofz221CBI5lMucxXPkXirW1+s7wB3Rb
BQaOQzd8v7yeb70zlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE

-----END CERTIFICATE-----
"}');
```

655
For more information, see `mysql_rds_import_binlog_ssl_material` using SSL/TLS with Aurora MySQL DB clusters (p. 638).

Note
After running the procedure, the secrets are stored in files. To erase the files later, you can run the `mysql_rds_remove_binlog_ssl_material` stored procedure.

Synchronizing the Amazon Aurora MySQL DB cluster with the external MySQL database

You can synchronize your Amazon Aurora MySQL DB cluster with the MySQL database using replication.

To synchronize your Aurora MySQL DB cluster with the MySQL database using replication

1. Ensure that the `/etc/my.cnf` file for the external MySQL database has the relevant entries.

   If encrypted replication is not required, ensure that the external MySQL database is started with binary logs (binlogs) enabled and SSL disabled. The following are the relevant entries in the `/etc/my.cnf` file for unencrypted data.

   ```
   log-bin=mysql-bin
   server-id=2133421
   innodb_flush_log_at_trx_commit=1
   sync_binlog=1
   ```

   If encrypted replication is required, ensure that the external MySQL database is started with SSL and binlogs enabled. The entries in the `/etc/my.cnf` file include the .pem file locations for the MySQL database server.

   ```
   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
   ```

   You can verify that SSL is enabled with the following command.

   ```
   mysql> show variables like 'have_ssl';
   ```
2. Determine the starting binary log position for replication:
   a. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
   b. In the navigation pane, choose Events.
   c. In the Events list, note the position in the Recovered from Binary log filename event.

   ![Events](image)

   You specify the position to start replication in a later step.

3. While connected to the external MySQL database, create a user to be used for replication. This account is used solely for replication and must be restricted to your domain to improve security. The following is an example.

   ```
   mysql> CREATE USER '<user_name>'@'<domain_name>' IDENTIFIED BY '<password>'; 
   ```

   The user requires the REPLICATION CLIENT and REPLICATION SLAVE privileges. Grant these privileges to the user.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO '<user_name>'@'<domain_name>'; 
   ```

   If you need to use encrypted replication, require SSL connections for the replication user. For example, you can use the following statement to require SSL connections on the user account <user_name>.

   ```
   GRANT USAGE ON *.* TO '<user_name>'@'<domain_name>' REQUIRE SSL; 
   ```

   **Note**
   If REQUIRE SSL is not included, the replication connection might silently fall back to an unencrypted connection.
4. In the Amazon RDS console, add the IP address of the server that hosts the external MySQL database to the VPC security group for the Aurora MySQL DB cluster. For more information on modifying a VPC security group, see Security groups for your VPC in the Amazon Virtual Private Cloud User Guide.

You might also need to configure your local network to permit connections from the IP address of your Aurora MySQL DB cluster, so that it can communicate with your external MySQL database. To find the IP address of the Aurora MySQL DB cluster, use the `host` command.

```
host <db_cluster_endpoint>
```

The host name is the DNS name from the Aurora MySQL DB cluster endpoint.

5. Enable binary log replication by running the `mysql.rds_set_external_master` stored procedure. This stored procedure has the following 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
);
```

For information about the parameters, see `mysql_rds_set_external_master`.

For `mysql_binary_log_file_name` and `mysql_binary_log_file_location`, use the position in the `Recovered from Binary log filename` event you noted earlier.

If the data in the Aurora MySQL DB cluster is not encrypted, the `ssl_encryption` parameter must be set to 0. If the data is encrypted, the `ssl_encryption` parameter must be set to 1.

The following example runs the procedure for an Aurora MySQL DB cluster that has encrypted data.

```
CALL mysql.rds_set_external_master(
    'Externaldb.some.com',
    3306,
    'repl_user'@'mydomain.com',
    'password',
    'mysql-bin.000010',
    120,
    1);
```

This stored procedure sets the parameters that the Aurora MySQL DB cluster uses for connecting to the external MySQL database and reading its binary log. If the data is encrypted, it also downloads the SSL certificate authority certificate, client certificate, and client key to the local disk.

6. Start binary log replication by running the `mysql.rds_start_replication` stored procedure.

```
CALL mysql.rds_start_replication;
```

7. Monitor how far the Aurora MySQL DB cluster is behind the MySQL replication primary database. To do so, connect to the Aurora MySQL DB cluster and run the following command.
SHOW SLAVE STATUS;

In the command output, the `Seconds Behind Master` field shows how far the Aurora MySQL DB cluster is behind the MySQL primary. When this value is 0 (zero), the Aurora MySQL DB cluster has caught up to the primary, and you can move on to the next step to stop replication.

8. Connect to the MySQL replication primary database and stop replication. To do so, run the following command.

```sql
CALL mysql.rds_stop_replication;
```

### Migrating from MySQL to Amazon Aurora by using mysqldump

Because Amazon Aurora MySQL is a MySQL-compatible database, you can use the `mysqldump` utility to copy data from your MySQL or MariaDB database to an existing Aurora MySQL DB cluster.

For a discussion of how to do so with MySQL databases that are very large, see [Importing data to an Amazon RDS MySQL or MariaDB DB instance with reduced downtime](#). For MySQL databases that have smaller amounts of data, see [Importing data from a MySQL or MariaDB DB to an Amazon RDS MySQL or MariaDB DB instance](#).

### Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using a DB snapshot

You can migrate (copy) data to an Amazon Aurora MySQL DB cluster from an Amazon RDS MySQL DB snapshot, as described following.

**Topics**
- Migrating an RDS MySQL snapshot to Aurora (p. 659)
- Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using an Aurora read replica (p. 666)

**Note**
Because Amazon Aurora MySQL is compatible with MySQL, you can migrate data from your MySQL database by setting up replication between your MySQL database and an Amazon Aurora MySQL DB cluster. If you want to use replication to migrate data from your MySQL database, we recommend that your MySQL database run MySQL version 5.5 or later. For more information, see [Replication with Amazon Aurora](#).

### Migrating an RDS MySQL snapshot to Aurora

You can migrate a DB snapshot of an Amazon RDS MySQL DB instance to create an Aurora MySQL DB cluster. The new Aurora MySQL DB cluster is populated with the data from the original Amazon RDS MySQL DB instance. The DB snapshot must have been made from an Amazon RDS DB instance running MySQL version 5.6 or 5.7.

You can migrate either a manual or automated DB snapshot. After the DB cluster is created, you can then create optional Aurora Replicas.
When the MySQL DB instance and the Aurora DB cluster are running the same version of MySQL, you can restore the MySQL snapshot directly to the Aurora DB cluster. For example, you can restore a MySQL version 5.6 snapshot directly to Aurora MySQL version 5.6, but you can't restore a MySQL version 5.6 snapshot directly to Aurora MySQL version 5.7.

If you want to migrate a MySQL version 5.6 snapshot to Aurora MySQL version 5.7, you can perform the migration in one of the following ways:

- Migrate the MySQL version 5.6 snapshot to Aurora MySQL version 5.6, take a snapshot of the Aurora MySQL version 5.6 DB cluster, and then restore the Aurora MySQL version 5.6 snapshot to Aurora MySQL version 5.7.
- Upgrade the MySQL version 5.6 snapshot to MySQL version 5.7, take a snapshot of the MySQL version 5.7 DB instance, and then restore the MySQL version 5.7 snapshot to Aurora MySQL version 5.7.

**Note**
You can also migrate a MySQL DB instance to an Aurora MySQL DB cluster by creating an Aurora read replica of your source MySQL DB instance. For more information, see Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using an Aurora read replica (p. 666).

You can't migrate a MySQL version 5.7 snapshot to Aurora MySQL version 5.6.

The general steps you must take are as follows:

1. Determine the amount of space to provision for your Aurora MySQL DB cluster. For more information, see How much space do I need? (p. 660)
2. Use the console to create the snapshot in the AWS Region where the Amazon RDS MySQL instance is located. For information about creating a DB snapshot, see Creating a DB snapshot.
3. If the DB snapshot is not in the same AWS Region as your DB cluster, use the Amazon RDS console to copy the DB snapshot to that AWS Region. For information about copying a DB snapshot, see Copying a DB snapshot.
4. Use the console to migrate the DB snapshot and create an Aurora MySQL DB cluster with the same databases as the original MySQL DB instance.

**Warning**
Amazon RDS limits each AWS account to one snapshot copy into each AWS Region at a time.

**How much space do I need?**

When you migrate a snapshot of a MySQL DB instance into an Aurora MySQL DB cluster, Aurora uses an Amazon Elastic Block Store (Amazon EBS) volume to format the data from the snapshot before migrating it. In some cases, additional space is needed to format the data for migration.

Tables that are not MyISAM tables and are not compressed can be up to 16 TB in size. If you have MyISAM tables, then Aurora must use additional space in the volume to convert the tables to be compatible with Aurora MySQL. If you have compressed tables, then Aurora must use additional space in the volume to expand these tables before storing them on the Aurora cluster volume. Because of this additional space requirement, you should ensure that none of the MyISAM and compressed tables being migrated from your MySQL DB instance exceeds 8 TB in size.

**Reducing the amount of space required to migrate data into Amazon Aurora MySQL**

You might want to modify your database schema prior to migrating it into Amazon Aurora. Such modification can be helpful in the following cases:
• You want to speed up the migration process.
• You are unsure of how much space you need to provision.
• You have attempted to migrate your data and the migration has failed due to a lack of provisioned space.

You can make the following changes to improve the process of migrating a database into Amazon Aurora.

**Important**
Be sure to perform these updates on a new DB instance restored from a snapshot of a production database, rather than on a production instance. You can then migrate the data from the snapshot of your new DB instance into your Aurora DB cluster to avoid any service interruptions on your production database.

<table>
<thead>
<tr>
<th>Table type</th>
<th>Limitation or guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyISAM tables</td>
<td>Aurora MySQL supports InnoDB tables only. If you have MyISAM tables in your database, then those tables must be converted before being migrated into Aurora MySQL. The conversion process requires additional space for the MyISAM to InnoDB conversion during the migration procedure. To reduce your chances of running out of space or to speed up the migration process, convert all of your MyISAM tables to InnoDB tables before migrating them. The size of the resulting InnoDB table is equivalent to the size required by Aurora MySQL for that table. To convert a MyISAM table to InnoDB, run the following command: alter table &lt;schema&gt;.&lt;table_name&gt; engine=innodb, algorithm=copy;</td>
</tr>
<tr>
<td>Compressed tables</td>
<td>Aurora MySQL doesn’t support compressed tables (that is, tables created with ROW_FORMAT=COMPRESSED). To reduce your chances of running out of space or to speed up the migration process, expand your compressed tables by setting ROW_FORMAT to DEFAULT, COMPACT, DYNAMIC, or REDUNDANT. For more information, see <a href="https://dev.mysql.com/doc/refman/5.6/en/innodb-row-format.html">https://dev.mysql.com/doc/refman/5.6/en/innodb-row-format.html</a>.</td>
</tr>
</tbody>
</table>

You can use the following SQL script on your existing MySQL DB instance to list the tables in your database that are MyISAM tables or compressed tables.

```sql
-- 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. ' +
  '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
  or (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
  or (ROW_FORMAT = 'Compressed');

The script produces output similar to the output in the following example. The example shows two
tables that must be converted from MyISAM to InnoDB. The output also includes the approximate size of
each table in megabytes (MB).

<table>
<thead>
<tr>
<th>==&gt; MyISAM or Compressed Tables</th>
<th>Approx size (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>test.name_table</td>
<td>2102.25</td>
</tr>
<tr>
<td>test.my_table</td>
<td>65.25</td>
</tr>
</tbody>
</table>

2 rows in set (0.01 sec)

**Console**

You can migrate a DB snapshot of an Amazon RDS MySQL DB instance to create an Aurora MySQL DB
cluster. The new Aurora MySQL DB cluster is populated with the data from the original Amazon RDS
MySQL DB instance. The DB snapshot must have been made from an Amazon RDS DB instance running
MySQL version 5.6 or 5.7. For information about creating a DB snapshot, see Creating a DB snapshot.

If the DB snapshot is not in the AWS Region where you want to locate your data, use the Amazon RDS
console to copy the DB snapshot to that AWS Region. For information about copying a DB snapshot, see
Copying a DB snapshot.
When you migrate the DB snapshot by using the AWS Management Console, the console takes the actions necessary to create both the DB cluster and the primary instance.

You can also choose for your new Aurora MySQL DB cluster to be encrypted at rest using an AWS Key Management Service (AWS KMS) customer master key (CMK).

**To migrate a MySQL DB snapshot by using the AWS Management Console**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Either start the migration from the MySQL DB instance or from the snapshot:
   - To start the migration from the DB instance:
     1. In the navigation pane, choose **Databases**, and then select the MySQL DB instance.
     2. For **Actions**, choose **Migrate latest snapshot**.
   - To start the migration from the snapshot:
     1. Choose **Snapshots**.
     2. On the **Snapshots** page, choose the snapshot that you want to migrate into an Aurora MySQL DB cluster.
     3. Choose **Snapshot Actions**, and then choose **Migrate Snapshot**.

   The **Migrate Database** page appears.

3. Set the following values on the **Migrate Database** page:
   - **Migrate to DB Engine**: Select `aurora`.
   - **DB Engine Version**: Select the DB engine version for the Aurora MySQL DB cluster.
   - **DB Instance Class**: Select a DB instance class that has the required storage and capacity for your database, for example `db.r3.large`. Aurora cluster volumes automatically grow as the amount of data in your database increases. An Aurora cluster volume can grow to a maximum size of 128 tebibytes (TiB). So you only need to select a DB instance class that meets your current storage requirements. For more information, see Overview of Aurora storage (p. 51).
   - **DB Instance Identifier**: Type a name for the DB cluster that is unique for your account in the AWS Region you selected. This identifier is used in the endpoint addresses for the instances in your DB cluster. You might choose to add some intelligence to the name, such as including the AWS Region and DB engine you selected, for example `aurora-cluster1`.

   The DB instance identifier has the following constraints:
   - It must contain from 1 to 63 alphanumeric characters or hyphens.
   - Its first character must be a letter.
   - It cannot end with a hyphen or contain two consecutive hyphens.
   - It must be unique for all DB instances per AWS account, per AWS Region.
   - **Virtual Private Cloud (VPC)**: If you have an existing VPC, then you can use that VPC with your Aurora MySQL DB cluster by selecting your VPC identifier, for example `vpc-a464d1c1`. For information on using an existing VPC, see How to create a VPC for use with Amazon Aurora (p. 1281).

   Otherwise, you can choose to have Aurora create a VPC for you by selecting **Create a new VPC**.
   - **Subnet group**: If you have an existing subnet group, then you can use that subnet group with your Aurora MySQL DB cluster by selecting your subnet group identifier, for example `gs-subnet-group1`.
Otherwise, you can choose to have Aurora create a subnet group for you by selecting Create a new subnet group.

- **Public accessibility**: Select No to specify that instances in your DB cluster can only be accessed by resources inside of your VPC. Select Yes to specify that instances in your DB cluster can be accessed by resources on the public network. The default is Yes.

  **Note**
  Your production DB cluster might not need to be in a public subnet, because only your application servers require access to your DB cluster. If your DB cluster doesn't need to be in a public subnet, set Publicly Accessible to No.

- **Availability Zone**: Select the Availability Zone to host the primary instance for your Aurora MySQL DB cluster. To have Aurora select an Availability Zone for you, select No Preference.

- **Database Port**: Type the default port to be used when connecting to instances in the Aurora MySQL DB cluster. The default is 3306.

  **Note**
  You might be behind a corporate firewall that doesn't allow access to default ports such as the MySQL default port, 3306. In this case, provide a port value that your corporate firewall allows. Remember that port value later when you connect to the Aurora MySQL DB cluster.

- **Encryption**: Choose Enable Encryption for your new Aurora MySQL DB cluster to be encrypted at rest. If you choose Enable Encryption, you must choose an AWS KMS customer master key (CMK) as the Master Key value.

  If your DB snapshot isn't encrypted, specify an encryption key to have your DB cluster encrypted at rest.

  If your DB snapshot is encrypted, specify an encryption key to have your DB cluster encrypted at rest using the specified encryption key. You can specify the encryption key used by the DB snapshot or a different key. You can't create an unencrypted DB cluster from an encrypted DB snapshot.

- **Auto Minor Version Upgrade**: This setting doesn't apply to Aurora MySQL DB clusters.

  For more information about engine updates for Aurora MySQL, see Database engine updates for Amazon Aurora MySQL (p. 874).

4. Choose Migrate to migrate your DB snapshot.

5. Choose Instances, and then choose the arrow icon to show the DB cluster details and monitor the progress of the migration. On the details page, you can find the cluster endpoint used to connect to the primary instance of the DB cluster. For more information on connecting to an Aurora MySQL DB cluster, see Connecting to an Amazon Aurora DB cluster (p. 253).

**AWS CLI**

You can migrate a DB snapshot of an Amazon RDS MySQL DB instance to create an Aurora DB cluster. The new DB cluster is then populated with the data from the DB snapshot. The DB snapshot must come from an Amazon RDS DB instance running MySQL version 5.6 or 5.7. For more information, see Creating a DB snapshot.

If the DB snapshot is not in the AWS Region where you want to locate your data, copy the DB snapshot to that AWS Region. For more information, see Copying a DB snapshot.

You can create an Aurora DB cluster from a DB snapshot of an Amazon RDS MySQL DB instance by using the restore-db-cluster-from-snapshot command with the following parameters:

- `--db-cluster-identifier`
The name of the DB cluster to create.

- Either `--engine aurora-mysql` for a MySQL 5.7–compatible DB cluster, or `--engine aurora` for a MySQL 5.6–compatible DB cluster
- `--kms-key-id`

The AWS Key Management Service (AWS KMS) customer master key (CMK) to optionally encrypt the DB cluster with, depending on whether your DB snapshot is encrypted.

- If your DB snapshot isn't encrypted, specify an encryption key to have your DB cluster encrypted at rest. Otherwise, your DB cluster isn't encrypted.
- If your DB snapshot is encrypted, specify an encryption key to have your DB cluster encrypted at rest using the specified encryption key. Otherwise, your DB cluster is encrypted at rest using the encryption key for the DB snapshot.

**Note**

You can't create an unencrypted DB cluster from an encrypted DB snapshot.

- `--snapshot-identifier`

The Amazon Resource Name (ARN) of the DB snapshot to migrate. For more information about Amazon RDS ARNs, see Amazon Relational Database Service (Amazon RDS).

When you migrate the DB snapshot by using the `restore-db-cluster-from-snapshot` command, the command creates both the DB cluster and the primary instance.

In this example, you create a MySQL 5.7–compatible DB cluster named `mydbcluster` from a DB snapshot with an ARN set to `mydbsnapshotARN`.

For Linux, macOS, or Unix:

```
aws rds restore-db-cluster-from-snapshot \
  --db-cluster-identifier mydbcluster \
  --snapshot-identifier mydbsnapshotARN \
  --engine aurora-mysql
```

For Windows:

```
aws rds restore-db-cluster-from-snapshot ^
  --db-cluster-identifier mydbcluster ^
  --snapshot-identifier mydbsnapshotARN ^
  --engine aurora-mysql
```

In this example, you create a MySQL 5.6–compatible DB cluster named `mydbcluster` from a DB snapshot with an ARN set to `mydbsnapshotARN`.

For Linux, macOS, or Unix:

```
aws rds restore-db-cluster-from-snapshot \
  --db-cluster-identifier mydbcluster \
  --snapshot-identifier mydbsnapshotARN \
  --engine aurora
```

For Windows:

```
aws rds restore-db-cluster-from-snapshot ^
  --db-cluster-identifier mydbcluster ^
  --snapshot-identifier mydbsnapshotARN ^
  --engine aurora
```
Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using an Aurora read replica

Aurora uses the MySQL DB engines' binary log replication functionality to create a special type of DB cluster called an Aurora read replica for a source MySQL DB instance. Updates made to the source MySQL DB instance are asynchronously replicated to the Aurora read replica.

We recommend using this functionality to migrate from a MySQL DB instance to an Aurora MySQL DB cluster by creating an Aurora read replica of your source MySQL DB instance. When the replica lag between the MySQL DB instance and the Aurora read replica is 0, you can direct your client applications to the Aurora read replica and then stop replication to make the Aurora read replica a standalone Aurora MySQL DB cluster. Be prepared for migration to take a while, roughly several hours per tebibyte (TiB) of data.

For a list of regions where Aurora is available, see Amazon Aurora in the AWS General Reference.

When you create an Aurora read replica of a MySQL DB instance, Amazon RDS creates a DB snapshot of your source MySQL DB instance (private to Amazon RDS, and incurring no charges). Amazon RDS then migrates the data from the DB snapshot to the Aurora read replica. After the data from the DB snapshot has been migrated to the new Aurora MySQL DB cluster, Amazon RDS starts replication between your MySQL DB instance and the Aurora MySQL DB cluster. If your MySQL DB instance contains tables that use storage engines other than InnoDB, or that use compressed row format, you can speed up the process of creating an Aurora read replica by altering those tables to use the InnoDB storage engine and dynamic row format before you create your Aurora read replica. For more information about the process of copying a MySQL DB snapshot to an Aurora MySQL DB cluster, see Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using a DB snapshot (p. 659).

You can only have one Aurora read replica for a MySQL DB instance.

**Note**

Replication issues can arise due to feature differences between Amazon Aurora MySQL and the MySQL database engine version of your RDS MySQL DB instance that is the replication primary. If you encounter an error, you can find help in the Amazon RDS community forum or by contacting AWS Support.

For more information on MySQL read replicas, see Working with read replicas of MariaDB, MySQL, and PostgreSQL DB instances.

Creating an Aurora read replica

You can create an Aurora read replica for a MySQL DB instance by using the console or the AWS CLI.

**Console**

**To create an Aurora read replica from a source MySQL DB instance**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the MySQL DB instance that you want to use as the source for your Aurora read replica.
4. For Actions, choose Create Aurora read replica.
5. Choose the DB cluster specifications you want to use for the Aurora read replica, as described in the following table.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB instance class</td>
<td>Choose a DB instance class that defines the processing and memory requirements for the primary instance in the DB cluster. For more information about DB instance class options, see DB instance classes (p. 46).</td>
</tr>
<tr>
<td>Multi-AZ deployment</td>
<td>Choose <strong>Create Replica in Different Zone</strong> to create a standby replica of the new DB cluster in another Availability Zone in the target AWS Region for failover support. For more information about multiple Availability Zones, see Regions and Availability Zones (p. 5).</td>
</tr>
<tr>
<td>DB instance identifier</td>
<td>Type a name for the primary instance in your Aurora read replica DB cluster. This identifier is used in the endpoint address for the primary instance of the new DB cluster.</td>
</tr>
<tr>
<td></td>
<td>The DB instance identifier has the following constraints:</td>
</tr>
<tr>
<td></td>
<td>• It must contain from 1 to 63 alphanumeric characters or hyphens.</td>
</tr>
<tr>
<td></td>
<td>• Its first character must be a letter.</td>
</tr>
<tr>
<td></td>
<td>• It cannot end with a hyphen or contain two consecutive hyphens.</td>
</tr>
<tr>
<td></td>
<td>• It must be unique for all DB instances for each AWS account, for each AWS Region.</td>
</tr>
<tr>
<td></td>
<td>Because the Aurora read replica DB cluster is created from a snapshot of the source DB instance, the master user name and master password for the Aurora read replica are the same as the master user name and master password for the source DB instance.</td>
</tr>
<tr>
<td>Virtual Private Cloud (VPC)</td>
<td>Select the VPC to host the DB cluster. Select <strong>Create new VPC</strong> to have Aurora create a VPC for you. For more information, see DB cluster prerequisites (p. 118).</td>
</tr>
<tr>
<td>Subnet group</td>
<td>Select the DB subnet group to use for the DB cluster. Select <strong>Create new DB subnet group</strong> to have Aurora create a DB subnet group for you. For more information, see DB cluster prerequisites (p. 118).</td>
</tr>
<tr>
<td>Public accessibility</td>
<td>Select <strong>Yes</strong> to give the DB cluster a public IP address; otherwise, select <strong>No</strong>. The instances in your DB cluster can be a mix of both public and private DB instances. For more information about hiding instances from public access, see Hiding a DB instance in a VPC from the internet (p. 1293).</td>
</tr>
<tr>
<td>Availability zone</td>
<td>Determine if you want to specify a particular Availability Zone. For more information about Availability Zones, see Regions and Availability Zones (p. 5).</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VPC security groups</td>
<td>Select <a href="#">Create new VPC security group</a> to have Aurora create a VPC security group for you. Select <a href="#">Select existing VPC security groups</a> to specify one or more VPC security groups to secure network access to the DB cluster. For more information, see <a href="#">DB cluster prerequisites</a>.</td>
</tr>
<tr>
<td>Database port</td>
<td>Specify the port for applications and utilities to use to access the database. Aurora MySQL DB clusters default to the default MySQL port, 3306. Firewalls at some companies block connections to this port. If your company firewall blocks the default port, choose another port for the new DB cluster.</td>
</tr>
<tr>
<td>DB parameter group</td>
<td>Select a DB parameter group for the Aurora MySQL DB cluster. Aurora has a default DB parameter group you can use, or you can create your own DB parameter group. For more information about DB parameter groups, see <a href="#">Working with DB parameter groups and DB cluster parameter groups</a>.</td>
</tr>
<tr>
<td>DB cluster parameter group</td>
<td>Select a DB cluster parameter group for the Aurora MySQL DB cluster. Aurora has a default DB cluster parameter group you can use, or you can create your own DB cluster parameter group. For more information about DB cluster parameter groups, see <a href="#">Working with DB parameter groups and DB cluster parameter groups</a>.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Choose <a href="#">Disable encryption</a> if you don't want your new Aurora DB cluster to be encrypted. Choose <a href="#">Enable encryption</a> for your new Aurora DB cluster to be encrypted at rest. If you choose Enable encryption, you must choose an AWS KMS customer master key (CMK) as the Master key value. If your MySQL DB instance isn't encrypted, specify an encryption key to have your DB cluster encrypted at rest. If your MySQL DB instance is encrypted, specify an encryption key to have your DB cluster encrypted at rest using the specified encryption key. You can specify the encryption key used by the MySQL DB instance or a different key. You can't create an unencrypted DB cluster from an encrypted MySQL DB instance.</td>
</tr>
<tr>
<td>Priority</td>
<td>Choose a failover priority for the DB cluster. If you don't select a value, the default is tier-1. This priority determines the order in which Aurora Replicas are promoted when recovering from a primary instance failure. For more information, see <a href="#">Fault tolerance for an Aurora DB cluster</a>.</td>
</tr>
<tr>
<td>Backup retention period</td>
<td>Select the length of time, from 1 to 35 days, that Aurora retains backup copies of the database. Backup copies can be used for point-in-time restores (PITR) of your database down to the second.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enhanced Monitoring</td>
<td>Choose <strong>Enable enhanced monitoring</strong> to enable gathering metrics in real time for the operating system that your DB cluster runs on. For more information, see Enhanced Monitoring (p. 504).</td>
</tr>
<tr>
<td>Monitoring Role</td>
<td>Only available if <strong>Enhanced Monitoring</strong> is set to <strong>Enable enhanced monitoring</strong>. Choose the IAM role that you created to permit Aurora to communicate with Amazon CloudWatch Logs for you, or choose <strong>Default</strong> to have Aurora create a role for you named <strong>rds-monitoring-role</strong>. For more information, see Enhanced Monitoring (p. 504).</td>
</tr>
<tr>
<td>Granularity</td>
<td>Only available if <strong>Enhanced Monitoring</strong> is set to <strong>Enable enhanced monitoring</strong>. Set the interval, in seconds, between when metrics are collected for your DB cluster.</td>
</tr>
<tr>
<td>Auto minor version upgrade</td>
<td>This setting doesn't apply to Aurora MySQL DB clusters. For more information about engine updates for Aurora MySQL, see Database engine updates for Amazon Aurora MySQL (p. 874).</td>
</tr>
<tr>
<td>Maintenance window</td>
<td>Select <strong>Select window</strong> and specify the weekly time range during which system maintenance can occur. Or, select <strong>No preference</strong> for Aurora to assign a period randomly.</td>
</tr>
</tbody>
</table>

6. Choose **Create read replica**.

**AWS CLI**

To create an Aurora read replica from a source MySQL DB instance, use the `create-db-cluster` and `create-db-instance` AWS CLI commands to create a new Aurora MySQL DB cluster. When you call the `create-db-cluster` command, include the `--replication-source-identifier` parameter to identify the Amazon Resource Name (ARN) for the source MySQL DB instance. For more information about Amazon RDS ARNs, see Amazon Relational Database Service (Amazon RDS).

Don't specify the master username, master password, or database name as the Aurora read replica uses the same master username, master password, and database name as the source MySQL DB instance.

For Linux, macOS, or Unix:

```bash
```

For Windows:

```bash
```

If you use the console to create an Aurora read replica, then Aurora automatically creates the primary instance for your DB cluster Aurora read replica. If you use the AWS CLI to create an Aurora read replica,
you must explicitly create the primary instance for your DB cluster. The primary instance is the first instance that is created in a DB cluster.

You can create a primary instance for your DB cluster by using the `create-db-instance` AWS CLI command with the following parameters.

- `--db-cluster-identifier`  
The name of your DB cluster.
- `--db-instance-class`  
The name of the DB instance class to use for your primary instance.
- `--db-instance-identifier`  
The name of your primary instance.
- `--engine aurora`

In this example, you create a primary instance named `myreadreplicainstance` for the DB cluster named `myreadreplicacluster`, using the DB instance class specified in `myinstanceclass`.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds create-db-instance \
  --db-cluster-identifier myreadreplicacluster \
  --db-instance-class myinstanceclass \
  --db-instance-identifier myreadreplicainstance \
  --engine aurora
```

For Windows:

```bash
aws rds create-db-instance ^
  --db-cluster-identifier myreadreplicacluster ^
  --db-instance-class myinstanceclass ^
  --db-instance-identifier myreadreplicainstance ^
  --engine aurora
```

**RDS API**

To create an Aurora read replica from a source MySQL DB instance, use the `CreateDBCluster` and `CreateDBInstance` Amazon RDS API commands to create a new Aurora DB cluster and primary instance. Do not specify the master username, master password, or database name as the Aurora read replica uses the same master username, master password, and database name as the source MySQL DB instance.

You can create a new Aurora DB cluster for an Aurora read replica from a source MySQL DB instance by using the `CreateDBCluster` Amazon RDS API command with the following parameters:

- `DBClusterIdentifier`  
The name of the DB cluster to create.
- `DBSubnetGroupName`
  
The name of the DB subnet group to associate with this DB cluster.
- `Engine=aurora`
• **KmsKeyId**

The AWS Key Management Service (AWS KMS) customer master key (CMK) to optionally encrypt the DB cluster with, depending on whether your MySQL DB instance is encrypted.

- If your MySQL DB instance isn't encrypted, specify an encryption key to have your DB cluster encrypted at rest. Otherwise, your DB cluster is encrypted at rest using the default encryption key for your account.
- If your MySQL DB instance is encrypted, specify an encryption key to have your DB cluster encrypted at rest using the specified encryption key. Otherwise, your DB cluster is encrypted at rest using the encryption key for the MySQL DB instance.

**Note**

You can't create an unencrypted DB cluster from an encrypted MySQL DB instance.

• **ReplicationSourceIdentifier**

The Amazon Resource Name (ARN) for the source MySQL DB instance. For more information about Amazon RDS ARNs, see [Amazon Relational Database Service (Amazon RDS)](https://aws.amazon.com/rds/).

• **VpcSecurityGroupIds**

The list of EC2 VPC security groups to associate with this DB cluster.

In this example, you create a DB cluster named `myreadreplicaclusternode` from a source MySQL DB instance with an ARN set to `mysqlprimaryARN`, associated with a DB subnet group named `mysubnetgroup` and a VPC security group named `mysecuritygroup`.

**Example**

```url
https://rds.us-east-1.amazonaws.com/
?Action=CreateDBCluster
&DBClusterIdentifier=myreadreplicaclusternode
&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=20150927T162848Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=6a8f4bd6a98fe649c75ea04a6b392eccc75ac0973958391cd7250f5280e716db
```

If you use the console to create an Aurora read replica, then Aurora automatically creates the primary instance for your DB cluster Aurora read replica. If you use the AWS CLI to create an Aurora read replica, you must explicitly create the primary instance for your DB cluster. The primary instance is the first instance that is created in a DB cluster.

You can create a primary instance for your DB cluster by using the `CreateDBInstance` Amazon RDS API command with the following parameters:

- **DBClusterIdentifier**

  The name of your DB cluster.

- **DBInstanceClass**

  The name of the DB instance class to use for your primary instance.

- **DBInstanceIdentifier**
The name of your primary instance.

- Engine=aurora

In this example, you create a primary instance named `myreadreplicainstance` for the DB cluster named `myreadreplicacluster`, using the DB instance class specified in `myinstanceclass`.

**Example**

```plaintext
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=bee4aabc750bf7dad0cd9e22b952bd6089d91e2a16592c2293e532eeab8bc77
```

**Viewing an Aurora read replica**

You can view the MySQL to Aurora MySQL replication relationships for your Aurora MySQL DB clusters by using the AWS Management Console or the AWS CLI.

**Console**

**To view the primary MySQL DB instance for an Aurora read replica**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Databases**.
3. Choose the DB cluster for the Aurora read replica to display its details. The primary MySQL DB instance information is in the **Replication source** field.
To view the MySQL to Aurora MySQL replication relationships for your Aurora MySQL DB clusters by using the AWS CLI, use the `describe-db-clusters` and `describe-db-instances` commands.

To determine which MySQL DB instance is the primary, use the `describe-db-clusters` and specify the cluster identifier of the Aurora read replica for the `--db-cluster-identifier` option. Refer to the `ReplicationSourceIdentifier` element in the output for the ARN of the DB instance that is the replication primary.

To determine which DB cluster is the Aurora read replica, use the `describe-db-instances` and specify the instance identifier of the MySQL DB instance for the `--db-instance-identifier` option. Refer to the `ReadReplicaDBClusterIdentifiers` element in the output for the DB cluster identifier of the Aurora read replica.

**Example**

For Linux, macOS, or Unix:
Promoting an Aurora read replica

After migration completes, you can promote the Aurora read replica to a stand-alone DB cluster and direct your client applications to the endpoint for the Aurora read replica. For more information on the Aurora endpoints, see Amazon Aurora connection management (p. 24). Promotion should complete fairly quickly, and you can read from and write to the Aurora read replica during promotion. However, you can't delete the primary MySQL DB instance or unlink the DB Instance and the Aurora read replica during this time.

Before you promote your Aurora read replica, stop any transactions from being written to the source MySQL DB instance, and then wait for the replica lag on the Aurora read replica to reach 0. You can view the replica lag for an Aurora read replica by calling the `SHOW SLAVE STATUS` command on your Aurora read replica and reading the `Seconds behind master` value.

You can start writing to the Aurora read replica after write transactions to the primary have stopped and replica lag is 0. If you write to the Aurora read replica before this and you modify tables that are also being modified on the MySQL primary, you risk breaking replication to Aurora. If this happens, you must delete and recreate your Aurora read replica.

**Console**

**To promote an Aurora read replica to an Aurora DB cluster**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Databases**.
3. Choose the DB cluster for the Aurora read replica.
4. For **Actions**, choose **Promote**.
5. Choose **Promote read replica**.

After you promote, confirm that the promotion has completed by using the following procedure.

**To confirm that the Aurora read replica was promoted**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. In the navigation pane, choose **Events**.
3. On the **Events** page, verify that there is a **Promoted Read Replica cluster to a stand-alone database cluster** event for the cluster that you promoted.
After promotion is complete, the primary MySQL DB instance and the Aurora read replica are unlinked, and you can safely delete the DB instance if you want.

AWS CLI

To promote an Aurora read replica to a stand-alone DB cluster, use the `promote-read-replica-db-cluster` AWS CLI command.

Example

For Linux, macOS, or Unix:

```bash
aws rds promote-read-replica-db-cluster
    --db-cluster-identifier myreadreplicacluster
```

For Windows:

```bash
aws rds promote-read-replica-db-cluster ^
    --db-cluster-identifier myreadreplicacluster
```

Managing Amazon Aurora MySQL

The following sections discuss managing an Amazon Aurora MySQL DB cluster.

Topics

- Managing performance and scaling for Amazon Aurora MySQL (p. 675)
- Backtracking an Aurora DB cluster (p. 677)
- Testing Amazon Aurora using fault injection queries (p. 690)
- Altering tables in Amazon Aurora using fast DDL (p. 693)
- Displaying volume status for an Aurora DB cluster (p. 696)

Managing performance and scaling for Amazon Aurora MySQL

Scaling Aurora MySQL DB instances

You can scale Aurora MySQL DB instances in two ways, instance scaling and read scaling. For more information about read scaling, see Read scaling (p. 353).

You can scale your Aurora MySQL DB cluster by modifying the DB instance class for each DB instance in the DB cluster. Aurora MySQL supports several DB instance classes optimized for Aurora. Don't use db.t2 or db.t3 instance classes for larger Aurora clusters of size greater than 40 TB. For the specifications of the DB instance classes supported by Aurora MySQL, see DB instance classes (p. 46).

Maximum connections to an Aurora MySQL DB instance

The maximum number of connections allowed to an Aurora MySQL DB instance is determined by the `max_connections` parameter in the instance-level parameter group for the DB instance.
The following table lists the resulting default value of `max_connections` for each DB instance class available to Aurora MySQL. You can increase the maximum number of connections to your Aurora MySQL DB instance by scaling the instance up to a DB instance class with more memory, or by setting a larger value for the `max_connections` parameter in the DB parameter group for your instance, up to 16,000.

<table>
<thead>
<tr>
<th>Instance class</th>
<th>max_connections default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>db.t2.small</td>
<td>45</td>
</tr>
<tr>
<td>db.t2.medium</td>
<td>90</td>
</tr>
<tr>
<td>db.t3.small</td>
<td>45</td>
</tr>
<tr>
<td>db.t3.medium</td>
<td>90</td>
</tr>
<tr>
<td>db.r3.large</td>
<td>1000</td>
</tr>
<tr>
<td>db.r3.xlarge</td>
<td>2000</td>
</tr>
<tr>
<td>db.r3.2xlarge</td>
<td>3000</td>
</tr>
<tr>
<td>db.r3.4xlarge</td>
<td>4000</td>
</tr>
<tr>
<td>db.r3.8xlarge</td>
<td>5000</td>
</tr>
<tr>
<td>db.r4.large</td>
<td>1000</td>
</tr>
<tr>
<td>db.r4.xlarge</td>
<td>2000</td>
</tr>
<tr>
<td>db.r4.2xlarge</td>
<td>3000</td>
</tr>
<tr>
<td>db.r4.4xlarge</td>
<td>4000</td>
</tr>
<tr>
<td>db.r4.8xlarge</td>
<td>5000</td>
</tr>
<tr>
<td>db.r4.16xlarge</td>
<td>6000</td>
</tr>
<tr>
<td>db.r5.large</td>
<td>1000</td>
</tr>
<tr>
<td>db.r5.xlarge</td>
<td>2000</td>
</tr>
<tr>
<td>db.r5.2xlarge</td>
<td>3000</td>
</tr>
<tr>
<td>db.r5.4xlarge</td>
<td>4000</td>
</tr>
<tr>
<td>db.r5.8xlarge</td>
<td>5000</td>
</tr>
<tr>
<td>db.r5.12xlarge</td>
<td>6000</td>
</tr>
<tr>
<td>db.r5.16xlarge</td>
<td>6000</td>
</tr>
<tr>
<td>db.r5.24xlarge</td>
<td>7000</td>
</tr>
</tbody>
</table>

If you create a new parameter group to customize your own default for the connection limit, you'll see that the default connection limit is derived using a formula based on the `DBInstanceClassMemory` value. As shown in the preceding table, the formula produces connection limits that increase by 1000 as the memory doubles between progressively larger R3, R4, and R5 instances, and by 45 for different memory sizes of T2 and T3 instances.
The DBInstanceClassMemory value represents the memory capacity, in bytes, available for the DB instance. It's a number that Aurora computes internally and isn't directly available for you to query. Aurora reserves some memory in each DB instance for the Aurora management components. This adjustment to the available memory produces a lower max_connections value than if the formula used the full memory for the associated DB instance class.

Aurora MySQL and RDS MySQL DB instances have different amounts of memory overhead. Therefore, the max_connections value can be different for Aurora MySQL and RDS MySQL DB instances that use the same instance class. The values in the table only apply to Aurora MySQL DB instances.

The much lower connectivity limits for T2 and T3 instances are because with Aurora, those instance classes are intended only for development and test scenarios, not for production workloads.

The default connection limits are tuned for systems that use the default values for other major memory consumers, such as the buffer pool and query cache. If you change those other settings for your cluster, consider adjusting the connection limit to account for the increase or decrease in available memory on the DB instances.

Backtracking an Aurora DB cluster

With Amazon Aurora with MySQL compatibility, you can backtrack a DB cluster to a specific time, without restoring data from a backup.

Overview of backtracking

Backtracking "rewinds" the DB cluster to the time you specify. Backtracking is not a replacement for backing up your DB cluster so that you can restore it to a point in time. However, backtracking provides the following advantages over traditional backup and restore:

• You can easily undo mistakes. If you mistakenly perform a destructive action, such as a DELETE without a WHERE clause, you can backtrack the DB cluster to a time before the destructive action with minimal interruption of service.

• You can backtrack a DB cluster quickly. Restoring a DB cluster to a point in time launches a new DB cluster and restores it from backup data or a DB cluster snapshot, which can take hours. Backtracking a DB cluster doesn't require a new DB cluster and rewinds the DB cluster in minutes.

• You can explore earlier data changes. You can repeatedly backtrack a DB cluster back and forth in time to help determine when a particular data change occurred. For example, you can backtrack a DB cluster three hours and then backtrack forward in time one hour. In this case, the backtrack time is two hours before the original time.

Note

For information about restoring a DB cluster to a point in time, see Overview of backing up and restoring an Aurora DB cluster (p. 415).

Backtrack window

With backtracking, there is a target backtrack window and an actual backtrack window:

• The target backtrack window is the amount of time you want to be able to backtrack your DB cluster. When you enable backtracking, you specify a target backtrack window. For example, you might specify a target backtrack window of 24 hours if you want to be able to backtrack the DB cluster one day.

• The actual backtrack window is the actual amount of time you can backtrack your DB cluster, which can be smaller than the target backtrack window. The actual backtrack window is based on your workload and the storage available for storing information about database changes, called change records.
As you make updates to your Aurora DB cluster with backtracking enabled, you generate change records. Aurora retains change records for the target backtrack window, and you pay an hourly rate for storing them. Both the target backtrack window and the workload on your DB cluster determine the number of change records you store. The workload is the number of changes you make to your DB cluster in a given amount of time. If your workload is heavy, you store more change records in your backtrack window than you do if your workload is light.

You can think of your target backtrack window as the goal for the maximum amount of time you want to be able to backtrack your DB cluster. In most cases, you can backtrack the maximum amount of time that you specified. However, in some cases, the DB cluster can’t store enough change records to backtrack the maximum amount of time, and your actual backtrack window is smaller than your target. Typically, the actual backtrack window is smaller than the target when you have extremely heavy workload on your DB cluster. When your actual backtrack window is smaller than your target, we send you a notification.

When backtracking is enabled for a DB cluster, and you delete a table stored in the DB cluster, Aurora keeps that table in the backtrack change records. It does this so that you can revert back to a time before you deleted the table. If you don't have enough space in your backtrack window to store the table, the table might be removed from the backtrack change records eventually.

### Backtracking time

Aurora always backtracks to a time that is consistent for the DB cluster. Doing so eliminates the possibility of uncommitted transactions when the backtrack is complete. When you specify a time for a backtrack, Aurora automatically chooses the nearest possible consistent time. This approach means that the completed backtrack might not exactly match the time you specify, but you can determine the exact time for a backtrack by using the `describe-db-cluster-backtracks` AWS CLI command. For more information, see Retrieving existing backtracks (p. 689).

### Backtracking limitations

The following limitations apply to backtracking:

- Backtracking an Aurora DB cluster is available in certain AWS Regions and for specific Aurora MySQL versions only. For more information, see Backtracking in Aurora (p. 13).
- Backtracking is only available for DB clusters that were created with the Backtrack feature enabled. You can enable the Backtrack feature when you create a new DB cluster or restore a snapshot of a DB cluster. For DB clusters that were created with the Backtrack feature enabled, you can create a clone DB cluster with the Backtrack feature enabled. Currently, you can't perform backtracking on DB clusters that were created with the Backtrack feature disabled.
- The limit for a backtrack window is 72 hours.
- Backtracking affects the entire DB cluster. For example, you can't selectively backtrack a single table or a single data update.
- Backtracking isn't supported with binary log (binlog) replication. Cross-Region replication must be disabled before you can configure or use backtracking.
- You can't backtrack a database clone to a time before that database clone was created. However, you can use the original database to backtrack to a time before the clone was created. For more information about database cloning, see Cloning an Aurora DB cluster volume (p. 355).
- Backtracking causes a brief DB instance disruption. You must stop or pause your applications before starting a backtrack operation to ensure that there are no new read or write requests. During the backtrack operation, Aurora pauses the database, closes any open connections, and drops any uncommitted reads and writes. It then waits for the backtrack operation to complete.
- Backtracking isn't supported for the following AWS Regions:
  - Africa (Cape Town)
  - China (Ningxia)
Backtracking is available for Aurora MySQL 1.*, which is compatible with MySQL 5.6. It's also available for Aurora MySQL 2.06 and higher, which is compatible with MySQL 5.7. Because of the Aurora MySQL 2.* version requirement, if you created the Aurora MySQL 1.* cluster with the Backtrack setting enabled, you can only upgrade to a Backtrack-compatible version of Aurora MySQL 2.*. This requirement affects the following types of upgrade paths:

• You can only restore a snapshot of the Aurora MySQL 1.* DB cluster to a Backtrack-compatible version of Aurora MySQL 2.*.
• You can only perform point-in-time recovery on the Aurora MySQL 1.* DB cluster to restore it to a Backtrack-compatible version of Aurora MySQL 2.*.

These upgrade requirements still apply even if you turn off Backtrack for the Aurora MySQL 1.* cluster.

Configuring backtracking

To use the Backtrack feature, you must enable backtracking and specify a target backtrack window. Otherwise, backtracking is disabled.

For the target backtrack window, specify the amount of time that you want to be able to rewind your database using Backtrack. Aurora tries to retain enough change records to support that window of time.

Console

You can use the console to configure backtracking when you create a new DB cluster. You can also modify a DB cluster to enable backtracking.

Topics

• Configuring backtracking with the console when creating a DB cluster (p. 679)
• Configuring backtrack with the console when modifying a DB cluster (p. 680)

Configuring backtracking with the console when creating a DB cluster

When you create a new Aurora MySQL DB cluster, backtracking is configured when you choose Enable Backtrack and specify a Target Backtrack window value that is greater than zero in the Backtrack section.

To create a DB cluster, follow the instructions in Creating an Amazon Aurora DB cluster (p. 118). The following image shows the Backtrack section.
When you create a new DB cluster, Aurora has no data for the DB cluster's workload. So it can't estimate a cost specifically for the new DB cluster. Instead, the console presents a typical user cost for the specified target backtrack window based on a typical workload. The typical cost is meant to provide a general reference for the cost of the Backtrack feature.

**Important**
Your actual cost might not match the typical cost, because your actual cost is based on your DB cluster's workload.

### Configuring backtrack with the console when modifying a DB cluster

You can modify backtracking for a DB cluster using the console.

**Note**
Currently, you can modify backtracking only for a DB cluster that has the Backtrack feature enabled. The Backtrack section doesn't appear for a DB cluster that was created with the Backtrack feature disabled or if the Backtrack feature has been disabled for the DB cluster.

### To modify backtracking for a DB cluster using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. Choose **Databases**.
3. Choose the cluster that you want to modify, and choose **Modify**.
4. For **Target Backtrack window**, modify the amount of time that you want to be able to backtrack. The limit is 72 hours.
Backtracking a DB cluster

The console shows the estimated cost for the amount of time you specified based on the DB cluster's past workload:

- If backtracking was disabled on the DB cluster, the cost estimate is based on the VolumeWriteIOPS metric for the DB cluster in Amazon CloudWatch.
- If backtracking was enabled previously on the DB cluster, the cost estimate is based on the BacktrackChangeRecordsCreationRate metric for the DB cluster in Amazon CloudWatch.

5. Choose Continue.

6. For Scheduling of Modifications, choose one of the following:
   - **Apply during the next scheduled maintenance window** – Wait to apply the Target Backtrack window modification until the next maintenance window.
   - **Apply immediately** – Apply the Target Backtrack window modification as soon as possible.

7. Choose Modify cluster.

**AWS CLI**

When you create a new Aurora MySQL DB cluster using the `create-db-cluster` AWS CLI command, backtracking is configured when you specify a `--backtrack-window` value that is greater than zero. The `--backtrack-window` value specifies the target backtrack window. For more information, see Creating an Amazon Aurora DB cluster (p. 118).

You can also specify the `--backtrack-window` value using the following AWS CLI commands:

- `modify-db-cluster`
- `restore-db-cluster-from-s3`
- `restore-db-cluster-from-snapshot`
- `restore-db-cluster-to-point-in-time`

The following procedure describes how to modify the target backtrack window for a DB cluster using the AWS CLI.
To modify the target backtrack window for a DB cluster using the AWS CLI

- Call the modify-db-cluster AWS CLI command and supply the following values:
  - `--db-cluster-identifier` – The name of the DB cluster.
  - `--backtrack-window` – The maximum number of seconds that you want to be able to backtrack the DB cluster.

The following example sets the target backtrack window for `sample-cluster` to one day (86,400 seconds).

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster \
  --db-cluster-identifier sample-cluster \
  --backtrack-window 86400
```

For Windows:

```bash
aws rds modify-db-cluster ^
  --db-cluster-identifier sample-cluster ^
  --backtrack-window 86400
```

**Note**
Currently, you can enable backtracking only for a DB cluster that was created with the Backtrack feature enabled.

**RDS API**

When you create a new Aurora MySQL DB cluster using the CreateDBCluster Amazon RDS API operation, backtracking is configured when you specify a `BacktrackWindow` value that is greater than zero. The `BacktrackWindow` value specifies the target backtrack window for the DB cluster specified in the `DBClusterIdentifier` value. For more information, see Creating an Amazon Aurora DB cluster (p. 118).

You can also specify the `BacktrackWindow` value using the following API operations:

- ModifyDBCluster
- RestoreDBClusterFromS3
- RestoreDBClusterFromSnapshot
- RestoreDBClusterToPointInTime

**Note**
Currently, you can enable backtracking only for a DB cluster that was created with the Backtrack feature enabled.

**Performing a backtrack**

You can backtrack a DB cluster to a specified backtrack time stamp. If the backtrack time stamp isn't earlier than the earliest possible backtrack time, and isn't in the future, the DB cluster is backtracked to that time stamp.
Otherwise, an error typically occurs. Also, if you try to backtrack a DB cluster for which binary logging is enabled, an error typically occurs unless you've chosen to force the backtrack to occur. Forcing a backtrack to occur can interfere with other operations that use binary logging.

**Important**
Backtracking doesn't generate binlog entries for the changes that it makes. If you have binary logging enabled for the DB cluster, backtracking might not be compatible with your binlog implementation.

**Note**
For database clones, you can't backtrack the DB cluster earlier than the date and time when the clone was created. For more information about database cloning, see Cloning an Aurora DB cluster volume (p. 355).

**Console**

The following procedure describes how to perform a backtrack operation for a DB cluster using the console.

**To perform a backtrack operation using the console**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Instances**.
3. Choose the primary instance for the DB cluster that you want to backtrack.
4. For **Actions**, choose **Backtrack DB cluster**.
5. On the **Backtrack DB cluster** page, enter the backtrack time stamp to backtrack the DB cluster to.

6. Choose **Backtrack DB cluster**.

**AWS CLI**

The following procedure describes how to backtrack a DB cluster using the AWS CLI.

**To backtrack a DB cluster using the AWS CLI**

- Call the `backtrack-db-cluster` AWS CLI command and supply the following values:
Backtracking a DB cluster

- `--db-cluster-identifier` - The name of the DB cluster.
- `--backtrack-to` - The backtrack time stamp to backtrack the DB cluster to, specified in ISO 8601 format.

The following example backtracks the DB cluster `sample-cluster` to March 19, 2018, at 10 a.m.

For Linux, macOS, or Unix:

```
aws rds backtrack-db-cluster
   --db-cluster-identifier sample-cluster
   --backtrack-to 2018-03-19T10:00:00+00:00
```

For Windows:

```
aws rds backtrack-db-cluster
   --db-cluster-identifier sample-cluster
   --backtrack-to 2018-03-19T10:00:00+00:00
```

RDS API

To backtrack a DB cluster using the Amazon RDS API, use the BacktrackDBCluster action. This action backtracks the DB cluster specified in the `DBClusterIdentifier` value to the specified time.

Monitoring backtracking

You can view backtracking information and monitor backtracking metrics for a DB cluster.

Console

To view backtracking information and monitor backtracking metrics using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Databases.
3. Choose the DB cluster name to open information about it.

The backtrack information is in the Backtrack section.
When backtracking is enabled, the following information is available:

- **Target window** – The current amount of time specified for the target backtrack window. The target is the maximum amount of time that you can backtrack if there is sufficient storage.

- **Actual window** – The actual amount of time you can backtrack, which can be smaller than the target backtrack window. The actual backtrack window is based on your workload and the storage available for retaining backtrack change records.

- **Earliest backtrack time** – The earliest possible backtrack time for the DB cluster. You can't backtrack the DB cluster to a time before the displayed time.

4. Do the following to view backtracking metrics for the DB cluster:

   a. In the navigation pane, choose **Instances**.

   b. Choose the name of the primary instance for the DB cluster to display its details.

   c. In the **CloudWatch** section, type **Backtrack** into the **CloudWatch** box to show only the Backtrack metrics.

   ![Screen capture of CloudWatch showing backtrack metrics](image)

   The following metrics are displayed:
• **Backtrack Change Records Creation Rate (Count)** – This metric shows the number of backtrack change records created over five minutes for your DB cluster. You can use this metric to estimate the backtrack cost for your target backtrack window.

• **[Billed] Backtrack Change Records Stored (Count)** – This metric shows the actual number of backtrack change records used by your DB cluster.

• **Backtrack Window Actual (Minutes)** – This metric shows whether there is a difference between the target backtrack window and the actual backtrack window. For example, if your target backtrack window is 2 hours (120 minutes), and this metric shows that the actual backtrack window is 100 minutes, then the actual backtrack window is smaller than the target.

• **Backtrack Window Alert (Count)** – This metric shows how often the actual backtrack window is smaller than the target backtrack window for a given period of time.

**Note**
The following metrics might lag behind the current time:

• **Backtrack Change Records Creation Rate (Count)**
• **[Billed] Backtrack Change Records Stored (Count)**

### AWS CLI

The following procedure describes how to view backtrack information for a DB cluster using the AWS CLI.

**To view backtrack information for a DB cluster using the AWS CLI**

• Call the `describe-db-clusters` AWS CLI command and supply the following values:
  
  • `--db-cluster-identifier` – The name of the DB cluster.

  The following example lists backtrack information for `sample-cluster`.

  For Linux, macOS, or Unix:

  ```bash
  aws rds describe-db-clusters "
  --db-cluster-identifier sample-cluster
  ```

  For Windows:

  ```bash
  aws rds describe-db-clusters ^
  --db-cluster-identifier sample-cluster
  ```

### RDS API

To view backtrack information for a DB cluster using the Amazon RDS API, use the `DescribeDBClusters` operation. This action returns backtrack information for the DB cluster specified in the `DBClusterIdentifier` value.
Subscribing to a backtrack event with the console

The following procedure describes how to subscribe to a backtrack event using the console. The event sends you an email or text notification when your actual backtrack window is smaller than your target backtrack window.

To view backtrack information using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Event subscriptions.
3. Choose Create event subscription.
4. In the Name box, type a name for the event subscription, and ensure that Yes is selected for Enabled.
5. In the Target section, choose New email topic.
6. For Topic name, type a name for the topic, and for With these recipients, enter the email addresses or phone numbers to receive the notifications.
7. In the Source section, choose Instances for Source type.
8. For Instances to include, choose Select specific instances, and choose your DB instance.
9. For Event categories to include, choose Select specific event categories, and choose backtrack.

Your page should look similar to the following page.
10. Choose **Create**.

### Retrieving existing backtracks

You can retrieve information about existing backtracks for a DB cluster. This information includes the unique identifier of the backtrack, the date and time backtracked to and from, the date and time the backtrack was requested, and the current status of the backtrack.

**Note**
Currently, you can't retrieve existing backtracks using the console.

**AWS CLI**

The following procedure describes how to retrieve existing backtracks for a DB cluster using the AWS CLI.

**To retrieve existing backtracks using the AWS CLI**

- Call the `describe-db-cluster-backtracks` AWS CLI command and supply the following values:
  - `--db-cluster-identifier` – The name of the DB cluster.

The following example retrieves existing backtracks for `sample-cluster`.

For Linux, macOS, or Unix:

```bash
aws rds describe-db-cluster-backtracks \
  --db-cluster-identifier sample-cluster
```

For Windows:

```bash
aws rds describe-db-cluster-backtracks ^
  --db-cluster-identifier sample-cluster
```

**RDS API**

To retrieve information about the backtracks for a DB cluster using the Amazon RDS API, use the `DescribeDBClusterBacktracks` operation. This action returns information about backtracks for the DB cluster specified in the `DBClusterIdentifier` value.

### Disabling backtracking for a DB cluster

You can disable the Backtrack feature for a DB cluster.

**Console**

You can disable backtracking for a DB cluster using the console.

**To disable the backtrack feature for a DB cluster using the console**

1. Sign in to the AWS Management Console and open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. Choose **Databases**.
3. Choose the cluster you want to modify, and choose **Modify**.
4. In the **Backtrack** section, choose **Disable Backtrack**.
5. Choose **Continue**.
6. For **Scheduling of Modifications**, choose one of the following:
   - **Apply during the next scheduled maintenance window** – Wait to apply the modification until the next maintenance window.
   - **Apply immediately** – Apply the modification as soon as possible.
7. Choose **Modify Cluster**.

**AWS CLI**

You can disable the Backtrack feature for a DB cluster using the AWS CLI by setting the target backtrack window to 0 (zero).

**To modify the target backtrack window for a DB cluster using the AWS CLI**

- Call the `modify-db-cluster` AWS CLI command and supply the following values:
  - `--db-cluster-identifier` – The name of the DB cluster.
  - `--backtrack-window 0`.

The following example disables the Backtrack feature for the `sample-cluster` by setting `--backtrack-window` to 0.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster --db-cluster-identifier sample-cluster --backtrack-window 0
```

For Windows:

```bash
aws rds modify-db-cluster --db-cluster-identifier sample-cluster --backtrack-window 0
```

**RDS API**

To disable the Backtrack feature for a DB cluster using the Amazon RDS API, use the `ModifyDBCluster` operation. Set the `BacktrackWindow` value to 0 (zero), and specify the DB cluster in the `DBClusterIdentifier` value.

**Testing Amazon Aurora using fault injection queries**

You can test the fault tolerance of your Amazon Aurora DB cluster by using fault injection queries. Fault injection queries are issued as SQL commands to an Amazon Aurora instance and they enable you to schedule a simulated occurrence of one of the following events:

- A crash of a writer or reader DB instance
- A failure of an Aurora Replica
- A disk failure
- Disk congestion
When a fault injection query specifies a crash, it forces a crash of the Aurora DB instance. The other fault injection queries result in simulations of failure events, but don't cause the event to occur. When you submit a fault injection query, you also specify an amount of time for the failure event simulation to occur for.

You can submit a fault injection query to one of your Aurora Replica instances by connecting to the endpoint for the Aurora Replica. For more information, see Amazon Aurora connection management (p. 24).

**Testing an instance crash**

You can force a crash of an Amazon Aurora instance using the `ALTER SYSTEM CRASH` fault injection query.

For this fault injection query, a failover will not occur. If you want to test a failover, then you can choose the **Failover** instance action for your DB cluster in the RDS console, or use the `failover-db-cluster` AWS CLI command or the `FailoverDBCluster` RDS API operation.

**Syntax**

```
ALTER SYSTEM CRASH [ INSTANCE | DISPATCHER | NODE ];
```

**Options**

This fault injection query takes one of the following crash types:

- **INSTANCE** — A crash of the MySQL-compatible database for the Amazon Aurora instance is simulated.
- **DISPATCHER** — A crash of the dispatcher on the writer instance for the Aurora DB cluster is simulated. The dispatcher writes updates to the cluster volume for an Amazon Aurora DB cluster.
- **NODE** — A crash of both the MySQL-compatible database and the dispatcher for the Amazon Aurora instance is simulated. For this fault injection simulation, the cache is also deleted.

The default crash type is **INSTANCE**.

**Testing an Aurora replica failure**

You can simulate the failure of an Aurora Replica using the `ALTER SYSTEM SIMULATE READ REPLICA FAILURE` fault injection query.

An Aurora Replica failure will block all requests to an Aurora Replica or all Aurora Replicas in the DB cluster for a specified time interval. When the time interval completes, the affected Aurora Replicas will be automatically synced up with master instance.

**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 };
```

**Options**

This fault injection query takes the following parameters:

- **percentage_of_failure** — The percentage of requests to block during the failure event. This value can be a double between 0 and 100. If you specify 0, then no requests are blocked. If you specify 100, then all requests are blocked.
• **Failure type** — The type of failure to simulate. Specify **TO ALL** to simulate failures for all Aurora Replicas in the DB cluster. Specify **TO** and the name of the Aurora Replica to simulate a failure of a single Aurora Replica. The default failure type is **TO ALL**.

• **quantity** — The amount of time for which to simulate the Aurora Replica failure. The interval is an amount followed by a time unit. The simulation will occur for that amount of the specified unit. For example, **20 MINUTE** will result in the simulation running for 20 minutes.

  **Note**
  Take care when specifying the time interval for your Aurora Replica failure event. If you specify too long of a time interval, and your writer instance writes a large amount of data during the failure event, then your Aurora DB cluster might assume that your Aurora Replica has crashed and replace it.

### Testing a disk failure

You can simulate a disk failure for an Aurora DB cluster using the `ALTER SYSTEM SIMULATE DISK FAILURE` fault injection query.

During a disk failure simulation, the Aurora DB cluster randomly marks disk segments as faulting. Requests to those segments will be blocked for the duration of the simulation.

#### 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 };
```

#### Options

This fault injection query takes the following parameters:

• **percentage_of_failure** — The percentage of the disk to mark as faulting during the failure event. This value can be a double between 0 and 100. If you specify 0, then none of the disk is marked as faulting. If you specify 100, then the entire disk is marked as faulting.

• **DISK index** — A specific logical block of data to simulate the failure event for. If you exceed the range of available logical blocks of data, you will receive an error that tells you the maximum index value that you can specify. For more information, see Displaying volume status for an Aurora DB cluster (p. 696).

• **NODE index** — A specific storage node to simulate the failure event for. If you exceed the range of available storage nodes, you will receive an error that tells you the maximum index value that you can specify. For more information, see Displaying volume status for an Aurora DB cluster (p. 696).

• **quantity** — The amount of time for which to simulate the disk failure. The interval is an amount followed by a time unit. The simulation will occur for that amount of the specified unit. For example, **20 MINUTE** will result in the simulation running for 20 minutes.

### Testing disk congestion

You can simulate a disk failure for an Aurora DB cluster using the `ALTER SYSTEM SIMULATE DISK CONGESTION` fault injection query.

During a disk congestion simulation, the Aurora DB cluster randomly marks disk segments as congested. Requests to those segments will be delayed between the specified minimum and maximum delay time for the duration of the simulation.
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 };
```

Options

This fault injection query takes the following parameters:

- **`percentage_of_failure`** — The percentage of the disk to mark as congested during the failure event. This value can be a double between 0 and 100. If you specify 0, then none of the disk is marked as congested. If you specify 100, then the entire disk is marked as congested.
- **`disk_index` or `node_index`** — A specific disk or node to simulate the failure event for. If you exceed the range of indexes for the disk or node, you will receive an error that tells you the maximum index value that you can specify.
- **`minimum` and `maximum`** — The minimum and maximum amount of congestion delay, in milliseconds. Disk segments marked as congested will be delayed for a random amount of time within the range of the minimum and maximum amount of milliseconds for the duration of the simulation.
- **`quantity`** — The amount of time for which to simulate the disk congestion. The interval is an amount followed by a time unit. The simulation will occur for that amount of the specified time unit. For example, `20 MINUTE` will result in the simulation running for 20 minutes.

Altering tables in Amazon Aurora using fast DDL

In MySQL, many data definition language (DDL) operations have a significant performance impact. Performance impacts occur even with recent online DDL improvements.

For example, suppose that you use an `ALTER TABLE` operation to add a column to a table. Depending on the algorithm specified for the operation, this operation can involve the following:

- Creating a full copy of the table
- Creating a temporary table to process concurrent data manipulation language (DML) operations
- Rebuilding all indexes for the table
- Applying table locks while applying concurrent DML changes
- Slowing concurrent DML throughput

In Amazon Aurora, you can use fast DDL to run an `ALTER TABLE` operation in place, nearly instantaneously. The operation completes without requiring the table to be copied and without having a material impact on other DML statements. Because the operation doesn't consume temporary storage for a table copy, it makes DDL statements practical even for large tables on small instance classes.

**Important**
Currently, Aurora lab mode must be enabled to use fast DDL for Aurora MySQL. We don't recommend using fast DDL for production DB clusters. For information about enabling Aurora lab mode, see [Amazon Aurora MySQL lab mode](p. 839).

**Note**
Fast DDL is available for Aurora version 1.12 and later. For more information about Aurora versions, see [Database engine updates for Amazon Aurora MySQL](p. 874)

Fast DDL limitations

Currently, fast DDL has the following limitations:
Fast DDL only supports adding nullable columns, without default values, to the end of an existing table.

Fast DDL does not support partitioned tables.

Fast DDL does not support InnoDB tables that use the REDUNDANT row format.

If the maximum possible record size for the DDL operation is too large, fast DDL is not used. A record size is too large if it is greater than half the page size. The maximum size of a record is computed by adding the maximum sizes of all columns. For variable sized columns, according to InnoDB standards, extern bytes are not included for computation.

Note
The maximum record size check was added in Aurora 1.15.

Fast DDL syntax

ALTER TABLE `tbl_name` ADD COLUMN `col_name` `column_definition`

This statement takes the following options:

• `tbl_name` — The name of the table to be modified.
• `col_name` — The name of the column to be added.
• `col_definition` — The definition of the column to be added.

Note
You must specify a nullable column definition without a default value. Otherwise, fast DDL isn't used.

Fast DDL examples

The following examples demonstrate the speedup from fast DDL operations. The first SQL example runs `ALTER TABLE` statements on a large table without using fast DDL. This operation takes substantial time. A CLI example shows how to enable fast DDL for the cluster. Then another SQL example runs the same `ALTER TABLE` statements on an identical table. With fast DDL enabled, the operation is very fast.

This example uses the `ORDERS` table from the TPC-H benchmark, containing 150 million rows. This cluster intentionally uses a relatively small instance class, to demonstrate how long `ALTER TABLE` statements can take when you can't use fast DDL. The example creates a clone of the original table containing identical data. Checking the `aurora_lab_mode` setting confirms that the cluster can't use fast DDL, because lab mode isn't enabled. Then `ALTER TABLE ADD COLUMN` statements take substantial time to add new columns at the end of the table.

```
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;
+-------------------+
<table>
<thead>
<tr>
<th>@@aurora_lab_mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
</tbody>
</table>
+-------------------+

mysql> ALTER TABLE orders_regular_ddl ADD COLUMN o_refunded boolean;
Query OK, 0 rows affected (40 min 31.41 sec)
```
This example does the same preparation of a large table as the previous example. However, you can’t simply enable lab mode within an interactive SQL session. That setting must be enabled in a custom parameter group. Doing so requires switching out of the `mysql` session and running some AWS CLI commands or using the AWS Management Console.

Enabling lab mode for the cluster requires some work with a parameter group. This AWS CLI example uses a cluster parameter group, to ensure that all DB instances in the cluster use the same value for the lab mode setting.

```bash
# aws rds create-db-cluster-parameter-group
   --db-parameter-group-family aurora5.6
   --db-cluster-parameter-group-name lab-mode-enabled-56 --description 'TBD'
# aws rds describe-db-cluster-parameters
   --db-cluster-parameter-group-name lab-mode-enabled-56
   --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-56
   --parameters ParameterName=aurora_lab_mode,ParameterValue=1,ApplyMethod=pending-reboot

# 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-56

# Reboot the primary instance for the cluster tpch100g:
# aws rds reboot-db-instance --db-instance-identifier instance-2020-12-22-5208

# aws rds describe-db-clusters --db-cluster-id tpch100g
   --query '.*[DBClusterParameterGroup]' --output text
lab-mode-enabled-56
# aws rds describe-db-cluster-parameters
   --db-cluster-parameter-group-name lab-mode-enabled-56
   --query '.*[ParameterName:ParameterName,ParameterValue:ParameterValue]'
   --output text | grep aurora_lab_mode
```
aurora_lab_mode 1

The following example shows the remaining steps after the parameter group change takes effect. It tests the aurora_lab_mode setting to make sure that the cluster can use fast DDL. Then it runs ALTER TABLE statements to add columns to the end of another large table. This time, the statements finish very quickly.

```
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)
```

Displaying volume status for an Aurora DB cluster

In Amazon Aurora, a DB cluster volume consists of a collection of logical blocks. Each of these represents 10 gigabytes of allocated storage. These blocks are called protection groups.

The data in each protection group is replicated across six physical storage devices, called storage nodes. These storage nodes are allocated across three Availability Zones (AZs) in the AWS Region where the DB cluster resides. In turn, each storage node contains one or more logical blocks of data for the DB cluster volume. For more information about protection groups and storage nodes, see Introducing the Aurora storage engine on the AWS Database Blog.

You can simulate the failure of an entire storage node, or a single logical block of data within a storage node. To do so, you use the ALTER SYSTEM SIMULATE DISK FAILURE fault injection statement. For the statement, you specify the index value of a specific logical block of data or storage node. However, if you specify an index value greater than the number of logical blocks of data or storage nodes used by the DB cluster volume, the statement returns an error. For more information about fault injection queries, see Testing Amazon Aurora using fault injection queries (p. 690).

You can avoid that error by using the SHOW VOLUME STATUS statement. The statement returns two server status variables, Disks and Nodes. These variables represent the total number of logical blocks of data and storage nodes, respectively, for the DB cluster volume.

**Note**
The SHOW VOLUME STATUS statement is available for Aurora version 1.12 and later. For more information about Aurora versions, see Database engine updates for Amazon Aurora MySQL (p. 874).

**Syntax**

```
SHOW VOLUME STATUS
```

**Example**
The following example illustrates a typical SHOW VOLUME STATUS result.
Working with parallel query for Amazon Aurora MySQL

Following, you can find a description of the parallel query performance optimization for Amazon Aurora with MySQL compatibility. This feature uses a special processing path for certain data-intensive queries, taking advantage of the Aurora shared storage architecture. Currently, Aurora MySQL versions that are compatible with MySQL 5.6 or MySQL 5.7 support parallel query. Parallel query works best with Aurora MySQL DB clusters that have tables with millions of rows and analytic queries that take minutes or hours to complete.

Topics
- Overview of parallel query for Aurora MySQL (p. 697)
- Planning for a parallel query cluster (p. 700)
- Creating a DB cluster that works with parallel query (p. 701)
- Enabling and disabling parallel query (p. 705)
- Upgrade considerations for parallel query (p. 707)
- Performance tuning for parallel query (p. 708)
- Creating schema objects to take advantage of parallel query (p. 709)
- Verifying which statements use parallel query (p. 709)
- Monitoring parallel query (p. 712)
- How parallel query works with SQL constructs (p. 715)

Overview of parallel query for Aurora MySQL

Aurora MySQL parallel query is an optimization that parallelizes some of the I/O and computation involved in processing data-intensive queries. The work that is parallelized includes retrieving rows from storage, extracting column values, and determining which rows match the conditions in the WHERE clause and join clauses. This data-intensive work is delegated (in database optimization terms, pushed down) to multiple nodes in the Aurora distributed storage layer. Without parallel query, each query brings all the scanned data to a single node within the Aurora MySQL cluster (the head node) and performs all the query processing there.

Tip
The PostgreSQL database engine also has a feature that's also called "parallel query". That feature is unrelated to Aurora parallel query.

When the parallel query feature is enabled, the Aurora MySQL engine automatically determines when queries can benefit, without requiring SQL changes such as hints or table attributes. In the following sections, you can find an explanation of when parallel query is applied to a query. You can also find how to make sure that parallel query is applied where it provides the most benefit.

Note
The parallel query optimization provides the most benefit for long-running queries that take minutes or hours to complete. Aurora MySQL generally doesn't perform parallel
query optimization for inexpensive queries. It also generally doesn’t perform parallel query optimization if another optimization technique makes more sense, such as query caching, buffer pool caching, or index lookups. If you find that parallel query isn’t being used when you expect it, see Verifying which statements use parallel query (p. 709).

Topics
- Benefits (p. 698)
- Architecture (p. 698)
- Prerequisites (p. 699)
- Limitations (p. 699)

Benefits

With parallel query, you can run data-intensive analytic queries on Aurora MySQL tables. In many cases, you can get an order-of-magnitude performance improvement over the traditional division of labor for query processing.

Benefits of parallel query include the following:

- Improved I/O performance, due to parallelizing physical read requests across multiple storage nodes.
- Reduced network traffic. Aurora doesn’t transmit entire data pages from storage nodes to the head node and then filter out unnecessary rows and columns afterward. Instead, Aurora transmits compact tuples containing only the column values needed for the result set.
- Reduced CPU usage on the head node, due to pushing down function processing, row filtering, and column projection for the WHERE clause.
- Reduced memory pressure on the buffer pool. The pages processed by the parallel query aren’t added to the buffer pool. This approach reduces the chance of a data-intensive scan evicting frequently used data from the buffer pool.
- Potentially reduced data duplication in your extract, transform, load (ETL) pipeline, by making it practical to perform long-running analytic queries on existing data.

Architecture

The parallel query feature uses the major architectural principles of Aurora MySQL: decoupling the database engine from the storage subsystem, and reducing network traffic by streamlining communication protocols. Aurora MySQL uses these techniques to speed up write-intensive operations such as redo log processing. Parallel query applies the same principles to read operations.

Note

The architecture of Aurora MySQL parallel query differs from that of similarly named features in other database systems. Aurora MySQL parallel query doesn’t involve symmetric multiprocessing (SMP) and so doesn’t depend on the CPU capacity of the database server. The parallel processing happens in the storage layer, independent of the Aurora MySQL server that serves as the query coordinator.

By default, without parallel query, the processing for an Aurora query involves transmitting raw data to a single node within the Aurora cluster (the head node). Aurora then performs all further processing for that query in a single thread on that single node. With parallel query, much of this I/O-intensive and CPU-intensive work is delegated to nodes in the storage layer. Only the compact rows of the result set are transmitted back to the head node, with rows already filtered, and column values already extracted and transformed. The performance benefit comes from the reduction in network traffic, reduction in CPU usage on the head node, and parallelizing the I/O across the storage nodes. The amount of parallel I/O, filtering, and projection is independent of the number of DB instances in the Aurora cluster that runs the query.
Prerequisites

To use all features of parallel query requires an Aurora MySQL DB cluster that's running version 1.23 or 2.09 and higher. If you already have a cluster that you want to use with parallel query, you can upgrade it to a compatible version and enable parallel query afterward. In that case, make sure to follow the upgrade procedure in Upgrade considerations for parallel query (p. 707) because the configuration setting names and default values are different in these newer versions.

You can also use parallel query with certain older Aurora MySQL versions that are compatible with MySQL 5.6: 1.22.2, 1.20.1, 1.19.6, and 5.6.10a. The parallel query support for these older versions is only available in certain AWS Regions. Those older versions have additional limitations, as described following. Using parallel query with an older Aurora MySQL version also requires creating a dedicated DB cluster with a special engine mode parameter that can't be changed later. For those reasons, we recommend using parallel query with Aurora MySQL 1.23 or 2.09 and higher where practical.

The DB instances in your cluster must be using the `db.r*` instance classes.

Your tables must be nonpartitioned for the parallel query optimization to apply to them.

Make sure that the hash join optimization is turned on for your cluster. The procedure to do so is different depending on whether your cluster is running an Aurora MySQL version higher or lower than 1.23 or 2.09. To learn how, see Enabling hash join for parallel query clusters (p. 706).

To customize parameters such as `aurora_parallel_query` and `aurora_disable_hash_join`, you must have a custom parameter group that you use with your cluster. You can specify these parameters individually for each DB instance by using a DB parameter group. However, we recommend that you specify them in a DB cluster parameter group. That way, all DB instances in your cluster inherit the same settings for these parameters.

Limitations

The following limitations apply to the parallel query feature:

- You can't use parallel query with the `db.t2` or `db.t3` instance classes. This limitation applies even if you request parallel query using the `aurora_pq_force` SQL hint.
- Parallel query doesn't apply to tables using the `COMPRESSED` or `RENDUNDANT` row formats. Use the `COMPACT` or `DYNAMIC` row formats for tables you plan to use with parallel query.
- Currently, partitioned tables aren't supported for parallel query. You can use partitioned tables in parallel query clusters. Queries against those tables use the non-parallel query processing path.
- Aurora uses a cost-based algorithm to determine whether to use the parallel query mechanism for each SQL statement. Using certain SQL constructs in a statement can prevent parallel query or make parallel query unlikely for that statement. For information about compatibility of SQL constructs with parallel query, see How parallel query works with SQL constructs (p. 715).
- Each Aurora DB instance can run only a certain number of parallel query sessions at one time. If a query has multiple parts that use parallel query, such as subqueries, joins, or `UNION` operators, those phases run in sequence. The statement only counts as a single parallel query session at any one time. You can monitor the number of active sessions using the `parallel query status variables` (p. 712). You can check the limit on concurrent sessions for a given DB instance by querying the status variable `Aurora_pq_max_concurrent_requests`.
- Parallel query is available in all AWS Regions that Aurora supports. For most AWS Regions, the minimum required Aurora MySQL version to use parallel query is 1.23 or 2.09. For more information, see Aurora parallel queries (p. 18).
- Aurora MySQL 1.22.2, 1.20.1, 1.19.6, and 5.6.10a only: Using parallel query with these older versions involves creating a new cluster, or restoring from an existing Aurora MySQL cluster snapshot.
- Aurora MySQL 1.22.2, 1.20.1, 1.19.6, and 5.6.10a only: Parallel query doesn't support AWS Identity and Access Management (IAM) database authentication.
Planning for a parallel query cluster

Planning for a DB cluster that's enabled for parallel query requires making some choices. These include performing setup steps (either creating or restoring a full Aurora MySQL cluster) and deciding how broadly to enable parallel query across your DB cluster.

Consider the following as part of planning:

- Which Aurora MySQL version do you plan to use for the cluster? Depending on your choice, you can use one of these ways to enable parallel query for the cluster:

  If you use Aurora MySQL that's compatible with MySQL 5.7, you must choose Aurora MySQL 2.09 or higher. In this case, you always create a provisioned cluster. Then you enable parallel query using the `aurora_parallel_query` parameter. We recommend this choice if you are starting with Aurora parallel query for the first time.

  If you use Aurora MySQL that's compatible with MySQL 5.6, you can choose version 1.23 or certain lower versions. With version 1.23 or higher, you create a provisioned cluster and then enable parallel query using the `aurora_parallel_query` DB cluster parameter. With a version lower than 1.23, you choose the `parallelquery` engine mode when creating the cluster. In this case, parallel query is permanently turned on for the cluster. The `parallelquery` engine mode imposes limitations on interoperating with other kinds of Aurora MySQL clusters. If you have a choice, we recommend choosing version 1.23 or higher for Aurora MySQL with MySQL 5.6 compatibility.

  If you have an existing Aurora MySQL cluster that's running version 1.23 or higher, or 2.09 or higher, you don't have to create a new cluster to use parallel query. You can associate your cluster, or specific DB instances in the cluster, with a parameter group that has the `aurora_parallel_query` parameter enabled. By doing so, you can reduce the time and effort to set up the relevant data to use with parallel query.

- Plan for any large tables that you need to reorganize so that you can use parallel query when accessing them. You might need to create new versions of some large tables where parallel query is useful. For example, you might need to make the table nonpartitioned or to remove full-text search indexes. For details, see Creating schema objects to take advantage of parallel query (p. 709).

Checking Aurora MySQL version compatibility for parallel query

To check which Aurora MySQL versions are compatible with parallel query clusters, use the `describe-db-engine-versions` AWS CLI command and check the value of the `SupportsParallelQuery` field. The following code example shows how to check which combinations are available for parallel query clusters in a specified AWS Region. Make sure to specify the full `--query` parameter string on a single line.

```
aws rds describe-db-engine-versions --region us-east-1 --engine aurora --query '*[?SupportsParallelQuery == `true`].[EngineVersion]' --output text
aws rds describe-db-engine-versions --region us-east-1 --engine aurora-mysql --query '*[?SupportsParallelQuery == `true`].[EngineVersion]' --output text
```

The preceding commands produce output similar to the following. The output might vary depending on which Aurora MySQL versions are available in the specified AWS Region.

```
5.6.10a
5.6.mysql_aurora.1.19.0
5.6.mysql_aurora.1.19.1
5.6.mysql_aurora.1.19.2
5.6.mysql_aurora.1.19.3
```
After you start using parallel query with a cluster, you can monitor performance and remove obstacles to parallel query usage. For those instructions, see Performance tuning for parallel query (p. 708).

Creating a DB cluster that works with parallel query

To create an Aurora MySQL cluster with parallel query, add new instances to it, or perform other administrative operations, you use the same AWS Management Console and AWS CLI techniques that you do with other Aurora MySQL clusters. You can create a new cluster to work with parallel query. You can also create a DB cluster to work with parallel query by restoring from a snapshot of a MySQL-compatible Aurora DB cluster. If you aren’t familiar with the process for creating a new Aurora MySQL cluster, you can find background information and prerequisites in Creating an Amazon Aurora DB cluster (p. 118).

However, certain options are different:

- When you choose an Aurora MySQL engine version, we recommend that you choose the latest engine that is compatible with MySQL 5.7. Currently, Aurora MySQL 2.09 or higher, and certain Aurora MySQL versions that are compatible with MySQL 5.6 support parallel query. You have more flexibility to turn parallel query on and off, or use parallel query with existing clusters, if you use Aurora MySQL 1.23 or 2.09 and higher.
- Only for Aurora MySQL before version 1.23: When you create or restore the DB cluster, make sure to choose the parallelquery engine mode.

Whether you create a new cluster or restore from a snapshot, you use the same techniques to add new DB instances that you do with other Aurora MySQL clusters.

Creating a parallel query cluster using the console

You can create a new parallel query cluster with the console as described following.

To create a parallel query cluster with the AWS Management Console

1. Follow the general AWS Management Console procedure in Creating an Amazon Aurora DB cluster (p. 118).
2. On the Select engine screen, choose Aurora MySQL.

For Engine version, choose Aurora MySQL 2.09 or higher, or Aurora MySQL 1.23 or higher if practical. With those versions, you have the fewest limitations on parallel query usage. Those versions also have the most flexibility to turn parallel query on or off at any time.
If it isn't practical to use a recent Aurora MySQL version for this cluster, choose **Show versions that support the parallel query feature**. Doing so filters the **Version** menu to show only the specific Aurora MySQL versions that are compatible with parallel query.

3. (For older versions only) For **Capacity type**, choose **Provisioned with Aurora parallel query enabled**. The AWS Management Console only displays this choice when you select an Aurora MySQL version lower than 1.23. For Aurora MySQL 1.23 or 2.09 and higher, you don't need to make any special choice to make the cluster compatible with parallel query.

4. (For recent versions only) For **Additional configuration**, choose a parameter group that you created for **DB cluster parameter group**. Using such a custom parameter group is required for Aurora MySQL 1.23 or 2.09 and higher. In your DB cluster parameter group, specify the parameter settings `aurora_parallel_query=ON` and `aurora_disable_hash_join=OFF`. Doing so turns on parallel query for the cluster, and enables the hash join optimization which works in combination with parallel query.

**To verify that a new cluster can use parallel query**

1. Create a cluster using the preceding technique.

2. (For recent versions only) Check that the `aurora_parallel_query` configuration setting is true, and that the `aurora_disable_hash_join` setting is false.

   ```
   mysql> select @@aurora_parallel_query;
   +-------------------------+
   | @@aurora_parallel_query |
   +-------------------------+
   |                       1 |
   +-------------------------+
   mysql> select @@aurora_disable_hash_join;
   +----------------------------+
   | @@aurora_disable_hash_join |
   +----------------------------+
   |                          0 |
   +----------------------------+
   ```

3. (For older versions only) Check that the `aurora_pq_supported` configuration setting is true.

   ```
   mysql> select @@aurora_pq_supported;
   +-----------------------+
   | @@aurora_pq_supported |
   +-----------------------+
   |                     1 |
   +-----------------------+
   ```

4. With some large tables and data-intensive queries, check the query plans to confirm that some of your queries are using the parallel query optimization. To do so, follow the procedure in **Verifying which statements use parallel query** (p. 709).

**Creating a parallel query cluster using the CLI**

You can create a new parallel query cluster with the CLI as described following.

**To create a parallel query cluster with the AWS CLI**

1. (Optional) Check which Aurora MySQL versions are compatible with parallel query clusters. To do so, use the `describe-db-engine-versions` command and check the value of the `SupportsParallelQuery` field. For an example, see **Checking Aurora MySQL version compatibility for parallel query** (p. 700).
2. (Optional) Create a custom DB cluster parameter group with the settings `aurora_parallel_query=ON` and `aurora_disable_hash_join=OFF`. Use commands such as the following:

```bash
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
```

If you perform this step, specify the option `--db-cluster-parameter-group-name` `my_cluster_parameter_group` in the subsequent `create-db-cluster` statement. Substitute the name of your own parameter group. If you omit this step, you create the parameter group and associate it with the cluster later, as described in Enabling and disabling parallel query (p. 705).

3. Follow the general AWS CLI procedure in Creating an Amazon Aurora DB cluster (p. 118).

4. Specify the following set of options:

   - For the `--engine` option, use `aurora` or `aurora-mysql`. These values produce parallel query clusters that are compatible with MySQL 5.6 or MySQL 5.7 respectively.
   - The value to use for the `--engine-mode` parameter depends on the engine version that you choose.
     
     For Aurora MySQL 1.23 or higher, or 2.09 or higher, specify `--engine-mode` `provisioned`. You can also omit the `--engine-mode` parameter, because provisioned is the default. In these versions, you can turn parallel query on or off for the default kind of Aurora MySQL clusters, instead of creating clusters dedicated to always using parallel query.

     Before Aurora MySQL 1.23, for the `--engine-mode` option, use `parallelquery`. The `--engine-mode` parameter applies to the `create-db-cluster` operation. Then the engine mode of the cluster is used automatically by subsequent `create-db-instance` operations.

   - For the `--db-cluster-parameter-group-name` option, specify the name of a DB cluster parameter group that you created and specified the parameter value `aurora_parallel_query=ON`. If you omit this option, you can create the cluster with a default parameter group and later modify it to use such a custom parameter group.

   - For the `--engine-version` option, use an Aurora MySQL version that's compatible with parallel query. Use the procedure from Planning for a parallel query cluster (p. 700) to get a list of versions if necessary. If practical, use at least 1.23.0 or 2.09.0. These versions and all higher ones contain substantial enhancements to parallel query.

The following code example shows how. Substitute your own value for each of the environment variables such as `#CLUSTER_ID`.

```bash
aws rds create-db-cluster --db-cluster-identifier #CLUSTER_ID--engine aurora-mysql --engine-version 5.7.mysql_aurora.2.09.0
   --master-username $MASTER_USER_ID --master-user-password $MASTER_USER_PW
   --db-cluster-parameter-group-name #CUSTOM_CLUSTER_PARAM_GROUP
aws rds create-db-cluster --db-cluster-identifier #CLUSTER_ID
   --engine aurora --engine-version 5.6.mysql_aurora.1.23.0
   --master-username $MASTER_USER_ID --master-user-password $MASTER_USER_PW
   --db-cluster-parameter-group-name #CUSTOM_CLUSTER_PARAM_GROUP
aws rds create-db-instance --db-instance-identifier #{INSTANCE_ID}-1
```
5. Verify that a cluster you created or restored has the parallel query feature available.

For Aurora MySQL 1.23 and 2.09 or higher: Check that the `aurora_parallel_query` configuration setting exists. If this setting has the value 1, parallel query is ready for you to use. If this setting has the value 0, set it to 1 before you can use parallel query. Either way, the cluster is capable of performing parallel queries.

```
mysql> select @@aurora_parallel_query;
+------------------------+
| @@aurora_parallel_query|
+------------------------+
|                      1 |
+------------------------+
```

Before Aurora MySQL 1.23: Check that the `aurora_pq_supported` configuration setting is true.

```
mysql> select @@aurora_pq_supported;
+-----------------------+
| @@aurora_pq_supported |
+-----------------------+
|                     1 |
+-----------------------+
```

**To restore a snapshot to a parallel query cluster with the AWS CLI**

1. Check which Aurora MySQL versions are compatible with parallel query clusters. To do so, use the `describe-db-engine-versions` command and check the value of the `SupportsParallelQuery` field. For an example, see Checking Aurora MySQL version compatibility for parallel query (p. 700). Decide which version to use for the restored cluster. If practical, choose Aurora MySQL 2.09.0 or higher for a MySQL 5.7-compatible cluster, or 1.23.0 or higher for a MySQL 5.6-compatible cluster.

2. Locate a Aurora MySQL-compatible cluster snapshot.

3. Follow the general AWS CLI procedure in Restoring from a DB cluster snapshot (p. 420).

4. The value to use for the `--engine-mode` parameter depends on the engine version that you choose.

   For Aurora MySQL 1.23 or higher, or 2.09 or higher, specify `--engine-mode provisioned`. You can also omit the `--engine-mode` parameter, because `provisioned` is the default. In these versions, you can turn parallel query on or off for your Aurora MySQL clusters, instead of creating clusters dedicated to always using parallel query.

   Before Aurora MySQL 1.23, specify `--engine-mode parallelquery`. The `--engine-mode` parameter applies to the `create-db-cluster` operation. Then the engine mode of the cluster is used automatically by subsequent `create-db-instance` operations.

```
aws rds restore-db-cluster-from-snapshot \
   --db-cluster-identifier mynewdbcluster \
   --snapshot-identifier mydbclustersnapshot \
   --engine aurora \
   --engine-mode parallelquery
```

5. Verify that a cluster you created or restored has the parallel query feature available. Use the same verification procedure as in Creating a parallel query cluster using the CLI (p. 702).
Enabling and disabling parallel query

Note
When parallel query is enabled, Aurora MySQL determines whether to use it at runtime for each query. In the case of joins, unions, subqueries, and so on, Aurora MySQL determines whether to use parallel query at runtime for each query block. For details, see Verifying which statements use parallel query (p. 709) and How parallel query works with SQL constructs (p. 715).

Aurora MySQL 1.23 and 2.09 or higher

In Aurora MySQL 1.23 and 2.09 or higher, you can enable and disable parallel query dynamically at both the global and session level for a DB instance by using the `aurora_parallel_query` option. You can change the `aurora_parallel_query` setting in your DB cluster group to turn parallel query on or off by default.

```
mysql> select @@aurora_parallel_query;
+------------------------+
| @@aurora_parallel_query|
+------------------------+
|                      1 |
+------------------------+
```

To toggle the `aurora_parallel_query` parameter at the session level, use the standard methods to change a client configuration setting. For example, you can do so through the `mysql` command line or within a JDBC or ODBC application. The command on the standard MySQL client is `set session aurora_pq = {'ON'/'OFF'}`. You can also add the session-level parameter to the JDBC configuration or within your application code to enable or disable parallel query dynamically.

You can permanently change the setting for the `aurora_parallel_query` parameter, either for a specific DB instance or for your whole cluster. If you specify the parameter value in a DB parameter group, that value only applies to specific DB instance in your cluster. If you specify the parameter value in a DB cluster parameter group, all DB instances in the cluster inherit the same setting. To toggle the `aurora_parallel_query` parameter, use the techniques for working with parameter groups, as described in Working with DB parameter groups and DB cluster parameter groups (p. 298). Follow these steps:

1. Create a custom cluster parameter group (recommended) or a custom DB parameter group.
2. In this parameter group, update `parallel_query` to the value that you want.
3. Depending on whether you created a DB cluster parameter group or a DB parameter group, attach the parameter group to your Aurora cluster or to the specific DB instances where you plan to use the parallel query feature.

   Tip
   Because `aurora_parallel_query` is a dynamic parameter, you don’t need to restart your cluster after changing this setting.

You can modify the parallel query parameter by using the `ModifyDBClusterParameterGroup` or `ModifyDBParameterGroup` API operation or the AWS Management Console.

Before Aurora MySQL 1.23

For these older versions, you can enable and disable parallel query dynamically at both the global and session level for a DB instance by using the `aurora_pq` option. On clusters where the parallel query feature is available, the parameter is enabled by default.

```
mysql> select @@aurora_pq;
+-------------+
|             |
+-------------+
```
To toggle the `aurora_pq` parameter at the session level, for example through the MySQL command line or within a JDBC or ODBC application, use the standard methods to change a client configuration setting. For example, the command on the standard MySQL client is `set session aurora_pq = {'ON'/'OFF'}`. You can also add the session-level parameter to the JDBC configuration or within your application code to enable or disable parallel query dynamically.

To toggle the `aurora_pq` parameter permanently, use the techniques for working with parameter groups, as described in Working with DB parameter groups and DB cluster parameter groups (p. 298). Follow these steps:

1. Create a custom cluster parameter group or DB instance parameter group. We recommend using a cluster parameter group, so that all DB instance in the cluster inherit the same settings.
2. In this parameter group, update `aurora_pq` to the value that you want.
3. Associate the custom cluster parameter group with the Aurora cluster where you plan to use the parallel query feature. Or, for a custom DB parameter group, associate it with one or more DB instances in the cluster.
4. Restart all the DB instances of the cluster.

You can modify the parallel query parameter by using the `ModifyDBClusterParameterGroup` or `ModifyDBParameterGroup` API operation or the AWS Management Console.

**Note**
When parallel query is enabled, Aurora MySQL determines whether to use it at runtime for each query. In the case of joins, unions, subqueries, and so on, Aurora MySQL determines whether to use parallel query at runtime for each query block. For details, see Verifying which statements use parallel query (p. 709) and How parallel query works with SQL constructs (p. 715).

### Enabling hash join for parallel query clusters

Parallel query is typically used for the kinds of resource-intensive queries that benefit from the hash join optimization. Thus, it's helpful to ensure that hash joins are enabled for clusters where you plan to use parallel query.

- For Aurora MySQL 5.6-compatible clusters before version 1.23, hash joins are always available in parallel query-enabled clusters. In this case, you don't need to take any action for the hash join feature. If you upgrade such clusters in the future, you do need to enable hash joins at that time.
- In Aurora MySQL 1.23 or 2.09 and higher, the parallel query and hash join settings are both turned off by default. When you enable parallel query for such a cluster, enable hash joins also. The simplest way to do so is to set the cluster configuration parameter `aurora_disable_hash_join=OFF`. For information about how to enable hash joins and use them effectively, see Working with hash joins in Aurora MySQL (p. 845).

### Enabling and disabling parallel query using the console

You can enable or disable parallel query at the DB instance level or the DB cluster level by working with parameter groups.

**To enable or disable parallel query for a DB cluster with the AWS Management Console**

1. Create a custom parameter group, as described in Working with DB parameter groups and DB cluster parameter groups (p. 298).
2. For Aurora MySQL 1.23 and 2.09 or higher: Update `aurora_parallel_query` to 1 (enabled) or 0 (disabled). On clusters where the parallel query feature is available, `aurora_parallel_query` is disabled by default.

   For Aurora MySQL before 1.23: Update `aurora_pq` to 1 (enabled) or 0 (disabled). On clusters where the parallel query feature is available, `aurora_pq` is enabled by default.

3. If you use a custom cluster parameter group, attach it to the Aurora DB cluster where you plan to use the parallel query feature. If you use a custom DVB parameter group, attach it to one or more DB instances in the cluster. We recommend using a cluster parameter group. Doing so makes sure that all DB instances in the cluster have the same settings for parallel query and associated features such as hash join.

### Enabling and disabling parallel query using the CLI

You can modify the parallel query parameter by using the `modify-db-cluster-parameter-group` or `modify-db-parameter-group` command. Choose the appropriate command depending on whether you specify the value of `aurora_parallel_query` through a DB cluster parameter group or a DB parameter group.

#### To enable or disable parallel query for a DB cluster with the CLI

- Modify the parallel query parameter by using the `modify-db-cluster-parameter-group` command. Use a command such as the following. Substitute the appropriate name for your own custom parameter group. Substitute either `ON` or `OFF` for the `ParameterValue` portion of the `--parameters` option.

  ```bash
  # Aurora MySQL 1.23 or 2.09 and higher:
  $ 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" }
  # Before Aurora MySQL 1.23:
  $ 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
  { "DBClusterParameterGroupName": "cluster_param_group_name" }
  ```

You can also enable or disable parallel query at the session level, for example through the `mysql` command line or within a JDBC or ODBC application. To do so, use the standard methods to change a client configuration setting. For example, the command on the standard MySQL client is `set session aurora_parallel_query = {'ON'/"OFF')} for Aurora MySQL 1.23 or 2.09 and higher. Before Aurora MySQL 1.23, the command is `set session aurora_pq = {'ON'/"OFF')}.

You can also add the session-level parameter to the JDBC configuration or within your application code to enable or disable parallel query dynamically.

### Upgrade considerations for parallel query

In Aurora MySQL 1.23 or 2.09 and higher, parallel query works for provisioned clusters and doesn't require the `parallelquery` engine mode parameter. Thus, you don't need to create a new cluster or
After you upgrade an earlier parallel query cluster to Aurora MySQL 1.23 or 2.09 and higher, you enable parallel query in the upgraded cluster. Parallel query is turned off by default in these versions, and the procedure for enabling it is different. The hash join optimization is also turned off by default and must be enabled separately. Thus, make sure that you enable these settings again after the upgrade. For instructions on doing so, see Enabling and disabling parallel query (p. 705) and Enabling hash join for parallel query clusters (p. 706).

In particular, you enable parallel query by using the configuration parameters `aurora_parallel_query=ON` and `aurora_disable_hash_join=OFF` instead of `aurora_pq_supported` and `aurora_pq`. The `aurora_pq_supported` and `aurora_pq` parameters are deprecated in the newer Aurora MySQL versions.

In the upgraded cluster, the `EngineMode` attribute has the value `provisioned` instead of `parallelquery`. To check whether parallel query is available for a specified engine version, now you check the value of the `SupportsParallelQuery` field in the output of the `describe-db-engine-versions` AWS CLI command. In earlier Aurora MySQL versions, you checked for the presence of `parallelquery` in the `SupportedEngineModes` list.

After you upgrade to Aurora MySQL 1.23 or 2.09 and higher, you can take advantage of the following features. These features aren't available to parallel query clusters running older Aurora MySQL versions.

- Performance Insights. For more information, see Using Amazon RDS Performance Insights (p. 514).
- Backtracking. For more information, see Backtracking an Aurora DB cluster (p. 677).
- Stopping and starting the cluster. For more information, see Stopping and starting an Amazon Aurora DB cluster (p. 323).

**Performance tuning for parallel query**

To manage the performance of a workload with parallel query, make sure that parallel query is used for the queries where this optimization helps the most.

To do so, you can do the following:

- Make sure that your biggest tables are compatible with parallel query. You might change table properties or recreate some tables so that queries for those tables can take advantage of the parallel query optimization. To learn how, see Creating schema objects to take advantage of parallel query (p. 709).
- Monitor which queries use parallel query. To learn how, see Monitoring parallel query (p. 712).
- Verify that parallel query is being used for the most data-intensive and long-running queries, and with the right level of concurrency for your workload. To learn how, see Verifying which statements use parallel query (p. 709).
- Fine-tune your SQL code to enable parallel query to apply to the queries that you expect. To learn how, see How parallel query works with SQL constructs (p. 715).
Creating schema objects to take advantage of parallel query

Before you create or modify tables that you plan to use for parallel query, make sure to familiarize yourself with the requirements described in Prerequisites (p. 699) and Limitations (p. 699).

Because parallel query requires tables to use the ROW_FORMAT=Compact or ROW_FORMAT=Dynamic setting, check your Aurora configuration settings for any changes to the INNODB_FILE_FORMAT configuration option. Issue the SHOW TABLE STATUS statement to confirm the row format for all the tables in a database.

Parallel query currently requires tables to be nonpartitioned. Thus, check your CREATE TABLE statements and SHOW CREATE TABLE output and remove any PARTITION BY clauses. For existing partitioned tables, first copy the data into nonpartitioned tables with the same column definitions and indexes. Then rename old and new tables so that the nonpartitioned table is used by existing queries and ETL workflows.

Before changing your schema to enable parallel query to work with more tables, make sure to test. Your tests should confirm if parallel query results in a net increase in performance for those tables. Also, make sure that the schema requirements for parallel query are otherwise compatible with your goals.

For example, before switching from ROW_FORMAT=Compressed to ROW_FORMAT=Compact or ROW_FORMAT=Dynamic, test the performance of workloads for the original and new tables. Also, consider other potential effects such as increased data volume.

Verifying which statements use parallel query

In typical operation, you don't need to perform any special actions to take advantage of parallel query. After a query meets the essential requirements for parallel query, the query optimizer automatically decides whether to use parallel query for each specific query.

If you run experiments in a development or test environment, you might find that parallel query isn't used because your tables are too small in number of rows or overall data volume. The data for the table might also be entirely in the buffer pool, especially for tables you created recently to perform experiments.

As you monitor or tune cluster performance, make sure to decide whether parallel query is being used in the appropriate contexts. You might adjust the database schema, settings, SQL queries, or even the cluster topology and application connection settings to take advantage of this feature.

To check if a query is using parallel query, check the query plan (also known as the "explain plan") by running the EXPLAIN statement. For examples of how SQL statements, clauses, and expressions affect EXPLAIN output for parallel query, see How parallel query works with SQL constructs (p. 715).

The following example demonstrates the difference between a traditional query plan and a parallel query plan. This explain plan is from Query 3 from the TPC-H benchmark. Many of the sample queries throughout this section use the tables from the TPC-H dataset. You can get the table definitions, queries, and the dbgen program that generates sample data from the TPC-h website.

```sql
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;

By default, the query might have a plan like the following. If you don't see hash join used in the query
plan, make sure that optimization is enabled first.

```
+----+-------------+----------+------------+------+---------------+------+---------+------+
| 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  | ALL | NULL       | NULL | NULL    | NULL |
| 14875240 |     3.33 | Using where; Using join buffer (Block Nested Loop) |
|  1 | SIMPLE      | lineitem | NULL       | ALL  | ALL | NULL       | NULL | NULL    | NULL |
| 59270573 |     3.33 | Using where; Using join buffer (Block Nested Loop) |
+----+-------------+----------+------------+------+---------------+------+---------+------+
```

You can enable hash join at the session level by issuing the following statement. Afterwards, try the
EXPLAIN statement again.

```
SET optimizer_switch='hash_join=on';
```

For information about how to enable hash joins permanently and use them effectively, see Working with
hash joins in Aurora MySQL (p. 845).

With hash join enabled but parallel query disabled, the query might have a plan like the following, which
uses hash join but not parallel query.

```
+----+-------------+----------+------------+------+---------------+------+---------+------+
| id | select_type | table    | partitions | type | possible_keys | key  | key_len | ref  |
| rows | filtered | 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) |
+----+-------------+----------+------------+------+---------------+------+---------+------+
```

After parallel query is enabled, two steps in this query plan can use the parallel query optimization, as
shown under the Extra column in the EXPLAIN output. The I/O-intensive and CPU-intensive processing
for those steps is pushed down to the storage layer.

```
+----+-------------+-----------+----------------+
| id | ... | Extra                      |
+----+-------------+-----------+----------------+
Verifying parallel query usage

The following example output shows the results of running the preceding query on a db.r4.2xlarge instance with a cold buffer pool. The query runs substantially faster when using parallel query.

**Note**
Because timings depend on many environmental factors, and this example query ran using an early version of parallel query, your results might be different. Always conduct your own performance tests to confirm the findings with your own environment, workload, and so on.

```sql
-- 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)
```

Many of the sample queries throughout this section use the tables from this TPC-H dataset, particularly the **PART** table, which has 20 million rows and the following definition.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>p_partkey</td>
<td>int(11)</td>
<td>NO</td>
<td>PRI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>p_name</td>
<td>varchar(55)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>p_mfgr</td>
<td>char(25)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>p_brand</td>
<td>char(10)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>p_type</td>
<td>varchar(25)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>p_size</td>
<td>int(11)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>p_container</td>
<td>char(10)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>p_retailprice</td>
<td>decimal(15,2)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>p_comment</td>
<td>varchar(23)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>

711
Experiment with your workload to get a sense of whether individual SQL statements can take advantage of parallel query. Then use the following monitoring techniques to help verify how often parallel query is used in real workloads over time. For real workloads, extra factors such as concurrency limits apply.

**Monitoring parallel query**

In addition to the Amazon CloudWatch metrics described in Monitoring Amazon Aurora DB cluster metrics (p. 489), Aurora provides other global status variables. You can use these global status variables to help monitor parallel query execution. They can give you insights into why the optimizer might use or not use parallel query in a given situation. To access these variables, you can use the `SHOW GLOBAL STATUS` command. You can also find these variables listed following.

A parallel query session isn't necessarily a one-to-one mapping with the queries performed by the database. For example, suppose that your query plan has two steps that use parallel query. In that case, the query involves two parallel sessions and the counters for requests attempted and requests successful are incremented by two.

When you experiment with parallel query by issuing `EXPLAIN` statements, expect to see increases in the counters designated as "not chosen" even though the queries aren't actually running. When you work with parallel query in production, you can check if the "not chosen" counters are increasing faster than you expect. At this point, you can adjust so that parallel query runs for the queries that you expect. To do so, you can change your cluster settings, query mix, DB instances where parallel query is enabled, and so on.

These counters are tracked at the DB instance level. When you connect to a different endpoint, you might see different metrics because each DB instance runs its own set of parallel queries. You might also see different metrics when the reader endpoint connects to a different DB instance for each session.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Aurora_pq_request_attempted</code></td>
<td>The number of parallel query sessions requested. This value might represent more than one session per query, depending on SQL constructs such as subqueries and joins.</td>
</tr>
<tr>
<td><code>Aurora_pq_request_executed</code></td>
<td>The number of parallel query sessions run successfully.</td>
</tr>
<tr>
<td><code>Aurora_pq_request_failed</code></td>
<td>The number of parallel query sessions that returned an error to the client. In some cases, a request for a parallel query might fail, for example due to a problem in the storage layer. In these cases, the query part that failed is retried using the nonparallel query mechanism. If the retried query also fails, an error is returned to the client and this counter is incremented.</td>
</tr>
<tr>
<td><code>Aurora_pq_pages_pushed_down</code></td>
<td>The number of data pages (each with a fixed size of 16 KiB) where parallel query avoided a network transmission to the head node.</td>
</tr>
<tr>
<td><code>Aurora_pq_bytes_returned</code></td>
<td>The number of bytes for the tuple data structures transmitted to the head node during parallel queries. Divide by 16,384 to compare against <code>Aurora_pq_pages_pushed_down</code>.</td>
</tr>
<tr>
<td><code>Aurora_pq_request_not_chosen</code></td>
<td>The number of times parallel query wasn't chosen to satisfy a query. This value is the sum of several</td>
</tr>
</tbody>
</table>
Aurora_pq_request_not_chosen_below_min_rows | The number of times parallel query wasn't chosen due to the number of rows in the table. An EXPLAIN statement can increment this counter even though the query isn't actually performed.

Aurora_pq_request_not_chosen_small_table | The number of times parallel query wasn't chosen due to the overall size of the table, as determined by number of rows and average row length. An EXPLAIN statement can increment this counter even though the query isn't actually performed.

Aurora_pq_request_not_chosen_high_buffer_pool_pct | The number of times parallel query wasn't chosen because a high percentage of the table data (currently, greater than 95 percent) was already in the buffer pool. In these cases, the optimizer determines that reading the data from the buffer pool is more efficient. An EXPLAIN statement can increment this counter even though the query isn't actually performed.

Aurora_pq_request_not_chosen_few_pages_outside_buffer_pool | The number of times parallel query wasn't chosen, even though less than 95 percent of the table data was in the buffer pool, because there wasn't enough unbuffered table data to make parallel query worthwhile.

Aurora_pq_max_concurrent_requests | The maximum number of parallel query sessions that can run concurrently on this Aurora DB instance. This is a fixed number that depends on the AWS DB instance class.

Aurora_pq_request_in_progress | The number of parallel query sessions currently in progress. This number applies to the particular Aurora DB instance that you are connected to, not the entire Aurora DB cluster. To see if a DB instance is close to its concurrency limit, compare this value to Aurora_pq_max_concurrent_requests.

Aurora_pq_request_throttled | The number of times parallel query wasn't chosen due to the maximum number of concurrent parallel queries already running on a particular Aurora DB instance.

Aurora_pq_request_not_chosen_long_trx | The number of parallel query requests that used the nonparallel query processing path, due to the query being started inside a long-running transaction. An EXPLAIN statement can increment this counter even though the query isn't actually performed.
<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora_pq_request_not_chosen_unsupported_access</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the WHERE clause doesn’t meet the criteria for parallel query. This result can occur if the query doesn’t require a data-intensive scan, or if the query is a DELETE or UPDATE statement.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_column_bit</td>
<td>The number of parallel query requests that use the nonparallel query processing path because of an unsupported data type in the list of projected columns.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_column_geometry</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the table has columns with the GEOMETRY data type.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_column_lob</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the table has columns with a LOB data type, or VARCHAR columns that are stored externally due the declared length.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_column_virtual</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the table contains a virtual column.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_custom_charset</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the table has columns with a custom character set.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_fast_ddl</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the table is currently being altered by a fast DDL ALTER statement.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_full_text_index</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the table has full-text indexes.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_index_hint</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the query includes an index hint.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_innodb_table_format</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the table uses an unsupported InnoDB row format. Aurora parallel query only applies to the COMPACT, REDUNDANT, and DYNAMIC row formats.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_no_where_clause</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the query doesn't include any WHERE clause.</td>
</tr>
<tr>
<td>Aurora_pq_request_not_chosen_range_scan</td>
<td>The number of parallel query requests that use the nonparallel query processing path because the query uses a range scan on an index.</td>
</tr>
</tbody>
</table>
### How parallel query works with SQL constructs

In the following section, you can find more detail about why particular SQL statements use or don’t use parallel query. This section also details how Aurora MySQL features interact with parallel query. This information can help you diagnose performance issues for a cluster that uses parallel query or understand how parallel query applies for your particular workload.

The decision to use parallel query relies on many factors that occur at the moment that the statement runs. Thus, parallel query might be used for certain queries always, never, or only under certain conditions.

**Tip**

When you view these examples in HTML, you can use the Copy widget in the upper-right corner of each code listing to copy the SQL code to try yourself. Using the Copy widget avoids copying the extra characters around the mysql> prompt and --> continuation lines.

**Topics**

- EXPLAIN statement (p. 716)
- WHERE clause (p. 717)
- Data definition language (DDL) (p. 718)
- Column data types (p. 718)
- Partitioned tables (p. 719)
- Function calls in WHERE clause (p. 719)
- Aggregate functions, GROUP BY clauses, and HAVING clauses (p. 720)
- LIMIT clause (p. 720)
- Comparison operators (p. 720)
- Joins (p. 721)
- Subqueries (p. 722)
- UNION (p. 722)
- Views (p. 723)
- Data manipulation language (DML) statements (p. 723)
EXPLAIN statement

As shown in examples throughout this section, the EXPLAIN statement indicates whether each stage of a query is currently eligible for parallel query. It also indicates which aspects of a query can be pushed down to the storage layer. The most important items in the query plan are the following:

- A value other than NULL for the key column suggests that the query can be performed efficiently using index lookups, and parallel query is unlikely.
- A small value for the rows column (a value not in the millions) suggests that the query isn't accessing enough data to make parallel query worthwhile. This means that parallel query is unlikely.
- The Extra column shows you if parallel query is expected to be used. This output looks like the following example.

Using parallel query (A columns, B filters, C exprs; D extra)

<table>
<thead>
<tr>
<th>id</th>
<th>select_type</th>
<th>table</th>
<th>...</th>
<th>rows</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SIMPLE</td>
<td>part</td>
<td>...</td>
<td>20427936</td>
<td></td>
</tr>
</tbody>
</table>

The columns number represents how many columns are referred to in the query block.

The filters number represents the number of WHERE predicates representing a simple comparison of a column value to a constant. The comparison can be for equality, inequality, or a range. Aurora can parallelize these kinds of predicates most effectively.

The exprs number represents the number of expressions such as function calls, operators, or other expressions that can also be parallelized, though not as effectively as a filter condition.

The extra number represents how many expressions can't be pushed down and are performed by the head node.

For example, consider the following EXPLAIN output.

```sql
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;
```

```
<table>
<thead>
<tr>
<th>id</th>
<th>select_type</th>
<th>table</th>
<th>...</th>
<th>rows</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SIMPLE</td>
<td>part</td>
<td>...</td>
<td>20427936</td>
<td></td>
</tr>
</tbody>
</table>
```

The information from the Extra column shows that five columns are extracted from each row to evaluate the query conditions and construct the result set. One WHERE predicate involves a filter, that is, a column that is directly tested in the WHERE clause. Two WHERE clauses require evaluating more complicated expressions, in this case involving function calls. The 0 extra field confirms that all
the operations in the WHERE clause are pushed down to the storage layer as part of parallel query processing.

In cases where parallel query isn't chosen, you can typically deduce the reason from the other columns of the EXPLAIN output. For example, the rows value might be too small, or the possible_keys column might indicate that the query can use an index lookup instead of a data-intensive scan. The following example shows a query where the optimizer can estimate that the query will scan only a small number of rows. It does so based on the characteristics of the primary key. In this case, parallel query isn't required.

```sql
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 |
|    | SIMPLE      | part  | range | PRIMARY      | PRIMARY | 4       | NULL | 99   |
|    |             |       |       |              |         |         |      |      |
|    |             |       |       |              |         |         |      |      |
|    |             |       |       |              |         |         |      |      |
```

The output showing whether parallel query will be used takes into account all available factors at the moment that the EXPLAIN statement is run. The optimizer might make a different choice when the query is actually run, if the situation changed in the meantime. For example, EXPLAIN might report that a statement will use parallel query. But when the query is actually run later, it might not use parallel query based on the conditions then. Such conditions can include several other parallel queries running concurrently. They can also include rows being deleted from the table, a new index being created, too much time passing within an open transaction, and so on.

**WHERE clause**

For a query to use the parallel query optimization, it must include a WHERE clause.

The parallel query optimization speeds up many kinds of expressions used in the WHERE clause:

- Simple comparisons of a column value to a constant, known as filters. These comparisons benefit the most from being pushed down to the storage layer. The number of filter expressions in a query is reported in the EXPLAIN output.
- Other kinds of expressions in the WHERE clause are also pushed down to the storage layer where possible. The number of such expressions in a query is reported in the EXPLAIN output. These expressions can be function calls, LIKE operators, CASE expressions, and so on.
- Certain functions and operators aren't currently pushed down by parallel query. The number of such expressions in a query is reported as the extra counter in the EXPLAIN output. The rest of the query can still use parallel query.
- While expressions in the select list aren't pushed down, queries containing such functions can still benefit from reduced network traffic for the intermediate results of parallel queries. For example, queries that call aggregation functions in the select list can benefit from parallel query, even though the aggregation functions aren't pushed down.

For example, the following query does a full-table scan and processes all the values for the P_BRAND column. However, it doesn't use parallel query because the query doesn't include any WHERE clause.

```sql
mysql> explain select count(*), p_brand from part group by p_brand;
+----+-------------+-------+-----------------+---------------+--------+---------+------+------+
| id | select_type | table | type | possible_keys | key | key_len | ref  | rows |
|    | SIMPLE      | part  | range | PRIMARY        |     |         |      |      |
|    |             |       |       |               |     |         |      |      |
|    |             |       |       |               |     |         |      |      |
```
In contrast, the following query includes WHERE predicates that filter the results, so parallel query can be applied:

```sql
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;
```

If the optimizer estimates that the number of returned rows for a query block is small, parallel query isn't used for that query block. The following example shows a case where a greater-than operator on the primary key column applies to millions of rows, which causes parallel query to be used. The converse less-than test is estimated to apply to only a few rows and doesn't use parallel query.

```sql
mysql> explain select count(*) from part where p_partkey > 10;
```

```sql
mysql> explain select count(*) from part where p_partkey < 10;
```

**Data definition language (DDL)**

Parallel query is only available for tables for which no fast data definition language (DDL) operations are pending. For information about fast DDL, see Altering tables in Amazon Aurora using fast DDL (p. 693).

**Column data types**

`TEXT`, `BLOB`, `JSON`, and `GEOMETRY` data types aren't supported with parallel query. A query that refers to any columns of these types can't use parallel query.
Variable-length columns (VARCHAR and CHAR data types) are compatible with parallel query up to a maximum declared length of 768 bytes. A query that refers to any columns of the types declared with a longer maximum length can't use parallel query. For columns that use multibyte character sets, the byte limit takes into account the maximum number of bytes in the character set. For example, for the character set utf8mb4 (which has a maximum character length of 4 bytes), a VARCHAR(192) column is compatible with parallel query but a VARCHAR(193) column isn't.

Partitioned tables

Currently, partitioned tables aren't supported for parallel query. You can use partitioned tables in parallel query clusters. Queries against those tables use the nonparallel query processing path.

Note

A join, union, or other multipart query can partially use parallel query, even if some query blocks refer to partitioned tables. The query blocks that refer only to nonpartitioned tables can use the parallel query optimization.

Function calls in WHERE clause

Aurora can apply the parallel query optimization to calls to most built-in functions in the WHERE clause. Parallelizing these function calls offloads some CPU work from the head node. Evaluating the predicate functions in parallel during the earliest query stage helps Aurora minimize the amount of data transmitted and processed during later stages.

Currently, the parallelization doesn't apply to function calls in the select list. Those functions are evaluated by the head node, even if identical function calls appear in the WHERE clause. The original values from relevant columns are included in the tuples transmitted from the storage nodes back to the head node. The head node performs any transformations such as UPPER, CONCATENATE, and so on to produce the final values for the result set.

In the following example, parallel query parallelizes the call to LOWER because it appears in the WHERE clause. Parallel query doesn't affect the calls to SUBSTR and UPPER because they appear in the select list.

```
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) |  
|----|...

The same considerations apply to other expressions, such as CASE expressions or LIKE operators. For example, the following example shows that parallel query evaluates the CASE expression and LIKE operators in the WHERE clause.

```
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;
```
Aggregate functions, GROUP BY clauses, and HAVING clauses

Queries involving aggregate functions are often good candidates for parallel query, because they involve scanning large numbers of rows within large tables. Aggregate function calls in the select list or the HAVING clause aren't pushed down to the storage layer. However, parallel query can still improve the performance of such queries with aggregate functions. It does so by first extracting column values from the raw data pages in parallel at the storage layer. It then transmits those values back to the head node in a compact tuple format instead of as entire data pages. As always, the query requires at least one WHERE predicate for parallel query to be activated.

The following simple examples illustrate the kinds of aggregate queries that can benefit from parallel query. They do so by returning intermediate results in compact form to the head node, filtering nonmatching rows from the intermediate results, or both.

```sql
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) |
+----+...+----------------------------------------------------------------------------+
```

LIMIT clause

Currently, parallel query isn't used for any query block that includes a LIMIT clause. Parallel query might still be used for earlier query phases with GROUP by, ORDER by, or joins.

Comparison operators

The optimizer estimates how many rows to scan to evaluate comparison operators, and determines whether to use parallel query based on that estimate.
The first example following shows that an equality comparison against the primary key column can be performed efficiently without parallel query. The second example following shows that a similar comparison against an unindexed column requires scanning millions of rows and therefore can benefit from parallel query.

```
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) |
+----+---+--------------------------+
```

The same considerations apply for not-equals tests and for range comparisons such as less than, greater than or equal to, or BETWEEN. The optimizer estimates the number of rows to scan, and determines whether parallel query is worthwhile based on the overall volume of I/O.

**Joins**

Join queries with large tables typically involve data-intensive operations that benefit from the parallel query optimization. The comparisons of column values between multiple tables (that is, the join predicates themselves) currently aren’t parallelized. However, parallel query can push down some of the internal processing for other join phases, such as constructing the Bloom filter during a hash join. Parallel query can apply to join queries even without a WHERE clause. Therefore, a join query is an exception to the rule that a WHERE clause is required to use parallel query.

Each phase of join processing is evaluated to check if it is eligible for parallel query. If more than one phase can use parallel query, these phases are performed in sequence. Thus, each join query counts as a single parallel query session in terms of concurrency limits.

For example, when a join query includes WHERE predicates to filter the rows from one of the joined tables, that filtering option can use parallel query. As another example, suppose that a join query uses the hash join mechanism, for example to join a big table with a small table. In this case, the table scan to produce the Bloom filter data structure might be able to use parallel query.

**Note**

Parallel query is typically used for the kinds of resource-intensive queries that benefit from the hash join optimization. Before Aurora MySQL 1.23, hash joins are always available in parallel query-enabled clusters. In Aurora MySQL 1.23 and 2.09 or higher, the parallel query and hash join settings are both turned off by default. When you enable parallel query for such a cluster, enable hash joins also. For information about how to enable hash joins and use them effectively, see *Working with hash joins in Aurora MySQL* (p. 845).

```
mysql> explain select count(*) from orders join customer where o_custkey = c_custkey;
+----+---+---------+--------+---------------+-------------+...+-----------+
| id |...| table   | type  | possible_keys | key         |...| rows      | Extra |
+----+---+---------+--------+---------------+-------------+...+-----------+
```
Parallel query and SQL constructs

For a join query that uses the nested loop mechanism, the outermost nested loop block might use parallel query. The use of parallel query depends on the same factors as usual, such as the presence of additional filter conditions in the WHERE clause.

```sql
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;
```

Subqueries

The outer query block and inner subquery block might each use parallel query, or not. Whether they do is based on the usual characteristics of the table, WHERE clause, and so on, for each block. For example, the following query uses parallel query for the subquery block but not the outer block.

```sql
mysql> explain select count(*) from part where p_partkey < (select max(p_partkey) from part where p_name like '%vanilla%');
```

Currently, correlated subqueries can't use the parallel query optimization.

**UNION**

Each query block in a UNION query can use parallel query, or not, based on the usual characteristics of the table, WHERE clause, and so on, for each part of the UNION.
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
Each UNION clause within the query is run sequentially. Even if the query includes multiple stages that all use parallel query, it only runs a single parallel query at any one time. Therefore, even a complex multistage query only counts as 1 toward the limit of concurrent parallel queries.

Views
The optimizer rewrites any query using a view as a longer query using the underlying tables. Thus, parallel query works the same whether table references are views or real tables. All the same considerations about whether to use parallel query for a query, and which parts are pushed down, apply to the final rewritten query.

For example, the following query plan shows a view definition that usually doesn't use parallel query. When the view is queried with additional WHERE clauses, Aurora MySQL uses 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) |
|  2 |...| 20427936 | Using where; Using parallel query (2 columns, 0 filters, 1 exprs; 0 extra) |
| NULL | UNION RESULT | <union1,2> |...|     NULL | Using temporary |
+----+--------------+...+----------
+----------------------------------------------------------------------------+

Data manipulation language (DML) statements
The INSERT statement can use parallel query for the SELECT phase of processing, if the SELECT part meets the other conditions for parallel query.

mysql> explain insert into part_subset select * from part where p_mfgr = 'Manufacturer#1';
+----+...+----------
| id |...| rows     | Extra
|    |...|----------|-------|
+----+--------------+...+----------
+----------------------------------------------------------------------------+
Note
Typically, after an INSERT statement, the data for the newly inserted rows is in the buffer pool. Therefore, a table might not be eligible for parallel query immediately after inserting a large number of rows. Later, after the data is evicted from the buffer pool during normal operation, queries against the table might begin using parallel query again.

The CREATE TABLE AS SELECT statement doesn’t use parallel query, even if the SELECT portion of the statement would otherwise be eligible for parallel query. The DDL aspect of this statement makes it incompatible with parallel query processing. In contrast, in the INSERT ... SELECT statement, the SELECT portion can use parallel query.

Parallel query is never used for DELETE or UPDATE statements, regardless of the size of the table and predicates in the WHERE clause.

Transactions and locking
You can use all the isolation levels on the Aurora primary instance.

On Aurora reader DB instances, parallel query applies to statements performed under the REPEATABLE READ isolation level. Aurora MySQL versions 1.23 and 2.09 or higher can also use the READ COMMITTED isolation level on reader DB instances. REPEATABLE READ is the default isolation level for Aurora reader DB instances. To use READ COMMITTED isolation level on reader DB instances requires setting the aurora_read_replica_read_committed configuration option at the session level.

For more information about Aurora isolation levels, see Aurora MySQL isolation levels (p. 865).

After a big transaction is finished, the table statistics might be stale. Such stale statistics might require an ANALYZE TABLE statement before Aurora can accurately estimate the number of rows. A large-scale DML statement might also bring a substantial portion of the table data into the buffer pool. Having this data in the buffer pool can lead to parallel query being chosen less frequently for that table until the data is evicted from the pool.

When your session is inside a long-running transaction (by default, 10 minutes), further queries inside that session don’t use parallel query. A timeout can also occur during a single long-running query. This type of timeout might happen if the query runs for longer than the maximum interval (currently 10 minutes) before the parallel query processing starts.

You can reduce the chance of starting long-running transactions accidentally by setting autocommit=1 in mysql sessions where you perform ad hoc (one-time) queries. Even a SELECT statement against a table begins a transaction by creating a read view. A read view is a consistent set of data for subsequent queries that remains until the transaction is committed. Be aware of this restriction also when using JDBC or ODBC applications with Aurora, because such applications might run with the autocommit setting turned off.

The following example shows how, with the autocommit setting turned off, running a query against a table creates a read view that implicitly begins a transaction. Queries that are run shortly afterward
can still use parallel query. However, after a pause of several minutes, queries are no longer eligible for parallel query. Ending the transaction with COMMIT or ROLLBACK restores parallel query eligibility.

```sql
mysql> set autocommit=0;

mysql> explain select sql_no_cache count(*) from part_txn where p_retailprice > 10.0;
+----+...+---------+-------------+
| id |...| rows    | Extra       |
| 2  |...| 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_txn where p_retailprice > 10.0;
+------------+
| sleep(720) |
+------------+
| 0          |
+------------+
1 row in set (12 min 0.00 sec)

mysql> commit;

mysql> explain select sql_no_cache count(*) from part_txn where p_retailprice > 10.0;
+----+...+---------+-------------+
| id |...| rows    | Extra       |
| 1  |...| 2976129 | Using where; Using parallel query (1 columns, 1 filters, 0 exprs; 0 extra) |
+----+...+---------+-------------+
```

To see how many times queries weren't eligible for parallel query because they were inside long-running transactions, check the status variable `Aurora_pq_not_chosen_long_trx`.

```sql
mysql> show global status like '%pq%trx%';
+-------------------------------+-------+
| Variable_name                 | Value |
| Aurora_pq_not_chosen_long_trx | 4     |
+-------------------------------+-------+
```

Any SELECT statement that acquires locks, such as the SELECT FOR UPDATE or SELECT LOCK IN SHARE MODE syntax, can't use parallel query.

Parallel query can work for a table that is locked by a LOCK TABLES statement.

```sql
mysql> explain select o_orderpriority, o_shippriority from orders where o_clerk = 'Clerk#000095055';
```
B-tree indexes

The statistics gathered by the `ANALYZE TABLE` statement help the optimizer to decide when to use parallel query or index lookups, based on the characteristics of the data for each column. Keep statistics current by running `ANALYZE TABLE` after DML operations that make substantial changes to the data within a table.

If index lookups can perform a query efficiently without a data-intensive scan, Aurora might use index lookups. Doing so avoids the overhead of parallel query processing. There are also concurrency limits on the number of parallel queries that can run simultaneously on any Aurora DB cluster. Make sure to use best practices for indexing your tables, so that your most frequent and most highly concurrent queries use index lookups.

Full-text search (FTS) indexes

Currently, parallel query isn’t used for tables that contain a full-text search index, regardless of whether the query refers to such indexed columns or uses the `MATCH` operator.

Built-in caching mechanisms

Aurora includes built-in caching mechanisms, namely the buffer pool and the query cache. The Aurora optimizer chooses between these caching mechanisms and parallel query depending on which one is most effective for a particular query.

When a parallel query filters rows and transforms and extracts column values, data is transmitted back to the head node as tuples rather than as data pages. Therefore, running a parallel query doesn’t add any pages to the buffer pool, or evict pages that are already in the buffer pool.

Aurora checks the number of pages of table data that are present in the buffer pool, and what proportion of the table data that number represents. Aurora uses that information to determine whether it is more efficient to use parallel query (and bypass the data in the buffer pool). Alternatively, Aurora might use the nonparallel query processing path, which uses data cached in the buffer pool. Which pages are cached and how data-intensive queries affect caching and eviction depends on configuration settings related to the buffer pool. Therefore, it can be hard to predict whether any particular query uses parallel query, because the choice depends on the ever-changing data within the buffer pool.
Also, Aurora imposes concurrency limits on parallel queries. Because not every query uses parallel query, tables that are accessed by multiple queries simultaneously typically have a substantial portion of their data in the buffer pool. Therefore, Aurora often doesn’t choose these tables for parallel queries.

When you run a sequence of nonparallel queries on the same table, the first query might be slow due to the data not being in the buffer pool. Then the second and subsequent queries are much faster because the buffer pool is now "warmed up". Parallel queries typically show consistent performance from the very first query against the table. When conducting performance tests, benchmark the nonparallel queries with both a cold and a warm buffer pool. In some cases, the results with a warm buffer pool can compare well to parallel query times. In these cases, consider factors such as the frequency of queries against that table. Also consider whether it is worthwhile to keep the data for that table in the buffer pool.

The query cache avoids rerunning a query when an identical query is submitted and the underlying table data hasn’t changed. Queries optimized by parallel query feature can go into the query cache, effectively making them instantaneous when run again.

**Note**
When conducting performance comparisons, the query cache can produce artificially low timing numbers. Therefore, in benchmark-like situations, you can use the `sql_no_cache` hint. This hint prevents the result from being served from the query cache, even if the same query had been run previously. The hint comes immediately after the `SELECT` statement in a query. Many parallel query examples in this topic include this hint, to make query times comparable between versions of the query that are enabled with parallel query and not. Make sure that you remove this hint from your source when you move to production use of parallel query.

**MyISAM temporary tables**

The parallel query optimization only applies to InnoDB tables. Because Aurora MySQL uses MyISAM behind the scenes for temporary tables, internal query phases involving temporary tables never use parallel query. These query phases are indicated by `Using temporary` in the EXPLAIN output.

### Using advanced auditing with an Amazon Aurora MySQL DB cluster

You can use the high-performance Advanced Auditing feature in Amazon Aurora MySQL to audit database activity. To do so, you enable the collection of audit logs by setting several DB cluster parameters. When Advanced Auditing is enabled, you can use it to log any combination of supported events. You can view or download the audit logs to review them.

**Note**
You can publish Aurora MySQL general, slow, audit, and error log data to a log group in CloudWatch Logs. For more information, see Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs (p. 824).

### Enabling advanced auditing

Use the parameters described in this section to enable and configure Advanced Auditing for your DB cluster.

Use the `server_audit_logging` parameter to enable or disable Advanced Auditing, and the `server_audit_events` parameter to specify what events to log.

Use the `server_audit_excl_users` and `server_audit_incl_users` parameters to specify who gets audited. If `server_audit_excl_users` and `server_audit_incl_users` are empty
(the default), all users are audited. If you add users to `server_audit_incl_users` and leave `server_audit_excl_users` empty, then only those users are audited. If you add users to `server_audit_excl_users` and leave `server_audit_incl_users` empty, then only those users are not audited, and all other users are. If you add the same users to both `server_audit_excl_users` and `server_audit_incl_users`, then those users are audited because `server_audit_incl_users` is given higher priority.

Configure Advanced Auditing by setting these parameters in the parameter group used by your DB cluster. You can use the procedure shown in Modifying parameters in a DB parameter group (p. 303) to modify DB cluster parameters using the AWS Management Console. You can use the `modify-db-cluster-parameter-group` AWS CLI command or the `ModifyDBClusterParameterGroup` Amazon RDS API command to modify DB cluster parameters programmatically.

Modifying these parameters doesn't require a DB cluster restart.

**server_audit_logging**

Enables or disables Advanced Auditing. This parameter defaults to OFF; set it to ON to enable Advanced Auditing.

**server_audit_events**

Contains the comma-delimited list of events to log. Events must be specified in all caps, and there should be no white space between the list elements, for example: `CONNECT, QUERY_DDL`. This parameter defaults to an empty string.

You can log any combination of the following events:

- **CONNECT** – Logs both successful and failed connections and also disconnections. This event includes user information.
- **QUERY** – Logs all queries in plain text, including queries that fail due to syntax or permission errors.
- **QUERY_DCL** – Similar to the QUERY event, but returns only data control language (DCL) queries (GRANT, REVOKE, and so on).
- **QUERY_DDL** – Similar to the QUERY event, but returns only data definition language (DDL) queries (CREATE, ALTER, and so on).
- **QUERY_DML** – Similar to the QUERY event, but returns only data manipulation language (DML) queries (INSERT, UPDATE, and so on, and also SELECT).
- **TABLE** – Logs the tables that were affected by query execution.

**server_audit_excl_users**

Contains the comma-delimited list of user names for users whose activity isn't logged. There should be no white space between the list elements, for example: `rdsadmin, user_1, user_2`. This parameter defaults to an empty string. The maximum length is 1024 characters. Specified user names must match corresponding values in the `User` column of the `mysql.user` table. For more information about user names, see the MySQL documentation.

Connect and disconnect events aren't affected by this variable; they are always logged if specified. A user is logged if that user is also specified in the `server_audit_incl_users` parameter, because that setting has higher priority than `server_audit_excl_users`.

**server_audit_incl_users**

Contains the comma-delimited list of user names for users whose activity is logged. There should be no white space between the list elements, for example: `user_3, user_4`. This parameter defaults to an empty string. The maximum length is 1024 characters. Specified user names must match corresponding
values in the `User` column of the `mysql.user` table. For more information about user names, see the MySQL documentation.

Connect and disconnect events aren't affected by this variable; they are always logged if specified. A user is logged even if that user is also specified in the `serverAuditExclUsers` parameter, because `serverAuditInclUsers` has higher priority.

## Viewing audit logs

You can view and download the audit logs by using the console. On the Databases page, choose the DB instance to show its details, then scroll to the Logs section.

To download a log file, choose that file in the Logs section and then choose Download.

You can also get a list of the log files by using the `describe-db-log-files` AWS CLI command. You can download the contents of a log file by using the `download-db-log-file-portion` AWS CLI command. For more information, see Viewing and listing database log files (p. 618) and Downloading a database log file (p. 618).

## Audit log details

Log files are in UTF-8 format. Logs are written in multiple files, the number of which varies based on instance size. To see the latest events, you might have to review all of the audit log files.

Log entries are not in sequential order. You can use the timestamp value for ordering.

Log files are rotated when they reach 100 MB in aggregate. This limit is not configurable.

The audit log files include the following comma-delimited information in rows, in the specified order:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>The Unix time stamp for the logged event with microsecond precision.</td>
</tr>
<tr>
<td>serverhost</td>
<td>The name of the instance that the event is logged for.</td>
</tr>
<tr>
<td>username</td>
<td>The connected user name of the user.</td>
</tr>
<tr>
<td>host</td>
<td>The host that the user connected from.</td>
</tr>
<tr>
<td>connectionid</td>
<td>The connection ID number for the logged operation.</td>
</tr>
<tr>
<td>queryid</td>
<td>The query ID number, which can be used for finding the relational table events and related queries. For <code>TABLE</code> events, multiple lines are added.</td>
</tr>
</tbody>
</table>
### Single-master replication with Amazon Aurora MySQL

The Aurora MySQL replication features are key to the high availability and performance of your cluster. Aurora makes it easy to create or resize clusters with up to 15 Aurora Replicas.

All the replicas work from the same underlying data. If some database instances go offline, others remain available to continue processing queries or to take over as the writer if needed. Aurora automatically spreads your read-only connections across multiple database instances, helping an Aurora cluster to support query-intensive workloads.

Following, you can find information about how Aurora MySQL replication works and how to fine-tune replication settings for best availability and performance.

**Note**

Following, you can learn about replication features for Aurora clusters using single-master replication. This kind of cluster is the default for Aurora. For information about Aurora multi-master clusters, see Working with Aurora multi-master clusters (p. 766).

**Topics**

- Using Aurora replicas (p. 730)
- Replication options for Amazon Aurora MySQL (p. 731)
- Performance considerations for Amazon Aurora MySQL replication (p. 732)
- High availability considerations for Amazon Aurora MySQL replication (p. 732)
- Monitoring Amazon Aurora MySQL replication (p. 732)
- Replicating Amazon Aurora MySQL DB clusters across AWS Regions (p. 733)
- Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster (binary log replication) (p. 743)
- Using GTID-based replication for Aurora MySQL (p. 762)

### Using Aurora replicas

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region. Although the DB cluster volume is made up of multiple copies of the data for the DB cluster, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster. For more information about Aurora Replicas, see Aurora Replicas (p. 57).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operation</td>
<td>The recorded action type. Possible values are: CONNECT, QUERY, READ, WRITE,</td>
</tr>
<tr>
<td></td>
<td>CREATE, ALTER, RENAME, and DROP.</td>
</tr>
<tr>
<td>database</td>
<td>The active database, as set by the USE command.</td>
</tr>
<tr>
<td>object</td>
<td>For QUERY events, this value indicates the query that the database performed.</td>
</tr>
<tr>
<td></td>
<td>For TABLE events, it indicates the table name.</td>
</tr>
<tr>
<td>retcode</td>
<td>The return code of the logged operation.</td>
</tr>
</tbody>
</table>
Aurora Replicas work well for read scaling because they are fully dedicated to read operations on your cluster volume. Write operations are managed by the primary instance. Because the cluster volume is shared among all instances in your Aurora MySQL DB cluster, no additional work is required to replicate a copy of the data for each Aurora Replica. In contrast, MySQL read replicas must replay, on a single thread, all write operations from the source DB instance to their local data store. This limitation can affect the ability of MySQL read replicas to support large volumes of read traffic.

With Aurora MySQL, when an Aurora Replica is deleted, its instance endpoint is removed immediately, and the Aurora Replica is removed from the reader endpoint. If there are statements running on the Aurora Replica that is being deleted, there is a three minute grace period. Existing statements can finish gracefully during the grace period. When the grace period ends, the Aurora Replica is shut down and deleted.

**Important**

Aurora Replicas for Aurora MySQL always use the `REPEATABLE READ` default transaction isolation level for operations on InnoDB tables. You can use the `SET TRANSACTION ISOLATION LEVEL` command to change the transaction level only for the primary instance of an Aurora MySQL DB cluster. This restriction avoids user-level locks on Aurora Replicas, and allows Aurora Replicas to scale to support thousands of active user connections while still keeping replica lag to a minimum.

**Note**

DDL statements that run on the primary instance might interrupt database connections on the associated Aurora Replicas. If an Aurora Replica connection is actively using a database object, such as a table, and that object is modified on the primary instance using a DDL statement, the Aurora Replica connection is interrupted.

**Note**

The China (Ningxia) Region does not support cross-Region read replicas.

### Replication options for Amazon Aurora MySQL

You can set up replication between any of the following options:

- Two Aurora MySQL DB clusters in different AWS Regions, by creating a cross-Region read replica of an Aurora MySQL DB cluster.

  For more information, see [Replicating Amazon Aurora MySQL DB clusters across AWS Regions](p. 733).

- Two Aurora MySQL DB clusters in the same AWS Region, by using MySQL binary log (binlog) replication.

  For more information, see [Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster (binary log replication)](p. 743).

- An Amazon RDS MySQL DB instance as the source and an Aurora MySQL DB cluster, by creating an Aurora read replica of an Amazon RDS MySQL DB instance.

  You can use this approach to bring existing and ongoing data changes into Aurora MySQL during migration to Aurora. For more information, see [Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using a DB snapshot](p. 659).

  You can also use this approach to increase the scalability of read queries for your data. You do so by querying the data using one or more DB instances within a read-only Aurora MySQL cluster. For more information, see [Using Amazon Aurora to scale reads for your MySQL database](p. 755).

- An Aurora MySQL DB cluster in one AWS Region and up to five Aurora read-only Aurora MySQL DB clusters in different Regions, by creating an Aurora global database.

  You can use an Aurora global database to support applications with a world-wide footprint. The primary Aurora MySQL DB cluster has a Writer instance and up to 15 Aurora Replicas. The read-only
secondary Aurora MySQL DB clusters can each be made up of as many as 16 Aurora Replicas. For more information, see Using Amazon Aurora global databases (p. 206).

**Note**
Rebooting the primary instance of an Amazon Aurora DB cluster also automatically reboots the Aurora Replicas for that DB cluster, to re-establish an entry point that guarantees read/write consistency across the DB cluster.

**Performance considerations for Amazon Aurora MySQL replication**

The following features help you to fine-tune the performance of Aurora MySQL replication.

Starting in Aurora MySQL 1.17.4, the replica log compression feature automatically reduces network bandwidth for replication messages. Because each message is transmitted to all Aurora Replicas, the benefits are greater for larger clusters. This feature involves some CPU overhead on the writer node to perform the compression. Thus, the feature is only available on the 8xlarge and 16xlarge instance classes, which have high CPU capacity. It is enabled by default on these instance classes. You can control this feature by turning off the `aurora_enable_replica_log_compression` parameter. For example, you might turn off replica log compression for larger instance classes if your writer node is near its maximum CPU capacity.

Starting in Aurora MySQL 1.17.4, the binlog filtering feature automatically reduces network bandwidth for replication messages. Because the Aurora Replicas don't use the binlog information that is included in the replication messages, that data is omitted from the messages sent to those nodes. You control this feature by changing the `aurora_enable_repl_bin_log_filtering` parameter. This parameter is on by default. Because this optimization is intended to be transparent, you might turn off this setting only during diagnosis or troubleshooting for issues related to replication. For example, you can do so to match the behavior of an older Aurora MySQL cluster where this feature was not available.

**High availability considerations for Amazon Aurora MySQL replication**

Having more Aurora Replicas in your cluster helps to ensure high availability. A database instance with a full copy of your data is always available for you to query, even if some database instances become unavailable.

The tradeoff with having multiple Aurora Replicas is that replicas become unavailable for brief periods when the underlying database instances are restarted. These restarts can happen during maintenance operations, or when a replica begins to lag too far behind the source. Restarting a replica interrupts existing connections to the corresponding database instance. Restarting an Aurora cluster causes all the replicas to become unavailable at the same time.

The following features help to ensure high availability even during these intervals when replicas are restarted.

Starting in Aurora 1.17.4, the zero-downtime restart (ZDR) feature preserves existing connections when an Aurora MySQL Replica is restarted, for example if the replica falls too far behind the source. Any open transaction is rolled back, and your application must retry it. To enable this feature, turn on the `aurora_enable_zdr` parameter in the cluster parameter group. This parameter is off by default.

**Monitoring Amazon Aurora MySQL replication**

Read scaling and high availability depend on minimal lag time. You can monitor how far an Aurora Replica is lagging behind the primary instance of your Aurora MySQL DB cluster by monitoring the
Amazon CloudWatch AuroraReplicaLag metric. The AuroraReplicaLag metric is recorded in each Aurora Replica.

The primary DB instance also records the AuroraReplicaLagMaximum and AuroraReplicaLagMinimum Amazon CloudWatch metrics. The AuroraReplicaLagMaximum metric records the maximum amount of lag between the primary DB instance and each Aurora Replica in the DB cluster. The AuroraReplicaLagMinimum metric records the minimum amount of lag between the primary DB instance and each Aurora Replica in the DB cluster.

If you need the most current value for Aurora Replica lag, you can query the mysql.ro_replica_status table on the primary instance in your Aurora MySQL DB cluster and check the value in the Replica_lag_in_msec column. This column value is provided to Amazon CloudWatch as the value for the AuroraReplicaLag metric. The Aurora Replica lag is also recorded on each Aurora Replica in the INFORMATION_SCHEMA.REPLICA_HOST_STATUS table in your Aurora MySQL DB cluster.

For more information on monitoring RDS instances and CloudWatch metrics, see Monitoring an Amazon Aurora DB cluster (p. 459).

Replicating Amazon Aurora MySQL DB clusters across AWS Regions

You can create an Amazon Aurora MySQL DB cluster as a read replica in a different AWS Region than the source DB cluster. Taking this approach can improve your disaster recovery capabilities, let you scale read operations into an AWS Region that is closer to your users, and make it easier to migrate from one AWS Region to another.

You can create read replicas of both encrypted and unencrypted DB clusters. The read replica must be encrypted if the source DB cluster is encrypted.

For each source DB cluster, you can have up to five cross-Region DB clusters that are read replicas.

Note
As an alternative to cross-Region read replicas, you can scale read operations with minimal lagtime by using an Aurora global database. An Aurora global database has a primary Aurora DB cluster in one AWS Region and up to five secondary read-only DB clusters in different Regions. Each secondary DB cluster can include up to 16 (rather than 15) Aurora Replicas. Replication from the primary DB cluster to all secondaries is handled by the Aurora storage layer rather than by the database engine, so lagtime for replicating changes is minimal—typically, less than 1 second. Keeping the database engine out of the replication process means that the database engine is dedicated to processing workloads. It also means that you don't need to configure or manage Aurora MySQL's binlog (binary logging) replication. To learn more, see Using Amazon Aurora global databases (p. 206).

When you create an Aurora MySQL DB cluster read replica in another AWS Region, you should be aware of the following:

- Both your source DB cluster and your cross-Region read replica DB cluster can have up to 15 Aurora Replicas, along with the primary instance for the DB cluster. By using this functionality, you can scale read operations for both your source AWS Region and your replication target AWS Region.
- In a cross-Region scenario, there is more lag time between the source DB cluster and the read replica due to the longer network channels between AWS Regions.
- Data transferred for cross-Region replication incurs Amazon RDS data transfer charges. The following cross-Region replication actions generate charges for the data transferred out of the source AWS Region:
  - When you create the read replica, Amazon RDS takes a snapshot of the source cluster and transfers the snapshot to the AWS Region that holds the read replica.
• For each data modification made in the source databases, Amazon RDS transfers data from the source region to the AWS Region that holds the read replica.

For more information about Amazon RDS data transfer pricing, see Amazon Aurora pricing.

• You can run multiple concurrent create or delete actions for read replicas that reference the same source DB cluster. However, you must stay within the limit of five read replicas for each source DB cluster.

• For replication to operate effectively, each read replica should have the same amount of compute and storage resources as the source DB cluster. If you scale the source DB cluster, you should also scale the read replicas.

Topics

• Before you begin (p. 734)
• Creating an Amazon Aurora MySQL DB cluster that is a cross-Region read replica (p. 734)
• Viewing Amazon Aurora MySQL cross-Region replicas (p. 741)
• Promoting a read replica to be a DB cluster (p. 741)
• Troubleshooting Amazon Aurora MySQL cross Region replicas (p. 742)

Before you begin

Before you can create an Aurora MySQL DB cluster that is a cross-Region read replica, you must enable binary logging on your source Aurora MySQL DB cluster. Cross-region replication for Aurora MySQL uses MySQL binary replication to replay changes on the cross-Region read replica DB cluster.

To enable binary logging on an Aurora MySQL DB cluster, update the `binlog_format` parameter for your source DB cluster. The `binlog_format` parameter is a cluster-level parameter that is in the default cluster parameter group. If your DB cluster uses the default DB cluster parameter group, create a new DB cluster parameter group to modify `binlog_format` settings. We recommend that you set the `binlog_format` to MIXED. However, you can also set `binlog_format` to ROW or STATEMENT if you need a specific binlog format. Reboot your Aurora DB cluster for the change to take effect.

For more information, see Amazon Aurora DB cluster and DB instance parameters (p. 300) and Working with DB parameter groups and DB cluster parameter groups (p. 298).

Creating an Amazon Aurora MySQL DB cluster that is a cross-Region read replica

You can create an Aurora DB cluster that is a cross-Region read replica by using the AWS Management Console, the AWS Command Line Interface (AWS CLI), or the Amazon RDS API. You can create cross-Region read replicas from both encrypted and unencrypted DB clusters.

When you create a cross-Region read replica for Aurora MySQL by using the AWS Management Console, Amazon RDS creates a DB cluster in the target AWS Region, and then automatically creates a DB instance that is the primary instance for that DB cluster.

When you create a cross-Region read replica using the AWS CLI or RDS API, you first create the DB cluster in the target AWS Region and wait for it to become active. Once it is active, you then create a DB instance that is the primary instance for that DB cluster.

Replication begins when the primary instance of the read replica DB cluster becomes available.

Use the following procedures to create a cross-Region read replica from an Aurora MySQL DB cluster. These procedures work for creating read replicas from either encrypted or unencrypted DB clusters.
To create an Aurora MySQL DB cluster that is a cross-Region read replica with the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the top-right corner of the AWS Management Console, select the AWS Region that hosts your source DB cluster.
3. In the navigation pane, choose Instances.
4. Choose the check box for the DB instance that you want to create a cross-Region read replica for. For Actions, choose Create cross region read replica.
5. On the Create cross region read replica page, choose the option settings for your cross-Region read replica DB cluster, as described in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination region</td>
<td>Choose the AWS Region to host the new cross-Region read replica DB cluster.</td>
</tr>
<tr>
<td>Destination DB subnet group</td>
<td>Choose the DB subnet group to use for the cross-Region read replica DB cluster.</td>
</tr>
<tr>
<td>Publicly accessible</td>
<td>Choose Yes to give the cross-Region read replica DB cluster a public IP address; otherwise, select No.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Select Enable Encryption to enable encryption at rest for this DB cluster. For more information, see Encrypting Amazon Aurora resources (p. 1208).</td>
</tr>
<tr>
<td>Master key</td>
<td>Only available if Encryption is set to Enable Encryption. Select the master key to use for encrypting this DB cluster. For more information, see Encrypting Amazon Aurora resources (p. 1208).</td>
</tr>
<tr>
<td>DB instance class</td>
<td>Choose a DB instance class that defines the processing and memory requirements for the primary instance in the DB cluster. For more information about DB instance class options, see DB instance classes (p. 46).</td>
</tr>
<tr>
<td>Multi-AZ deployment</td>
<td>Choose Yes to create a read replica of the new DB cluster in another Availability Zone in the target AWS Region for failover support. For more information about multiple Availability Zones, see Regions and Availability Zones (p. 5).</td>
</tr>
<tr>
<td>Read replica source</td>
<td>Choose the source DB cluster to create a cross-Region read replica for.</td>
</tr>
<tr>
<td>DB instance identifier</td>
<td>Type a name for the primary instance in your cross-Region read replica DB cluster. This identifier is used in the endpoint address for the primary instance of the new DB cluster. The DB instance identifier has the following constraints:</td>
</tr>
<tr>
<td></td>
<td>• It must contain from 1 to 63 alphanumeric characters or hyphens.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Its first character must be a letter.</td>
</tr>
<tr>
<td></td>
<td>• It cannot end with a hyphen or contain two consecutive hyphens.</td>
</tr>
<tr>
<td></td>
<td>• It must be unique for all DB instances for each AWS account, for each AWS Region.</td>
</tr>
<tr>
<td>DB cluster identifier</td>
<td>Type a name for your cross-Region read replica DB cluster that is unique for your account in the target AWS Region for your replica. This identifier is used in the cluster endpoint address for your DB cluster. For information on the cluster endpoint, see Amazon Aurora connection management (p. 24).</td>
</tr>
<tr>
<td></td>
<td>The DB cluster identifier has the following constraints:</td>
</tr>
<tr>
<td></td>
<td>• It must contain from 1 to 63 alphanumeric characters or hyphens.</td>
</tr>
<tr>
<td></td>
<td>• Its first character must be a letter.</td>
</tr>
<tr>
<td></td>
<td>• It cannot end with a hyphen or contain two consecutive hyphens.</td>
</tr>
<tr>
<td></td>
<td>• It must be unique for all DB clusters for each AWS account, for each AWS Region.</td>
</tr>
<tr>
<td>Priority</td>
<td>Choose a failover priority for the primary instance of the new DB cluster. This priority determines the order in which Aurora Replicas are promoted when recovering from a primary instance failure. If you don't select a value, the default is tier-1. For more information, see Fault tolerance for an Aurora DB cluster (p. 56).</td>
</tr>
<tr>
<td>Database port</td>
<td>Specify the port for applications and utilities to use to access the database. Aurora DB clusters default to the default MySQL port, 3306. Firewalls at some companies block connections to this port. If your company firewall blocks the default port, choose another port for the new DB cluster.</td>
</tr>
<tr>
<td>Enhanced monitoring</td>
<td>Choose Enable enhanced monitoring to enable gathering metrics in real time for the operating system that your DB cluster runs on. For more information, see Enhanced Monitoring (p. 504).</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Monitoring Role</td>
<td>Only available if Enhanced Monitoring is set to Enable enhanced monitoring. Choose the IAM role that you created to permit Amazon RDS to communicate with Amazon CloudWatch Logs for you, or choose Default to have RDS create a role for you named rds-monitoring-role. For more information, see Enhanced Monitoring (p. 504).</td>
</tr>
<tr>
<td>Granularity</td>
<td>Only available if Enhanced Monitoring is set to Enable enhanced monitoring. Set the interval, in seconds, between when metrics are collected for your DB cluster.</td>
</tr>
<tr>
<td>Auto minor version upgrade</td>
<td>This setting doesn't apply to Aurora MySQL DB clusters. For more information about engine updates for Aurora MySQL, see Database engine updates for Amazon Aurora MySQL (p. 874).</td>
</tr>
</tbody>
</table>

6. Choose Create to create your cross-Region read replica for Aurora.

AWS CLI

To create an Aurora MySQL DB cluster that is a cross-Region read replica with the CLI

1. Call the AWS CLI `create-db-cluster` command in the AWS Region where you want to create the read replica DB cluster. Include the `--replication-source-identifier` option and specify the Amazon Resource Name (ARN) of the source DB cluster to create a read replica for.

   For cross-Region replication where the DB cluster identified by `--replication-source-identifier` is encrypted, you must specify the `--kms-key-id` option and the `--storage-encrypted` option. You must also specify either the `--source-region` or `--pre-signed-url` option. Using `--source-region` autogenerates a presigned URL that is a valid request for the `CreateDBCluster` API operation that can be performed in the source AWS Region that contains the encrypted DB cluster to be replicated. Using `--pre-signed-url` requires you to construct a presigned URL manually instead. The AWS KMS key identifier is used to encrypt the read replica. It must be an AWS KMS customer master key (CMK) valid for the destination AWS Region. To learn more about these options, see `create-db-cluster`.

   **Note**
   You can set up cross-Region replication from an unencrypted DB cluster to an encrypted read replica by specifying `--storage-encrypted` and providing a value for `--kms-key-id`. In this case, you don't need to specify `--source-region` or `--pre-signed-url`.

   You can't specify the `--master-username` and `--master-user-password` parameters. Those values are taken from the source DB cluster.

   The following code example creates a read replica in the us-east-1 Region from an unencrypted DB cluster snapshot in the us-west-2 Region. The command is called in the us-east-1 Region.

   For Linux, macOS, or Unix:

   ```bash
   aws rds create-db-cluster \
   --db-cluster-identifier sample-replica-cluster \
   --engine aurora \
   ```
For Windows:

```bash
aws rds create-db-cluster ^
  --db-cluster-identifier sample-replica-cluster ^
  --engine aurora ^
```

The following code example creates a read replica in the us-east-1 Region from an encrypted DB cluster snapshot in the us-west-2 Region. The command is called in the us-east-1 Region.

For Linux, macOS, or Unix:

```bash
aws rds create-db-cluster \
  --db-cluster-identifier sample-replica-cluster \
  --engine aurora \
  --kms-key-id my-us-east-1-key \
  --source-region us-west-2 \
  --storage-encrypted
```

For Windows:

```bash
aws rds create-db-cluster ^
  --db-cluster-identifier sample-replica-cluster ^
  --engine aurora ^
  --kms-key-id my-us-east-1-key ^
  --source-region us-west-2 ^
  --storage-encrypted
```

2. Check that the DB cluster has become available to use by using the AWS CLI `describe-db-clusters` command, as shown in the following example.

```bash
aws rds describe-db-clusters --db-cluster-identifier sample-replica-cluster
```

When the `describe-db-clusters` results show a status of available, create the primary instance for the DB cluster so that replication can begin. To do so, use the AWS CLI `create-db-instance` command as shown in the following example.

For Linux, macOS, or Unix:

```bash
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
```

For Windows:

```bash
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
```
When the DB instance is created and available, replication begins. You can determine if the DB instance is available by calling the AWS CLI `describe-db-instances` command.

**RDS API**

**To create an Aurora MySQL DB cluster that is a cross-Region read replica with the API**

1. Call the RDS API `CreateDBCluster` action in the AWS Region where you want to create the read replica DB cluster. Include the `ReplicationSourceIdentifier` parameter and specify the Amazon Resource Name (ARN) of the source DB cluster to create a read replica for.

For cross-Region replication where the DB cluster identified by `ReplicationSourceIdentifier` is encrypted, you must specify the `KmsKeyId` parameter and set the `StorageEncrypted` parameter to `true`. You must also specify the `PreSignedUrl` parameter. The presigned URL must be a valid request for the `CreateDBCluster` API operation that can be performed in the source AWS Region that contains the encrypted DB cluster to be replicated. The AWS KMS key identifier is used to encrypt the read replica, and must be a AWS KMS customer master key (CMK) valid for the destination AWS Region. To automatically rather than manually generate a presigned URL, use the AWS CLI `create-db-cluster` command with the `--source-region` option instead.

**Note**

You can set up cross-Region replication from an unencrypted DB cluster to an encrypted read replica by specifying `StorageEncrypted` as `true` and providing a value for `KmsKeyId`. In this case, you don't need to specify `PreSignedUrl`.

You don't need to include the `MasterUsername` and `MasterUserPassword` parameters, because those values are taken from the source DB cluster.

The following code example creates a read replica in the us-east-1 Region from an unencrypted DB cluster snapshot in the us-west-2 Region. The action is called in the us-east-1 Region.

```bash
https://rds.us-east-1.amazonaws.com/?Action=CreateDBCluster
&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=a04c831a0b54b9e4ced36a900dcb9f5f9f47b185eb3b25ebe97a4e95790c8b7
```

The following code example creates a read replica in the us-east-1 Region from an encrypted DB cluster snapshot in the us-west-2 Region. The action is called in the us-east-1 Region.

```bash
https://rds.us-east-1.amazonaws.com/?Action=CreateDBCluster
&KmsKeyId=my-us-east-1-key
&StorageEncrypted=true
&PreSignedUrl=https%253A%252F%252F%252Fconfigured-url
%253FAction%253DCreateDBCluster
%2526DestinationRegion%253Dus-east-1
%2526KmsKeyId%253Dmy-us-east-1-key
%2526ReplicationSourceIdentifier%253Darn%25253Aaws%25253Arrds%25253Aus-west-2%25253A123456789012%25253Acluster%25253A1sample-master-cluster
```

739
2. Check that the DB cluster has become available to use by using the RDS API `DescribeDBClusters` action, as shown in the following example.

```bash
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/20160201/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=84c2e4f8fba7c577ac5d820711e34c6e45fcd35be8a6b7c50f359a7e95790c8b7
```

When the `DescribeDBClusters` results show a status of available, create the primary instance for the DB cluster so that replication can begin. To do so, use the RDS API `CreateDBInstance` action as shown in the following example.

```bash
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/20160201/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=125fe575959f5bbcebd553f2365f907179757a08b5d7a16a378dafa59387f58cdb
```

When the DB instance is created and available, replication begins. You can determine if the DB instance is available by calling the AWS CLI `DescribeDBInstances` command.
Viewing Amazon Aurora MySQL cross-Region replicas

You can view the cross-Region replication relationships for your Amazon Aurora MySQL DB clusters by calling the `describe-db-clusters` AWS CLI command or the `DescribeDBClusters` RDS API operation. In the response, refer to the `ReadReplicaIdentifiers` field for the DB cluster identifiers of any cross-Region read replica DB clusters, and refer to the `ReplicationSourceIdentifier` element for the ARN of the source DB cluster that is the replication source.

Promoting a read replica to be a DB cluster

You can promote an Aurora MySQL read replica to a standalone DB cluster. When you promote an Aurora MySQL read replica, its DB instances are rebooted before they become available.

Typically, you promote an Aurora MySQL read replica to a standalone DB cluster as a data recovery scheme if the source DB cluster fails.

To do this, first create a read replica and then monitor the source DB cluster for failures. In the event of a failure, do the following:

1. Promote the read replica.
2. Direct database traffic to the promoted DB cluster.
3. Create a replacement read replica with the promoted DB cluster as its source.

When you promote a read replica, the read replica becomes a standalone Aurora DB cluster. The promotion process can take several minutes or longer to complete, depending on the size of the read replica. After you promote the read replica to a new DB cluster, it's just like any other DB cluster. For example, you can create read replicas from it and perform point-in-time restore operations. You can also create Aurora Replicas for the DB cluster.

Because the promoted DB cluster is no longer a read replica, you can't use it as a replication target.

The following steps show the general process for promoting a read replica to a DB cluster:

1. Stop any transactions from being written to the read replica source DB cluster, and then wait for all updates to be made to the read replica. Database updates occur on the read replica after they have occurred on the source DB cluster, and this replication lag can vary significantly. Use the `ReplicaLag` metric to determine when all updates have been made to the read replica. The `ReplicaLag` metric records the amount of time a read replica DB instance lags behind the source DB instance. When the `ReplicaLag` metric reaches 0, the read replica has caught up to the source DB instance.

2. Promote the read replica by using the `Promote` option on the Amazon RDS console, the AWS CLI command `promote-read-replica-db-cluster`, or the `PromoteReadReplicaDBCluster` Amazon RDS API operation.

   You choose an Aurora MySQL DB instance to promote the read replica. After the read replica is promoted, the Aurora MySQL DB cluster is promoted to a standalone DB cluster. The DB instance with the highest failover priority is promoted to the primary DB instance for the DB cluster. The other DB instances become Aurora Replicas.

   **Note**
   The promotion process takes a few minutes to complete. When you promote a read replica, replication is stopped and the DB instances are rebooted. When the reboot is complete, the read replica is available as a new DB cluster.
To promote an Aurora MySQL read replica to a DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. On the console, choose Instances.
   The Instance pane appears.
3. In the Instances pane, choose the read replica that you want to promote.
   The read replicas appear as Aurora MySQL DB instances.
4. For Actions, choose Promote read replica.
5. On the acknowledgment page, choose Promote read replica.

AWS CLI

To promote a read replica to a DB cluster, use the AWS CLI `promote-read-replica-db-cluster` command.

Example

For Linux, macOS, or Unix:

```bash
aws rds promote-read-replica-db-cluster \
--db-cluster-identifier mydbcluster
```

For Windows:

```bash
aws rds promote-read-replica-db-cluster ^
--db-cluster-identifier mydbcluster
```

RDS API

To promote a read replica to a DB cluster, call `PromoteReadReplicaDBCluster`.

Troubleshooting Amazon Aurora MySQL cross Region replicas

Following you can find a list of common error messages that you might encounter when creating an Amazon Aurora cross-Region read replica, and how to resolve the specified errors.

Source cluster [DB cluster ARN] doesn’t have binlogs enabled

To resolve this issue, enable binary logging on the source DB cluster. For more information, see Before you begin (p. 734).

Source cluster [DB cluster ARN] doesn’t have cluster parameter group in sync on writer

You receive this error if you have updated the `binlog_format` DB cluster parameter, but have not rebooted the primary instance for the DB cluster. Reboot the primary instance (that is, the writer) for the DB cluster and try again.

Source cluster [DB cluster ARN] already has a read replica in this region

You can have up to five cross-Region DB clusters that are read replicas for each source DB cluster in any AWS Region. If you already have the maximum number of read replicas for a DB cluster in a particular
AWS Region, you must delete an existing one before you can create a new cross-Region DB cluster in that Region.

**DB cluster [DB cluster ARN] requires a database engine upgrade for cross-Region replication support**

To resolve this issue, upgrade the database engine version for all of the instances in the source DB cluster to the most recent database engine version, and then try creating a cross-Region read replica DB again.

## Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster (binary log replication)

Because Amazon Aurora MySQL is compatible with MySQL, you can set up replication between a MySQL database and an Amazon Aurora MySQL DB cluster. This type of replication uses the MySQL binary log replication, also referred to as **binlog replication**. If you use binary log replication with Aurora, we recommend that your MySQL database run MySQL version 5.5 or later. You can set up replication where your Aurora MySQL DB cluster is the replication source or the replica. You can replicate with an Amazon RDS MySQL DB instance, a MySQL database external to Amazon RDS, or another Aurora MySQL DB cluster.

You can also replicate with an Amazon RDS MySQL DB instance or Aurora MySQL DB cluster in another AWS Region. When you're performing replication across AWS Regions, ensure that your DB clusters and DB instances are publicly accessible. Aurora MySQL DB clusters must be part of a public subnet in your VPC.

If you want to configure replication between an Aurora MySQL DB cluster and an Aurora MySQL DB cluster in another region, you can create an Aurora MySQL DB cluster as a read replica in a different AWS Region than the source DB cluster. For more information, see Replicating Amazon Aurora MySQL DB clusters across AWS Regions (p. 733).

With Aurora MySQL 2.04 and higher, you can replicate between Aurora MySQL and an external source or target that uses global transaction identifiers (GTIDs) for replication. Ensure that the GTID-related parameters in the Aurora MySQL DB cluster have settings that are compatible with the GTID status of the external database. To learn how to do this, see Using GTID-based replication for Aurora MySQL (p. 762).

**Warning**

When you replicate between Aurora MySQL and MySQL, ensure that you use only InnoDB tables. If you have MyISAM tables that you want to replicate, you can convert them to InnoDB before setting up replication with the following command:

```sql
alter table <schema>.<table_name> engine=innodb, algorithm=copy;
```

Setting up MySQL replication with Aurora MySQL involves the following steps, which are discussed in detail following in this topic:

1. Enable binary logging on the replication source (p. 744)
2. Retain binary logs on the replication source until no longer needed (p. 747)
3. Create a snapshot of your replication source (p. 748)
4. Load the snapshot into your replica target (p. 750)
5. Enable replication on your replica target (p. 752)
6. Monitor your replica (p. 753)
Setting up replication with MySQL or another Aurora DB cluster

To set up Aurora replication with MySQL, take the following steps.

1. Enable binary logging on the replication source

Find instructions on how to enable binary logging on the replication source for your database engine following.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aurora</strong></td>
<td><strong>To enable binary logging on an Aurora MySQL DB cluster</strong></td>
</tr>
<tr>
<td></td>
<td>Set the <code>binlog_format</code> parameter to <code>ROW</code>, <code>STATEMENT</code>, or <code>MIXED</code>. <code>MIXED</code> is recommended unless you have a need for a specific binlog format. The <code>binlog_format</code> parameter is a cluster-level parameter that is in the default cluster parameter group. If you are changing the <code>log_bin</code> parameter from <code>OFF</code> to another value, then you need to reboot your Aurora DB cluster for the change to take effect.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Amazon Aurora DB cluster and DB instance parameters (p. 300) and Working with DB parameter groups and DB cluster parameter groups (p. 298).</td>
</tr>
<tr>
<td><strong>RDS MySQL</strong></td>
<td><strong>To enable binary logging on an Amazon RDS DB instance</strong></td>
</tr>
<tr>
<td></td>
<td>You cannot enable binary logging directly for an Amazon RDS DB instance, but you can enable it by doing one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enable automated backups for the DB instance. You can enable automated backups when you create a DB instance, or you can enable backups by modifying an existing DB instance. For more information, see Creating a DB instance in the Amazon RDS User Guide.</td>
</tr>
<tr>
<td></td>
<td>• Create a read replica for the DB instance. For more information, see Working with read replicas in the Amazon RDS User Guide.</td>
</tr>
<tr>
<td><strong>MySQL (external)</strong></td>
<td><strong>To set up encrypted replication</strong></td>
</tr>
<tr>
<td></td>
<td>To replicate data securely with Aurora MySQL version 5.6, you can use encrypted replication.</td>
</tr>
<tr>
<td></td>
<td>Currently, encrypted replication with an external MySQL database is only supported for Aurora MySQL version 5.6.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If you don’t need to use encrypted replication, you can skip these steps.</td>
</tr>
<tr>
<td></td>
<td>The following are prerequisites for using encrypted replication:</td>
</tr>
<tr>
<td></td>
<td>• Secure Sockets Layer (SSL) must be enabled on the external MySQL source database.</td>
</tr>
<tr>
<td></td>
<td>• A client key and client certificate must be prepared for the Aurora MySQL DB cluster.</td>
</tr>
<tr>
<td></td>
<td>During encrypted replication, the Aurora MySQL DB cluster acts a client to the MySQL database server. The certificates and keys for the Aurora MySQL client are in files in .pem format.</td>
</tr>
<tr>
<td></td>
<td>1. Ensure that you are prepared for encrypted replication:</td>
</tr>
<tr>
<td>Database engine</td>
<td>Instructions</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>• If you don’t have SSL enabled on the external MySQL source database and don’t have a client key and client certificate prepared, enable SSL on the MySQL database server and generate the required client key and client certificate.</td>
</tr>
<tr>
<td></td>
<td>• If SSL is enabled on the external source, supply a client key and certificate for the Aurora MySQL DB cluster. If you don’t have these, generate a new key and certificate for the Aurora MySQL DB cluster. To sign the client certificate, you must have the certificate authority key that you used to configure SSL on the external MySQL source database.</td>
</tr>
</tbody>
</table>

For more information, see Creating SSL certificates and keys using openssl in the MySQL documentation.

You need the certificate authority certificate, the client key, and the client certificate.

2. Connect to the Aurora MySQL DB cluster as the master user using SSL.

For information about connecting to an Aurora MySQL DB cluster with SSL, see Using SSL/TLS with Aurora MySQL DB clusters (p. 638).

3. Run the `mysql.rds_import_binlog_ssl_material` stored procedure to import the SSL information into the Aurora MySQL DB cluster.

For the `ssl_material_value` parameter, insert the information from the .pem format files for the Aurora MySQL DB cluster in the correct JSON payload.

The following example imports SSL information into an Aurora MySQL DB cluster. In .pem format files, the body code typically is longer than the body code shown in the example.

call mysql.rds_import_binlog_ssl_material(
    '{"ssl_ca": "-----BEGIN CERTIFICATE-----AAAAAB3NzaC1yc2EAAAADQABAAAABAQGClksfkNkuSevGj3eYhc53pcjQ3maAbDcBvBS706Vh2zItc1h+PnDSUaw+WYNqnmzphTk/a/gU8jEzoOWbdM4yxyb/w896xbFVeSFJUOp/d6RjHJOI0IBXr
lsLnBlntcRl7FbtxJMXLvwvJryDUlBMTjYtwB+QhYXUMOzce5Pjz5/188e7tjnV3iAoG/cQK+OFZQ
qeeJAAHco+CY/5WrUBkrMfJr6HCXkVjdWPkYQ3xqCo+FmUZofz221CBt5IMucxFPkJx4rMi+7w7B3Rb
BQOQ6v7yeb70IlPnW0yNqFUOXA246RA8QFYiCNYwi3f0s6KLxEXmYpl

END CERTIFICATE-----
"ssl_cert": "-----BEGIN CERTIFICATE-----AAAAAB3NzaC1yc2EAAAADQABAAAABAQGClksfkNkuSevGj3eYhc53pcjQ3maAbDcBvBS706Vh2zItc1h+PnDSUaw+WYNqnmzphTk/a/gU8jEzoOWbdM4yxyb/w896xbFVeSFJUOp/d6RjHJOI0IBXr
lsLnBlntcRl7FbtxJMXLvwvJryDUlBMTjYtwB+QhYXUMOzce5Pjz5/188e7tjnV3iAoG/cQK+OFZQ
qeeJAAHco+CY/5WrUBkrMfJr6HCXkVjdWPkYQ3xqCo+FmUZofz221CBt5IMucxFPkJx4rMi+7w7B3Rb
BQOQ6v7yeb70IlPnW0yNqFUOXA246RA8QFYiCNYwi3f0s6KLxEXmYpl

END CERTIFICATE-----
"ssl_key": "-----BEGIN RSA PRIVATE KEY-----AAAAAB3NzaC1yc2EAAAADQABAAAABAQGClksfkNkuSevGj3eYhc53pcjQ3maAbDcBvBS706Vh2zItc1h+PnDSUaw+WYNqnmzphTk/a/gU8jEzoOWbdM4yxyb/w896xbFVeSFJUOp/d6RjHJOI0IBXr
lsLnBlntcRl7FbtxJMXLvwvJryDUlBMTjYtwB+QhYXUMOzce5Pjz5/188e7tjnV3iAoG/cQK+OFZQ
qeeJAAHco+CY/5WrUBkrMfJr6HCXkVjdWPkYQ3xqCo+FmUZofz221CBt5IMucxFPkJx4rMi+7w7B3Rb
BQOQ6v7yeb70IlPnW0yNqFUOXA246RA8QFYiCNYwi3f0s6KLxEXmYpl

END RSA PRIVATE KEY-----
## Amazon Aurora User Guide for Aurora

### Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster (binary log replication)

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instructions</th>
</tr>
</thead>
</table>
|                 | -----END RSA PRIVATE KEY-----\n
For more information, see `mysql_rds_import_binlog_ssl_material` and Using SSL/TLS with Aurora MySQL DB clusters (p. 638).

**Note**
After running the procedure, the secrets are stored in files. To erase the files later, you can run the `mysql_rds_remove_binlog_ssl_material` stored procedure.

### To enable binary logging on an external MySQL database

1. From a command shell, stop the `mysql` service.
   
   ```sh
   sudo service mysqld stop
   ```

2. Edit the `my.cnf` file (this file is usually under `/etc`).
   
   ```sh
   sudo vi /etc/my.cnf
   ```

   Add the `log_bin` and `server_id` options to the `[mysqld]` section. The `log_bin` option provides a file name identifier for binary log files. The `server_id` option provides a unique identifier for the server in source-replica relationships.

   If encrypted replication isn't required, ensure that the external MySQL database is started with binlogs enabled and SSL disabled.

   The following are the relevant entries in the `/etc/my.cnf` file for unencrypted data.

   ```ini
   log-bin=mysql-bin
   server-id=2133421
   innodb_flush_log_at_trx_commit=1
   sync_binlog=1
   ```

   If encrypted replication is required, ensure that the external MySQL database is started with SSL and binlogs enabled.

   The entries in the `/etc/my.cnf` file include the `.pem` file locations for the MySQL database server.

   ```ini
   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
   ```

   Additionally, the `sql_mode` option for your MySQL DB instance must be set to 0, or must not be included in your `my.cnf` file.
2. Retain binary logs on the replication source until no longer needed

When you use MySQL binary log replication, Amazon RDS doesn't manage the replication process. As a result, you need to ensure that the binlog files on your replication source are retained until after the changes have been applied to the replica. This maintenance helps ensure that you can restore your source database in the event of a failure.

Find instructions on how to retain binary logs for your database engine following.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora</td>
<td><strong>To retain binary logs on an Aurora MySQL DB cluster</strong></td>
</tr>
</tbody>
</table>

You do not have access to the binlog files for an Aurora MySQL DB cluster. As a result, you must choose a time frame to retain the binlog files on your replication source long enough to ensure that the changes have been applied to your replica before the binlog file is deleted by Amazon RDS. You can retain binlog files on an Aurora MySQL DB cluster for up to 90 days.

If you are setting up replication with a MySQL database or RDS MySQL DB instance as the replica, and the database that you are creating a replica for is very large, choose a large time frame to retain binlog files until the initial copy of the database to the replica is complete and the replica lag has reached 0.

To set the binary log retention time frame, use the `mysql_rds_set_configuration` procedure and specify a configuration parameter of 'binlog retention hours'.
### Database engine | Instructions
--- | ---
Aurora | along with the number of hours to retain binlog files on the DB cluster, up to 2160 (90 days). The following example that sets the retention period for binlog files to 6 days:

```sql
CALL mysql.rds_set_configuration('binlog retention hours', 144);
```

After replication has been started, you can verify that changes have been applied to your replica by running the `SHOW SLAVE STATUS` command on your replica and checking the `Seconds behind master` field. If the `Seconds behind master` field is 0, then there is no replica lag. When there is no replica lag, reduce the length of time that binlog files are retained by setting the `binlog retention hours` configuration parameter to a smaller time frame.

If you specify a value for `'binlog retention hours'` that is higher than 2160, then 2160 is used.

**RDS MySQL**

**To retain binary logs on an Amazon RDS DB instance**

You can retain binary log files on an Amazon RDS DB instance by setting the binlog retention hours just as with an Aurora MySQL DB cluster, described in the previous section.

You can also retain binlog files on an Amazon RDS DB instance by creating a read replica for the DB instance. This read replica is temporary and solely for the purpose of retaining binlog files. After the read replica has been created, call the `mysql.rds_stop_replication` procedure on the read replica (the `mysql.rds_stop_replication` procedure is only available for MySQL versions 5.5, 5.6 and later, and 5.7 and later). While replication is stopped, Amazon RDS doesn't delete any of the binlog files on the replication source. After you have set up replication with your permanent replica, you can delete the read replica when the replica lag (`Seconds behind master` field) between your replication source and your permanent replica reaches 0.

**MySQL (external)**

**To retain binary logs on an external MySQL database**

Because binlog files on an external MySQL database are not managed by Amazon RDS, they are retained until you delete them.

After replication has been started, you can verify that changes have been applied to your replica by running the `SHOW SLAVE STATUS` command on your replica and checking the `Seconds behind master` field. If the `Seconds behind master` field is 0, then there is no replica lag. When there is no replica lag, you can delete old binlog files.

---

### 3. Create a snapshot of your replication source

You use a snapshot of your replication source to load a baseline copy of your data onto your replica and then start replicating from that point on.

Find instructions on how to create a snapshot of your replication source for your database engine following.

### Database engine | Instructions
--- | ---
Aurora | **To create a snapshot of an Aurora MySQL DB cluster**
1. Create a DB cluster snapshot of your Amazon Aurora DB cluster. For more information, see [Creating a DB cluster snapshot](p. 418).

2. Create a new Aurora DB cluster by restoring from the DB cluster snapshot that you just created. Be sure to retain the same DB parameter group for your restored DB cluster as your original DB cluster. Doing this ensures that the copy of your DB cluster has binary logging enabled. For more information, see [Restoring from a DB cluster snapshot](p. 420).

3. In the console, choose **Databases** and choose the primary instance (writer) for your restored Aurora DB cluster to show its details. Scroll to **Recent Events**. An event message shows that includes the binlog file name and position. The event message is in the following format.

   Binlog position from crash recovery is `binlog-file-name binlog-position`

Save the binlog file name and position values for when you start replication.

You can also get the binlog file name and position by calling the `describe-events` command from the AWS CLI. The following shows an example `describe-events` command with example output.

```
PROMPT> aws rds describe-events

{
   "Events": [
      {
        "EventCategories": [],
        "SourceType": "db-instance",
        "Date": "2016-10-28T19:43:46.862Z",
        "Message": "Binlog position from crash recovery is mysql-bin-changelog.000003 4278",
        "SourceIdentifier": "sample-restored-instance"
      }
   ]
}
```

You can also get the binlog file name and position by checking the MySQL error log for the last MySQL binlog file position or for the `DB_CRASH_RECOVERY_BINLOG_POSITION` entry.

4. If your replica target is an Aurora DB cluster owned by another AWS account, an external MySQL database, or an RDS MySQL DB instance, then you can't load the data from an Amazon Aurora DB cluster snapshot. Instead, create a dump of your Amazon Aurora DB cluster by connecting to your DB cluster using a MySQL client and issuing the `mysqldump` command. Be sure to run the `mysqldump` command against the copy of your Amazon Aurora DB cluster that you created. The following is an example.

```
PROMPT> mysqldump --databases <database_name> --single-transaction --order-by-primary -r backup.sql -u <local_user> -p
```

5. When you have finished creating the dump of your data from the newly created Aurora DB cluster, delete that DB cluster as it is no longer needed.
To create a snapshot of an Amazon RDS DB instance

1. Create a read replica of your Amazon RDS DB instance. For more information, see Creating a read replica in the Amazon Relational Database Service User Guide.
2. Connect to your read replica and stop replication by running the mysql_rds_stop_replication procedure.
3. While the read replica is Stopped, connect to the read replica and run the SHOW SLAVE STATUS command. Retrieve the current binary log file name from the Relay_Master_Log_File field and the log file position from the Exec_Master_Log_Pos field. Save these values for when you start replication.
4. While the read replica remains Stopped, create a DB snapshot of the read replica. For more information, see Creating a DB snapshot in the Amazon Relational Database Service User Guide.
5. Delete the read replica.

To create a snapshot of an external MySQL database

1. Before you create a snapshot, you need to ensure that the binlog location for the snapshot is current with the data in your source instance. To do this, you must first stop any write operations to the instance with the following command:

```
mysql> FLUSH TABLES WITH READ LOCK;
```

2. Create a dump of your MySQL database using the mysqldump command as shown following:

```
PROMPT> sudo mysqldump --databases <database_name> --master-data=2 --single-transaction --order-by-primary -r backup.sql -u <local_user> -p
```

3. After you have created the snapshot, unlock the tables in your MySQL database with the following command:

```
mysql> UNLOCK TABLES;
```

4. Load the snapshot into your replica target

If you plan to load data from a dump of a MySQL database that is external to Amazon RDS, then you might want to create an EC2 instance to copy the dump files to, and then load the data into your DB cluster or DB instance from that EC2 instance. Using this approach, you can compress the dump file(s) before copying them to the EC2 instance in order to reduce the network costs associated with copying data to Amazon RDS. You can also encrypt the dump file or files to secure the data as it is being transferred across the network.

Find instructions on how to load the snapshot of your replication source into your replica target for your database engine following.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora</td>
<td>To load a snapshot into an Aurora MySQL DB cluster</td>
</tr>
<tr>
<td>Database engine</td>
<td>Instructions</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>RDS MySQL</td>
<td><strong>To load a snapshot into an Amazon RDS DB instance</strong>&lt;br&gt;1. Copy the output of the <code>mysqldump</code> command from your replication source to a location that can also connect to your MySQL DB instance.&lt;br&gt;2. Connect to your MySQL DB instance using the <code>mysql</code> command. The following is an example.&lt;br&gt;PROMPT&gt; mysql -h &lt;host_name&gt; -port=3306 -u &lt;db_master_user&gt; -p&lt;br&gt;3. At the <code>mysql</code> prompt, run the <code>source</code> command and pass it the name of your database dump file to load the data into the MySQL DB instance, for example:&lt;br&gt;<code>mysql&gt; source backup.sql;</code></td>
</tr>
<tr>
<td>MySQL (external)</td>
<td><strong>To load a snapshot into an external MySQL database</strong>&lt;br&gt;You cannot load a DB snapshot or a DB cluster snapshot into an external MySQL database. Instead, you must use the output from the <code>mysqldump</code> command.&lt;br&gt;1. Copy the output of the <code>mysqldump</code> command from your replication source to a location that can also connect to your MySQL database.&lt;br&gt;2. Connect to your MySQL database using the <code>mysql</code> command. The following is an example.&lt;br&gt;PROMPT&gt; mysql -h &lt;host_name&gt; -port=3306 -u &lt;db_master_user&gt; -p&lt;br&gt;3. At the <code>mysql</code> prompt, run the <code>source</code> command and pass it the name of your database dump file to load the data into your MySQL database. The following is an example.&lt;br&gt;<code>mysql&gt; source backup.sql;</code></td>
</tr>
</tbody>
</table>
5. Enable replication on your replica target

Before you enable replication, we recommend that you take a manual snapshot of the Aurora MySQL DB cluster or RDS MySQL DB instance replica target. If a problem arises and you need to re-establish replication with the DB cluster or DB instance replica target, you can restore the DB cluster or DB instance from this snapshot instead of having to import the data into your replica target again.

Also, create a user ID that is used solely for replication. The following is an example.

```sql
mysql> CREATE USER 'repl_user'@'<domain_name>' IDENTIFIED BY '<password>';
```

The user requires the REPLICATION CLIENT and REPLICATION SLAVE privileges. Grant these privileges to the user.

```sql
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'<domain_name>';
```

If you need to use encrypted replication, require SSL connections for the replication user. For example, you can use one of the following statement to require SSL connections on the user account repl_user.

```sql
GRANT USAGE ON *.* TO 'repl_user'@'<domain_name>' REQUIRE SSL;
```

**Note**

If REQUIRE SSL isn't included, the replication connection might silently fall back to an unencrypted connection.

Find instructions on how to enable replication for your database engine following.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora</td>
<td><strong>To enable replication from an Aurora MySQL DB cluster</strong></td>
</tr>
<tr>
<td></td>
<td>1. If your DB cluster replica target was created from a DB cluster snapshot, then connect to the DB cluster replica target and issue the <code>SHOW MASTER STATUS</code> command. Retrieve the current binary log file name from the <code>File</code> field and the log file position from the <code>Position</code> field.</td>
</tr>
<tr>
<td></td>
<td>If your DB cluster replica target was created from a DB snapshot, then you need the binlog file and binlog position that are the starting place for replication. You retrieved these values from the <code>SHOW SLAVE STATUS</code> command when you created the snapshot of your replication source.</td>
</tr>
<tr>
<td></td>
<td>2. Connect to the DB cluster and issue the <code>mysql_rds_set_external_master</code> and <code>mysql_rds_start_replication</code> procedures to start replication with your replication source using the binary log file name and location from the previous step. The following is an example.</td>
</tr>
</tbody>
</table>
|                 | ```sql
|                 | CALL mysql.rds_set_external_master ('mydbinstance.123456789012.us-east-1.rds.amazonaws.com', 3306, 'repl_user', '<password>', 'mysql-bin-changelog.000031', 107, 0);
|                 | CALL mysql.rds_start_replication;
|                 | ``` |
| RDS MySQL       | **To enable replication from an Amazon RDS DB instance** |
|                 | 1. If your DB instance replica target was created from a DB snapshot, then you need the binlog file and binlog position that are the starting place for replication. You retrieved
### Database engine | Instructions
---|---
**MySQL (external)**<br>1. Retrieve the binlog file and binlog position that are the starting place for replication. You retrieved these values from the `SHOW SLAVE STATUS` command when you created the snapshot of your replication source. If your external MySQL replica target was populated from the output of the `mysqldump` command with the `--master-data=2` option, then the binlog file and binlog position are included in the output. The following is an example.

```sql
-- 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. Connect to the external MySQL replica target, and issue `CHANGE MASTER TO` and `START SLAVE` to start replication with your replication source using the binary log file name and location from the previous step, for example:

```sql
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;
START SLAVE;
```

### To enable replication from an external MySQL database
1. Connect to the DB instance and issue the `mysql_rds_set_external_master` and `mysql_rds_start_replication` procedures to start replication with your replication source using the binary log file name and location from the previous step. The following is an example.

```sql
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;
```

### 6. Monitor your replica

When you set up MySQL replication with an Aurora MySQL DB cluster, you must monitor failover events for the Aurora MySQL DB cluster when it is the replica target. If a failover occurs, then the DB cluster that is your replica target might be recreated on a new host with a different network address. For information on how to monitor failover events, see Using Amazon RDS event notification (p. 594).

You can also monitor how far the replica target is behind the replication source by connecting to the replica target and running the `SHOW SLAVE STATUS` command. In the command output, the `Seconds Behind Master` field tells you how far the replica target is behind the source.
Stopping replication between Aurora and MySQL or between Aurora and another Aurora DB cluster

To stop binary log replication with a MySQL DB instance, external MySQL database, or another Aurora DB cluster, follow these steps, discussed in detail following in this topic.

1. Stop binary log replication on the replica target (p. 754)

2. Disable binary logging on the replication source (p. 754)

1. Stop binary log replication on the replica target

Find instructions on how to stop binary log replication for your database engine following.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora</td>
<td>To stop binary log replication on an Aurora MySQL DB cluster replica target</td>
</tr>
<tr>
<td></td>
<td>Connect to the Aurora DB cluster that is the replica target, and call the mysql_rds_stop_replication procedure. The mysql.rds_stop_replication procedure is only available for MySQL versions 5.5 and later, 5.6 and later, and 5.7 and later.</td>
</tr>
<tr>
<td>RDS MySQL</td>
<td>To stop binary log replication on an Amazon RDS DB instance</td>
</tr>
<tr>
<td></td>
<td>Connect to the RDS DB instance that is the replica target and call the mysql_rds_stop_replication procedure. The mysql.rds_stop_replication procedure is only available for MySQL versions 5.5 and later, 5.6 and later, and 5.7 and later.</td>
</tr>
<tr>
<td>MySQL (external)</td>
<td>To stop binary log replication on an external MySQL database</td>
</tr>
<tr>
<td></td>
<td>Connect to the MySQL database and call the STOP REPLICATION command.</td>
</tr>
</tbody>
</table>

2. Disable binary logging on the replication source

Find instructions on how to disable binary logging on the replication source for your database engine following.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora</td>
<td>To disable binary logging on an Amazon Aurora DB cluster</td>
</tr>
<tr>
<td></td>
<td>1. Connect to the Aurora DB cluster that is the replication source, and set the binary log retention time frame to 0. To set the binary log retention time frame, use the mysql_rds_set_configuration procedure and specify a configuration parameter of 'binlog retention hours' along with the number of hours to retain binlog files on the DB cluster, in this case 0, as shown in the following example.</td>
</tr>
<tr>
<td></td>
<td>CALL mysql.rds_set_configuration('binlog retention hours', 0);</td>
</tr>
<tr>
<td></td>
<td>2. Set the binlog_format parameter to OFF on the replication source. The binlog_format parameter is a cluster-level parameter that is in the default cluster parameter group.</td>
</tr>
</tbody>
</table>
### Amazon Aurora User Guide for Aurora

**Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster (binary log replication)**

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you have changed the <code>binlog_format</code> parameter value, reboot your DB cluster for the change to take effect.</td>
<td></td>
</tr>
<tr>
<td>For more information, see Amazon Aurora DB cluster and DB instance parameters (p. 300) and Modifying parameters in a DB parameter group (p. 303).</td>
<td></td>
</tr>
</tbody>
</table>

**RDS MySQL**

**To disable binary logging on an Amazon RDS DB instance**

You cannot disable binary logging directly for an Amazon RDS DB instance, but you can disable it by doing the following:

1. Disable automated backups for the DB instance. You can disable automated backups by modifying an existing DB instance and setting the **Backup Retention Period** to 0. For more information, see Modifying an Amazon RDS DB instance and Working with backups in the Amazon Relational Database Service User Guide.

2. Delete all read replicas for the DB instance. For more information, see Working with read replicas of MariaDB, MySQL, and PostgreSQL DB instances in the Amazon Relational Database Service User Guide.

**MySQL (external)**

**To disable binary logging on an external MySQL database**

Connect to the MySQL database and call the `STOP REPLICATION` command.

1. From a command shell, stop the `mysqld` service,

   ```bash
   sudo service mysqld stop
   ```

2. Edit the `my.cnf` file (this file is usually under `/etc`).

   ```bash
   sudo vi /etc/my.cnf
   ```

   Delete the `log_bin` and `server_id` options from the `[mysqld]` section.

   For more information, see Setting the replication master configuration in the MySQL documentation.

3. Start the `mysql` service.

   ```bash
   sudo service mysqld start
   ```

### Using Amazon Aurora to scale reads for your MySQL database

You can use Amazon Aurora with your MySQL DB instance to take advantage of the read scaling capabilities of Amazon Aurora and expand the read workload for your MySQL DB instance. To use Aurora to read scale your MySQL DB instance, create an Amazon Aurora MySQL DB cluster and make it a read replica of your MySQL DB instance. This applies to an Amazon RDS MySQL DB instance, or a MySQL database running external to Amazon RDS.

For information on creating an Amazon Aurora DB cluster, see Creating an Amazon Aurora DB cluster (p. 118).

When you set up replication between your MySQL DB instance and your Amazon Aurora DB cluster, be sure to follow these guidelines:
• Use the Amazon Aurora DB cluster endpoint address when you reference your Amazon Aurora MySQL DB cluster. If a failover occurs, then the Aurora Replica that is promoted to the primary instance for the Aurora MySQL DB cluster continues to use the DB cluster endpoint address.

• Maintain the binlogs on your writer instance until you have verified that they have been applied to the Aurora Replica. This maintenance ensures that you can restore your writer instance in the event of a failure.

**Important**
When using self-managed replication, you’re responsible for monitoring and resolving any replication issues that may occur. For more information, see Diagnosing and resolving lag between read replicas (p. 1310).

**Note**
The permissions required to start replication on an Amazon Aurora MySQL DB cluster are restricted and not available to your Amazon RDS master user. Because of this, you must use the Amazon RDS mysql_rds_set_external_master and mysql_rds_start_replication procedures to set up replication between your Amazon Aurora MySQL DB cluster and your MySQL DB instance.

### Start replication between an external source instance and a MySQL DB instance on Amazon RDS

1. Make the source MySQL DB instance read-only:

```sql
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

2. Run the `SHOW MASTER STATUS` command on the source MySQL DB instance to determine the binlog location. You receive output similar to the following example:

<table>
<thead>
<tr>
<th>File</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>mysql-bin-changelog.000031</td>
<td>107</td>
</tr>
</tbody>
</table>

3. Copy the database from the external MySQL DB instance to the Amazon Aurora MySQL DB cluster using `mysqldump`. For very large databases, you might want to use the procedure in Importing data to an Amazon RDS MySQL or MariaDB DB instance with reduced downtime in the Amazon Relational Database Service User Guide.

   **For Linux, macOS, or Unix:**

   ```
   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>
   ```

   **For Windows:**

   ```
   mysqldump ^
   --databases <database_name> ^
   --single-transaction ^
   ```
Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster (binary log replication)

```bash
--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**
Make sure that there is not a space between the `-p` option and the entered password.

Use the `--host`, `--user` (`-u`), `--port` and `-p` options in the `mysql` command to specify the hostname, user name, port, and password to connect to your Aurora DB cluster. The host name is the DNS name from the Amazon Aurora DB cluster endpoint, for example, `mydbcluster.cluster-123456789012.us-east-1.rds.amazonaws.com`. You can find the endpoint value in the cluster details in the Amazon RDS Management Console.

4. Make the source MySQL DB instance writeable again:

```sql
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

For more information on making backups for use with replication, see Backing up a master or slave by making it read only in the MySQL documentation.

5. In the Amazon RDS Management Console, add the IP address of the server that hosts the source MySQL database to the VPC security group for the Amazon Aurora DB cluster. For more information on modifying a VPC security group, see Security groups for your VPC in the Amazon Virtual Private Cloud User Guide.

You might also need to configure your local network to permit connections from the IP address of your Amazon Aurora DB cluster, so that it can communicate with your source MySQL instance. To find the IP address of the Amazon Aurora DB cluster, use the `host` command:

```
host <aurora_endpoint_address>
```

The host name is the DNS name from the Amazon Aurora DB cluster endpoint.

6. Using the client of your choice, connect to the external MySQL instance and create a MySQL user to be used for replication. This account is used solely for replication and must be restricted to your domain to improve security. The following is an example.

```sql
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY '<password>';  
```

7. For the external MySQL instance, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. For example, to grant the REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the `'repl_user'` user for your domain, issue the following command.

```sql
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
IDENTIFIED BY '<password>';  
```

8. Take a manual snapshot of the Aurora MySQL DB cluster to be the read replica before setting up replication. If you need to reestablish replication with the DB cluster as a read replica, you can restore the Aurora MySQL DB cluster from this snapshot instead of having to import the data from your MySQL DB instance into a new Aurora MySQL DB cluster.

9. Make the Amazon Aurora DB cluster the replica. Connect to the Amazon Aurora DB cluster as the master user and identify the source MySQL database as the replication master by using the
mysql_rds_set_external_master procedure. Use the master log file name and master log position that you determined in Step 2. The following is an example.

```sql
CALL mysql.rds_set_external_master ('mymasterserver.mydomain.com', 3306, 'repl_user', '<password>', 'mysql-bin-changelog.000031', 107, 0);
```

10. On the Amazon Aurora DB cluster, issue the mysql_rds_start_replication procedure to start replication.

```sql
CALL mysql.rds_start_replication;
```

After you have established replication between your source MySQL DB instance and your Amazon Aurora DB cluster, you can add Aurora Replicas to your Amazon Aurora DB cluster. You can then connect to the Aurora Replicas to read scale your data. For information on creating an Aurora Replica, see Adding Aurora replicas to a DB cluster (p. 345).

### Optimizing binary log replication

Following, you can learn how to optimize binary log replication performance and troubleshoot related issues in Aurora MySQL.

**Tip**

This discussion presumes that you are familiar with the MySQL binary log replication mechanism and how it works. For background information, see Replication Implementation in the MySQL documentation.

To optimize binary log replication for Aurora MySQL, you adjust the following cluster-level optimization parameters. These parameters help you to specify the right balance between latency on the binlog source instance and replication lag.

- `aurora_binlog_use_large_read_buffer`
- `aurora_binlog_read_buffer_size`
- `aurora_binlog_replication_max_yield_seconds`

**Note**

For MySQL 5.7-compatible clusters, you can use these parameters in Aurora MySQL version 2.04.5 and later.
For MySQL 5.6-compatible clusters, you can use these parameters in Aurora MySQL version 1.17.6 and later.

**Topics**

- Overview of the large read buffer and max-yield optimizations (p. 758)
- Related parameters (p. 759)
- Enabling binary log replication max-yield mechanism (p. 761)
- Turning off the binary log replication max-yield optimization (p. 761)
- Turning off the large read buffer (p. 762)

**Overview of the large read buffer and max-yield optimizations**

You might experience reduced binary log replication performance when the binary log dump thread accesses the Aurora cluster volume while the cluster processes a high number of transactions. You can use the parameters `aurora_binlog_use_large_read_buffer`, `aurora_binlog_replication_max_yield_seconds`, and `aurora_binlog_read_buffer_size` to help minimize this type of contention.
When `aurora_binlog_replication_max_yield_seconds` is set to greater than 0, and the current binlog file of the dump thread is active, binary log dump thread waits up to a specified number of seconds for the current binlog file to be filled by transactions. This wait period avoids contention that can arise from replicating each binlog event individually. However, doing so increases the replica lag for binary log replicas. Those replicas can fall behind the source by the same number of seconds as the `aurora_binlog_replication_max_yield_seconds` setting.

The current binlog file means the binlog file that the dump thread is currently reading to perform replication. We consider that a binlog file is active when the binlog file is updating or open to be updated by incoming transactions. After Aurora MySQL fills up the active binlog file, MySQL creates and switches to a new binlog file. The old binlog file becomes inactive. It isn't updated by incoming transactions any longer.

**Note**
Before adjusting these parameters, measure your transaction latency and throughput over time. You might find that binary log replication performance is stable and has low latency even if there is occasional contention.

`aurora_binlog_use_large_read_buffer`

If this parameter is set to 1, Aurora MySQL optimizes binary log replication based on the settings of the parameters `aurora_binlog_read_buffer_size` and `aurora_binlog_replication_max_yield_seconds`. If `aurora_binlog_use_large_read_buffer` is 0, Aurora MySQL ignores the values of the `aurora_binlog_read_buffer_size` and `aurora_binlog_replication_max_yield_seconds` parameters.

`aurora_binlog_read_buffer_size`

Binary log dump threads with larger read buffer minimize the number of read I/O operations by reading more events for each I/O. The parameter `aurora_binlog_read_buffer_size` sets the read buffer size. The large read buffer effectively reduces binlog contentions when updating transactions generate binlog events fast enough to fill up the read buffer size before the dump threads start to read them.

**Note**
This parameter only has an effect when the cluster also has the setting `aurora_binlog_use_large_read_buffer=1`. Increasing the size of the read buffer doesn't affect the performance of binary log replication. Binary log dump threads don't wait for updating transactions to fill up the read buffer.

`aurora_binlog_replication_max_yield_seconds`

If your workload requires low transaction latency, and you can tolerate some replication lag, you can increase the `aurora_binlog_replication_max_yield_seconds` parameter. This parameter controls the maximum yield property of binary log replication in your cluster.

**Note**
This parameter only has an effect when the cluster also has the setting `aurora_binlog_use_large_read_buffer=1`.

Aurora MySQL recognizes any change to the `aurora_binlog_replication_max_yield_seconds` parameter value immediately. You don't need to restart the DB instance. However, when you enable this setting, the dump thread only starts to yield when the current binlog file reaches its maximum size of 128 MB and is rotated to a new file.

**Related parameters**

Use the following DB cluster parameters to enable the binlog optimization.
Binlog optimization parameters for Aurora MySQL version 2.04.5 and later

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Valid Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aurora_binlog_use_large_read_buffer</td>
<td>0, 1</td>
<td></td>
<td>Switch for turning on the feature of replication improvement. When it is 1, the binary log dump thread uses aurora_binlog_read_buffer_size for binary log replication; otherwise default buffer size (8K) is used.</td>
</tr>
<tr>
<td>aurora_binlog_read_buffer_size</td>
<td>8192-536870912</td>
<td></td>
<td>Read buffer size used by binary log dump thread when the parameter aurora_binlog_use_large_read_buffer is set to 1.</td>
</tr>
<tr>
<td>aurora_binlog_replication_max_yield_seconds</td>
<td>0-36000</td>
<td></td>
<td>For Aurora MySQL versions between 2.04.5 - 2.04.8 and between 2.05 - 2.08.* (inclusive), the maximum accepted value is 45. You can tune it to a higher value on 2.04.9 and later versions of 2.04.*, and on 2.09 and later versions. This parameter works only when the parameter aurora_binlog_use_large_read_buffer is set to 1.</td>
</tr>
</tbody>
</table>

Binlog optimization parameters for Aurora MySQL version 1.17.6 and later

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Valid Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aurora_binlog_use_large_read_buffer</td>
<td>0, 1</td>
<td></td>
<td>Switch for turning on the feature of replication improvement. When it is 1, the binary log dump thread uses aurora_binlog_read_buffer_size for binary log replication. Otherwise, the default buffer size (8 K) is used.</td>
</tr>
<tr>
<td>aurora_binlog_read_buffer_size</td>
<td>8192-536870912</td>
<td></td>
<td>Read buffer size used by binary log dump thread when the parameter aurora_binlog_use_large_read_buffer is set to 1.</td>
</tr>
</tbody>
</table>
Enabling binary log replication max-yield mechanism

You can turn on the binary log replication max-yield optimization as follows. Doing so minimizes latency for transactions on the binlog source instance. However, you might experience higher replication lag.

**To enable the max-yield binlog optimization for an Aurora MySQL cluster**

1. Create or edit a DB cluster parameter group using the following parameter settings:
   - `aurora_binlog_use_large_read_buffer`: turn on with a value of `ON` or 1.
   - `aurora_binlog_replication_max_yield_seconds`: specify a value greater than 0.
2. Associate the DB cluster parameter group with the Aurora MySQL cluster that works as the binlog source. To do so, follow the procedures in Working with DB parameter groups and DB cluster parameter groups (p. 298).
3. Confirm that the parameter change takes effect. To do so, run the following query on the binlog source instance.

   ```sql
   SELECT @@aurora_binlog_use_large_read_buffer, @@aurora_binlog_replication_max_yield_seconds;
   ````

   Your output should be similar to the following.

   ```plaintext
   +---------------------------------------+-----------------------------------------------+
   | @@aurora_binlog_use_large_read_buffer | @@aurora_binlog_replication_max_yield_seconds |
   | 1                                    | 45                                           |
   +---------------------------------------+-----------------------------------------------+
   ```

Turning off the binary log replication max-yield optimization

You can turn off the binary log replication max-yield optimization as follows. Doing so minimizes replication lag. However, you might experience higher latency for transactions on the binlog source instance.
To turn off the max-yield optimization for an Aurora MySQL cluster

1. Make sure that the DB cluster parameter group associated with the Aurora MySQL cluster has
aurora_binlog_replication_max_yield_seconds set to 0. For more information about
setting configuration parameters using parameter groups, see Working with DB parameter groups
and DB cluster parameter groups (p. 298).

2. Confirm that the parameter change takes effect. To do so, run the following query on the binlog
source instance.

   ```
   SELECT @@aurora_binlog_replication_max_yield_seconds;
   ```

   Your output should be similar to the following.

   +-----------------------------------------------+
   | @@aurora_binlog_replication_max_yield_seconds |
   +-----------------------------------------------+
   | 0 |
If you use binlog replication and aren’t familiar with GTID-based replication with MySQL, see Replication with global transaction identifiers in the MySQL documentation for background.

**Note**
GTID-based replication is supported for MySQL 5.7-compatible clusters in Aurora MySQL version 2.04 and later. GTID-based replication isn’t supported for MySQL 5.6-compatible clusters in Aurora MySQL version 1.

**Topics**
- Overview of global transaction identifiers (GTIDs) (p. 763)
- Parameters for GTID-based replication (p. 763)
- Configuring GTID-based replication for an Aurora MySQL cluster (p. 764)
- Disabling GTID-based replication for an Aurora MySQL DB cluster (p. 765)

### Overview of global transaction identifiers (GTIDs)

**Global transaction identifiers (GTIDs)** are unique identifiers generated for committed MySQL transactions. You can use GTIDs to make binlog replication simpler and easier to troubleshoot.

**Note**
When Aurora synchronizes data among the DB instances in a cluster, that replication mechanism doesn’t involve the binary log (binlog). For Aurora MySQL, GTID-based replication only applies when you also use binlog replication to replicate into or out of an Aurora MySQL DB cluster from an external MySQL-compatible database.

MySQL uses two different types of transactions for binlog replication:
- **GTID transactions** – Transactions that are identified by a GTID.
- **Anonymous transactions** – Transactions that don’t have a GTID assigned.

In a replication configuration, GTIDs are unique across all DB instances. GTIDs simplify replication configuration because when you use them, you don’t have to refer to log file positions. GTIDs also make it easier to track replicated transactions and determine whether the source instance and replicas are consistent.

You typically use GTID-based replication with Aurora when replicating from an external MySQL-compatible database into an Aurora cluster. You can set up this replication configuration as part of a migration from an on-premises or Amazon RDS database into Aurora MySQL. If the external database already uses GTIDs, enabling GTID-based replication for the Aurora cluster simplifies the replication process.

You configure GTID-based replication for an Aurora MySQL cluster by first setting the relevant configuration parameters in a DB cluster parameter group. You then associate that parameter group with the cluster.

### Parameters for GTID-based replication

Use the following parameters to configure GTID-based replication.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gtid_mode</td>
<td>OFF, OFF_PERMISSIVE, ON_PERMISSIVE, ON</td>
<td>OFF specifies that new transactions are anonymous transactions (that is, don’t have GTIDs), and a transaction must be anonymous to be replicated.</td>
</tr>
</tbody>
</table>
Using GTID-based replication

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF_PERMISSIVE</td>
<td>specifies that new transactions are anonymous transactions, but all transactions can be replicated.</td>
<td></td>
</tr>
<tr>
<td>ON_PERMISSIVE</td>
<td>specifies that new transactions are GTID transactions, but all transactions can be replicated.</td>
<td></td>
</tr>
<tr>
<td>ON</td>
<td>specifies that new transactions are GTID transactions, and a transaction must be a GTID transaction to be replicated.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>enforce_gtid_consistency</th>
<th>OFF</th>
<th>allows transactions to violate GTID consistency.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>prevents transactions from violating GTID consistency.</td>
<td></td>
</tr>
<tr>
<td>WARN</td>
<td>allows transactions to violate GTID consistency but generates a warning when a violation occurs.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
In the AWS Management Console, the gtid_mode parameter appears as gtid-mode.

For GTID-based replication, use these settings for the DB cluster parameter group for your Aurora MySQL DB cluster:

- **ON** and **ON_PERMISSIVE** apply only to outgoing replication from an RDS DB instance or Aurora MySQL cluster. Both of these values cause your RDS DB instance or Aurora DB cluster to use GTIDs for transactions that are replicated to an external database. **ON** requires that the external database also use GTID-based replication. **ON_PERMISSIVE** makes GTID-based replication optional on the external database.

- **OFF_PERMISSIVE**, if set, means that your RDS DB instances or Aurora DB cluster can accept incoming replication from an external database. It can do this whether the external database uses GTID-based replication or not.

- **OFF**, if set, means that your RDS DB instances or Aurora DB cluster only accept incoming replication from external databases that don't use GTID-based replication.

**Tip**
Incoming replication is the most common binlog replication scenario for Aurora MySQL clusters. For incoming replication, we recommend that you set the GTID mode to **OFF_PERMISSIVE**. That setting allows incoming replication from external databases regardless of the GTID settings at the replication source.

For more information about parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

**Configuring GTID-based replication for an Aurora MySQL cluster**

When GTID-based replication is enabled for an Aurora MySQL DB cluster, the GTID settings apply to both inbound and outbound binlog replication.
To enable GTID-based replication for an Aurora MySQL cluster

1. Create or edit a DB cluster parameter group using the following parameter settings:
   - `gtid_mode` – ON or ON_PERMISSIVE
   - `enforce_gtid_consistency` – ON

2. Associate the DB cluster parameter group with the Aurora MySQL cluster. To do so, follow the procedures in Working with DB parameter groups and DB cluster parameter groups (p. 298).

Disabling GTID-based replication for an Aurora MySQL DB cluster

You can disable GTID-based replication for an Aurora MySQL DB cluster. Doing so means that the Aurora cluster can't perform inbound or outbound binlog replication with external databases that use GTID-based replication.

Note
In the following procedure, read replica means the replication target in an Aurora configuration with binlog replication to or from an external database. It doesn't mean the read-only Aurora Replica DB instances. For example, when an Aurora cluster accepts incoming replication from an external source, the Aurora primary instance acts as the read replica for binlog replication.

For more details about the stored procedures mentioned in this section, see Aurora MySQL stored procedures (p. 871).

To disable GTID-based replication for an Aurora MySQL DB cluster

1. On the Aurora primary instance, run the following procedure.

   ```
   CALL mysql.rds_set_master_auto_position(0);
   ```

2. Reset the `gtid_mode` to ON_PERMISSIVE.
   a. Make sure that the DB cluster parameter group associated with the Aurora MySQL cluster has `gtid_mode` set to ON_PERMISSIVE.
      For more information about setting configuration parameters using parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).
   b. Restart the Aurora MySQL DB cluster.

3. Reset the `gtid_mode` to OFF_PERMISSIVE:
   a. Make sure that the DB cluster parameter group associated with the Aurora MySQL cluster has `gtid_mode` set to OFF_PERMISSIVE.
   b. Restart the Aurora MySQL DB cluster.

4. On the Aurora primary instance, run the `SHOW MASTER STATUS` command.

   Your output should be similar to the following.

<table>
<thead>
<tr>
<th>File</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>mysql-bin-changelog.000031</td>
<td>107</td>
</tr>
</tbody>
</table>

   Note the file and position in your output.
b. On each read replica, use the file and position information from its source instance in the previous step to run the following query.

```
SELECT MASTER_POS_WAIT('file', position);
```

For example, if the file name is `mysql-bin-changelog.000031` and the position is `107`, run the following statement.

```
SELECT MASTER_POS_WAIT('mysql-bin-changelog.000031', 107);
```

If the read replica is past the specified position, the query returns immediately. Otherwise, the function waits. When the query returns for all read replicas, go to the next step.

5. Reset the GTID parameters to disable GTID-based replication:

   a. Make sure that the DB cluster parameter group associated with the Aurora MySQL cluster has the following parameter settings:

      - `gtid_mode` – OFF
      - `enforce_gtid_consistency` – OFF

   b. Restart the Aurora MySQL DB cluster.

---

### Working with Aurora multi-master clusters

Following, you can learn about Aurora multi-master clusters. In a multi-master cluster, all DB instances have read/write capability. Multi-master clusters have different availability characteristics, support for database features, and procedures for monitoring and troubleshooting than single-master clusters.

#### Topics

- Overview of Aurora multi-master clusters (p. 766)
- Creating an Aurora multi-master cluster (p. 772)
- Managing Aurora multi-master clusters (p. 777)
- Application considerations for Aurora multi-master clusters (p. 780)
- Performance considerations for Aurora multi-master clusters (p. 789)
- Approaches to Aurora multi-master clusters (p. 791)

#### Overview of Aurora multi-master clusters

Use the following background information to help you choose a multi-master or single-master cluster when you set up a new Aurora cluster. For you to make an informed choice, we recommend that you first understand how you plan to adapt your schema design and application logic to work best with a multi-master cluster.

For each new Amazon Aurora cluster, you can choose whether to create a single-master or multi-master cluster.

Most kinds of Aurora clusters are *single-master* clusters. For example, provisioned, Aurora Serverless, parallel query, and Global Database clusters are all single-master clusters. In a single-master cluster, a single DB instance performs all write operations and any other DB instances are read-only. If the writer DB instance becomes unavailable, a failover mechanism promotes one of the read-only instances to be the new writer.
In a **multi-master cluster**, all DB instances can perform write operations. The notions of a single read/write primary instance and multiple read-only Aurora Replicas don’t apply. There isn't any failover when a writer DB instance becomes unavailable, because another writer DB instance is immediately available to take over the work of the failed instance. We refer to this type of availability as **continuous availability**, to distinguish it from the high availability (with brief downtime during failover) offered by a single-master cluster.

Multi-master clusters work differently in many ways from the other kinds of Aurora clusters, such as provisioned, Aurora Serverless, and parallel query clusters. With multi-master clusters, you consider different factors in areas such as high availability, monitoring, connection management, and database features. For example, in applications where you can't afford even brief downtime for database write operations, a multi-master cluster can help to avoid an outage when a writer instance becomes unavailable. The multi-master cluster doesn’t use the failover mechanism, because it doesn’t need to promote another DB instance to have read/write capability. With a multi-master cluster, you examine metrics related to DML throughput, latency, and deadlocks for all DB instances instead of a single primary instance.

Currently, multi-master clusters require Aurora MySQL version 1, which is compatible with MySQL 5.6. When specifying the DB engine version in the AWS Management Console, AWS CLI, or RDS API, choose 5.6.10a.

To create a multi-master cluster, you choose **Multiple writers** under **Database features** when creating the cluster. Doing so enables different behavior for replication among DB instances, availability, and performance than other kinds of Aurora clusters. This choice remains in effect for the life of the cluster. Make sure that you understand the specialized use cases that are appropriate for multi-master clusters.

**Topics**

- Multi-master cluster terminology (p. 767)
- Multi-master cluster architecture (p. 769)
- Recommended workloads for multi-master clusters (p. 769)
- Advantages of multi-master clusters (p. 770)
- Limitations of multi-master clusters (p. 770)

**Multi-master cluster terminology**

You can understand the terminology about multi-master clusters by learning the following definitions. These terms are used throughout the documentation for multi-master clusters.

**Writer**

A DB instance that can perform write operations. In an Aurora multi-master cluster, all DB instances are writers. This is a significant difference from Aurora single-master clusters, where only one DB instance can act as a writer. With a single-master cluster, if the writer becomes unavailable, the failover mechanism promotes another DB instance to become the new writer. With a multi-master cluster, your application can redirect write operations from the failed DB instance to any other DB instance in the cluster.

**Multi-master**

An architecture for Aurora clusters where each DB instance can perform both read and write operations. Contrast this with **single-master**. Multi-master clusters are best suited for segmented workloads, such as for multitenant applications.

**Single-master**

The default architecture for Aurora clusters. A single DB instance (the primary instance) performs writes. All other DB instances (the Aurora Replicas) handle read-only query traffic. Contrast this with
*multi-master*. This architecture is appropriate for general-purpose applications. In such applications, a single DB instance can handle all the data manipulation language (DML) and data definition language (DDL) statements. Scalability issues mostly involve `SELECT` queries.

**Write conflict**

A situation that occurs when different DB instances attempt to modify the same data page at the same time. Aurora reports a write conflict to your application as a deadlock error. This error condition causes the transaction to roll back. Your application must detect the error code and retry the transaction.

The main design consideration and performance tuning goal with Aurora multi-master clusters is to divide your write operations between DB instances in a way that minimizes write conflicts. That is why multi-master clusters are well-suited for sharded applications. For details about the write conflict mechanism, see Conflict resolution for multi-master clusters (p. 790).

**Sharding**

A particular class of segmented workloads. The data is physically divided into many partitions, tables, databases, or even separate clusters. The containers for specific portions of the data are known as *shards*. In an Aurora multi-master cluster, each shard is managed by a specific DB instance, and a DB instance can be responsible for multiple shards. A sharded schema design maps well to the way you manage connections in an Aurora multi-master cluster.

**Shard**

The unit of granularity within a sharded deployment. It might be a table, a set of related tables, a database, a partition, or even an entire cluster. With Aurora multi-master clusters, you can consolidate the data for a sharded application into a single Aurora shared storage volume, making the database continuously available and the data easy to manage. You decide which shards are managed by each DB instance. You can change this mapping at any time, without physically reorganizing the data.

**Resharding**

Physically reorganizing sharded data so that different DB instances can handle specific tables or databases. You don't need to physically reorganize data inside Aurora multi-master clusters in response to changing workload or DB instance failures. You can avoid resharding operations because all DB instances in a cluster can access all databases and tables through the shared storage volume.

**Multitenant**

A particular class of segmented workloads. The data for each customer, client, or user is kept in a separate table or database. This design ensures isolation and helps you to manage capacity and resources at the level of individual users.

**Bring-your-own-shard (BYOS)**

A situation where you already have a database schema and associated applications that use sharding. You can transfer such deployments relatively easily to Aurora multi-master clusters. In this case, you can devote your effort to investigating the Aurora benefits such as server consolidation and high availability. You don't need to create new application logic to handle multiple connections for write requests.

**Global read-after-write (GRAW)**

A setting that introduces synchronization so that any read operations always see the most current state of the data. By default, the data seen by a read operation in a multi-master cluster is subject to replication lag, typically a few milliseconds. During this brief interval, a query on one DB instance might retrieve stale data if the same data is modified at the same time by a different DB instance. To enable this setting, change `aurora_mm_session_consistency_level` from its default setting of `INSTANCE_RAW` to `REGIONAL_RAW`. Doing so ensures cluster-wide consistency for read operations regardless of the DB instances that perform the reads and writes. For details on GRAW mode, see Consistency model for multi-master clusters (p. 782).
Multi-master cluster architecture

Multi-master clusters have a different architecture than other kinds of Aurora clusters. In multi-master clusters, all DB instances have read/write capability. Other kinds of Aurora clusters have a single dedicated DB instance that performs all write operations, while all other DB instances are read-only and handle only SELECT queries. Multi-master clusters don't have a primary instance or read-only Aurora Replicas.

Your application controls which write requests are handled by which DB instance. Thus, with a multi-master cluster, you connect to individual instance endpoints to issue DML and DDL statements. That's different than other kinds of Aurora clusters, where you typically direct all write operations to the single cluster endpoint and all read operations to the single reader endpoint.

The underlying storage for Aurora multi-master clusters is similar to storage for single-master clusters. Your data is still stored in a highly reliable, shared storage volume that grows automatically. The core difference lies in the number and type of DB instances. In multi-master clusters, there are \(N\) read/write nodes. Currently, the maximum for \(N\) is 4.

Multi-master clusters have no dedicated read-only nodes. Thus, the Aurora procedures and guidelines about Aurora Replicas don't apply to multi-master clusters. You can temporarily make a DB instance read-only to place read and write workloads on different DB instances. To do so, see Using instance read-only mode (p. 788).

Multi-master cluster nodes are connected using low-latency and low-lag Aurora replication. Multi-master clusters use all-to-all peer-to-peer replication. Replication works directly between writers. Every writer replicates its changes to all other writers.

DB instances in a multi-master cluster handle restart and recovery independently. If a writer restarts, there is no requirement for other writers to also restart. For details, see High availability considerations for Aurora multi-master clusters (p. 779).

Multi-master clusters keep track of all changes to data within all database instances. The unit of measurement is the data page, which has a fixed size of 16 KB. These changes include modifications to table data, secondary indexes, and system tables. Changes can also result from Aurora internal housekeeping tasks. Aurora ensures consistency between the multiple physical copies that Aurora keeps for each data page in the shared storage volume, and in memory on the DB instances.

If two DB instances attempt to modify the same data page at almost the same instant, a write conflict occurs. The earliest change request is approved using a quorum voting mechanism. That change is saved to permanent storage. The DB instance whose change isn't approved rolls back the entire transaction containing the attempted change. Rolling back the transaction ensures that data is kept in a consistent state, and applications always see a predictable view of the data. Your application can detect the deadlock condition and retry the entire transaction.

For details about how to minimize write conflicts and associated performance overhead, see Conflict resolution for multi-master clusters (p. 790).

Recommended workloads for multi-master clusters

Multi-master clusters work best with certain kinds of workloads.

Active-passive workloads

With an active-passive workload, you perform all read and write operations on one DB instance at a time. You hold any other DB instances in the Aurora cluster in reserve. If the original active DB instance becomes unavailable, you immediately switch all read and write operations to the other DB instance. With this configuration, you minimize any downtime for write operations. The other DB instance can take over all processing for your application without performing a failover.
Active-active workloads

With an active-active workload, you perform read and write operations to all the DB instances at the same time. In this configuration, you typically segment the workload so that the different DB instances don't modify the same underlying data at the same time. Doing so minimizes the chance for write conflicts.

Multi-master clusters work well with application logic that's designed for a segmented workload. In this type of workload, you divide write operations by database instance, database, table, or table partition. For example, you can run multiple applications on the same cluster, each assigned to a specific DB instance. Alternatively, you can run an application that uses multiple small tables, such as one table for each user of an online service. Ideally, you design your schema so that write operations for different DB instances don't perform simultaneous updates to overlapping rows within the same tables. Sharded applications are one example of this kind of architecture.

For examples of designs for active-active workloads, see Using a multi-master cluster for a sharded database (p. 791).

Advantages of multi-master clusters

You can take advantage of the following benefits with Aurora multi-master clusters:

- Multi-master clusters improve Aurora's already high availability. You can restart a read/write DB instance without causing other DB instances in the cluster to restart. There is no failover process and associated delay when a read/write DB instance becomes unavailable.
- Multi-master clusters are well-suited to sharded or multitenant applications. As you manage the data, you can avoid complex resharding operations. You might be able to consolidate sharded applications with a smaller number of clusters or DB instances. For details, see Using a multi-master cluster for a sharded database (p. 791).
- Aurora detects write conflicts immediately, not when the transaction commits. For details about the write conflict mechanism, see Conflict resolution for multi-master clusters (p. 790).

Limitations of multi-master clusters

Note

Aurora multi-master clusters are highly specialized for continuous availability use cases. Thus, such clusters might not be generally applicable to all workloads. Your requirements for performance, scalability, and availability might be satisfied by using a larger DB instance class with an Aurora single-master cluster. If so, consider using a provisioned or Aurora Serverless cluster.

AWS and Aurora limitations

The following limitations currently apply to the AWS and Aurora features that you can use with multi-master clusters:

- Currently, you can have a maximum of four DB instances in a multi-master cluster.
- Currently, all DB instances in a multi-master cluster must be in the same AWS Region.
- You can't enable cross-Region replicas from multi-master clusters.
- Multi-master clusters are available in the following AWS Regions:
  - US East (N. Virginia) Region
  - US East (Ohio) Region
  - US West (Oregon) Region
  - Asia Pacific (Mumbai) Region
Overview of multi-master clusters

• Asia Pacific (Seoul) Region
• Asia Pacific (Tokyo) Region
• Europe (Frankfurt) Region
• Europe (Ireland) Region
• The **Stop** action isn't available for multi-master clusters.
• The Aurora survivable page cache, also known as the survivable buffer pool, isn't supported for multi-master clusters.
• A multi-master cluster doesn't do any load balancing for connections. Your application must implement its own connection management logic to distribute read and write operations among multiple DB instance endpoints. Typically, in a bring-your-own-shard (BYOS) application, you already have logic to map each shard to a specific connection. To learn how to adapt the connection management logic in your application, see Connection management for multi-master clusters (p. 781).
• Multi-master clusters have some processing and network overhead for coordination between DB instances. This overhead has the following consequences for write-intensive and read-intensive applications:
  • Throughput benefits are most obvious on busy clusters with multiple concurrent write operations. In many cases, a traditional Aurora cluster with a single primary instance can handle the write traffic for a cluster. In these cases, the benefits of multi-master clusters are mostly for high availability rather than performance.
  • Single-query performance is generally lower than for an equivalent single-master cluster.
• You can't take a snapshot created on a single-master cluster and restore it on a multi-master cluster, or the opposite. Instead, to transfer all data from one kind of cluster to the other, use a logical dump produced by a tool such as AWS Database Migration Service (AWS DMS) or the `mysqldump` command.
• You can't use the parallel query, Aurora Serverless, or Global Database features on a multi-master cluster.

The multi-master aspect is a permanent choice for a cluster. You can't switch an existing Aurora cluster between a multi-master cluster and another kind such as Aurora Serverless or parallel query.

• The zero-downtime patching (ZDP) and zero-downtime restart (ZDR) features aren't available for multi-master clusters.
• Integration with other AWS services such as AWS Lambda, Amazon S3, and AWS Identity and Access Management isn't available for multi-master clusters.
• The Performance Insights feature isn't available for multi-master clusters.
• You can't clone a multi-master cluster.
• You can't enable the backtrack feature for multi-master clusters.

Database engine limitations

The following limitations apply to the database engine features that you can use with a multi-master cluster:

• You can't perform binary log (binlog) replication to or from a multi-master cluster. This limitation means you also can't use global transaction ID (GTID) replication in a multi-master cluster.
• The event scheduler isn't available for multi-master clusters.
• The hash join optimization isn't enabled on multi-master clusters.
• The query cache isn't available on multi-master clusters.
• You can't use certain SQL language features on multi-master clusters. For the full list of SQL differences, and instructions about adapting your SQL code to address these limitations, see SQL considerations for multi-master clusters (p. 780).
Creating an Aurora multi-master cluster

You choose the multi-master or single-master architecture at the time you create an Aurora cluster. The following procedures show where to make the multi-master choice. If you haven't created any Aurora clusters before, you can learn the general procedure in Creating an Amazon Aurora DB cluster (p. 118).

Console

To create an Aurora multi-master cluster from the AWS Management Console, you make the following choices. On the first screen, you select an Aurora cluster:
Amazon RDS > Databases > Create database

Create database

Database settings

Quick create

Provides the fastest way to get started with your database. You can modify it later.

Engine options

- Amazon Aurora
- MySQL
- PostgreSQL
- Oracle
You also choose MySQL 5.6 compatibility and location **Regional**:

- **Amazon Aurora with MySQL compatibility**
- **Amazon Aurora with PostgreSQL compatibility**

**DB engine version Info**

**Aurora MySQL 1.21.0 (Compatible with MySQL 5.6)**

Select engine version Aurora MySQL 1.21.0 (Compatible with MySQL 5.6) to use created parallel query, multiple writers, serverless, or global databases.

**Database location**

- **Regional Info**
  You provision your Aurora database in a single region.
- **Global Info**
  You can provision your Aurora database in multiple regions. Writes in the primary typical latency of <1 sec to secondary regions.

On the second screen, choose **Multiple writers** under **Database features**.
Fill in the other settings for the cluster. This part of the procedure is the same as the general procedure for creating an Aurora cluster in Creating a DB cluster (p. 119).

After you create the multi-master cluster, add two DB instances to it by following the procedure in Adding Aurora replicas to a DB cluster (p. 345). Use the same AWS instance class for all DB instances within the multi-master cluster.

After you create the multi-master cluster and associated DB instances, you see the cluster in the AWS Management Console Databases page as follows. All DB instances show the role Writer.
AWS CLI

To create a multi-master cluster with the AWS CLI, run the `create-db-cluster` AWS CLI command and include the option `--engine_mode=multimaster`.

The following command shows the syntax for creating an Aurora cluster with multi-master replication. For the general procedure to create an Aurora cluster, see Creating a DB cluster (p. 119).

For Linux, macOS, or Unix:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora --engine-version 5.6.10a --master-username user-name --master-user-password password --db-subnet-group-name my_subnet_group --vpc-security-group-ids my_vpc_id --engine-mode multimaster
```

For Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster --engine aurora --engine-version 5.6.10a --master-username user-name --master-user-password password --db-subnet-group-name my_subnet_group --vpc-security-group-ids my_vpc_id --engine-mode multimaster
```

After you create the multi-master cluster, add a second DB instance to it by following the procedure in Adding Aurora replicas to a DB cluster (p. 345). Use the same AWS instance class for all DB instances within the multi-master cluster.
RDS API

To create a multi-master cluster with the RDS API, run the `CreateDBCluster` operation. Specify the value `multimaster` for the `EngineMode` parameter. For the general procedure to create an Aurora cluster, see `Creating a DB cluster (p. 119)`.

After you create the multi-master cluster, add two DB instances to it by following the procedure in `Adding Aurora replicas to a DB cluster (p. 345)`. Use the same AWS instance class for all DB instances within the multi-master cluster.

Adding a DB instance to a multi-master cluster

You need more than one DB instance to see the benefits of a multi-master cluster. After you create the first instance, you can create other DB instances, up to a maximum of four DB instances, using the procedures from `Adding Aurora replicas to a DB cluster (p. 345)`. The difference for multi-master clusters is that the new DB instances all have read/write capability instead of being read-only Aurora Replicas. Use the same AWS instance class for all DB instances within the multi-master cluster.

Managing Aurora multi-master clusters

You do most management and administration for Aurora multi-master clusters the same way as for other kinds of Aurora clusters. The following sections explain the differences and unique features of multi-master clusters for administration and management.

Topics

- Monitoring an Aurora multi-master cluster (p. 777)
- Data ingestion performance for multi-master clusters (p. 778)
- Exporting data from a multi-master cluster (p. 778)
- High availability considerations for Aurora multi-master clusters (p. 779)
- Replication between multi-master clusters and other clusters (p. 779)
- Upgrading a multi-master cluster (p. 779)

Monitoring an Aurora multi-master cluster

Most of the monitoring and diagnostic features supported by MySQL and Aurora single-master clusters are also supported for multi-master clusters:

- MySQL error logs, general logs and slow query logs.
- MySQL built-in diagnostic features such as SHOW commands, status variables, InnoDB runtime status tables, and so on.
- Advanced Auditing.
- CloudWatch metrics.
- Enhanced Monitoring.

Aurora multi-master clusters don't currently support the following monitoring features:

- Performance Insights.
Data ingestion performance for multi-master clusters

One best practice for DML operations on a multi-master cluster is to keep transactions small and brief. Also, route write operations for a particular table or database to a specific DB instance. Doing a bulk import might require relaxing the guidance for transaction size. However, you can still distribute the write operations to minimize the chance of write conflicts.

To distribute the write workload from a bulk import

1. Issue a separate `mysqldump` command for each database, table, or other object in your schema. Store the results of each `mysqldump` in a file whose name reflects the object being dumped. As an alternative, you can use a specialized dump and import tool that can automatically dump multiple tables in parallel, such as `mydumper`.

2. Run a separate `mysql` session for each data file, connecting to the appropriate instance endpoint that handles the corresponding schema object. Again, as an alternative, you can use a specialized parallel import command, such as `myloader`.

3. Run the import sessions in parallel across the DB instances in the multi-master cluster, instead of waiting for each to finish before starting the next.

You can use the following techniques to import data into an Aurora multi-master cluster:

- You can import logical (SQL-format) dumps from other MySQL-compatible servers to Aurora multi-master clusters, if the statements don't use any features that aren't supported in Aurora. For example, a logical dump from a table containing MySQL Full-Text Search (FTS) indexes doesn't work because the FTS feature is not supported on multi-master clusters.

- You can use managed services such as DMS to migrate data into an Aurora multi-master cluster.

- For migrations into an Aurora multi-master cluster from a server that isn't compatible with MySQL, follow existing instructions for heterogeneous Aurora migrations.

- Aurora multi-master clusters can produce MySQL-compatible logical dumps in SQL format. Any migration tool (for example, AWS DMS) that can understand such format can consume data dumps from Aurora multi-master clusters.

- Aurora doesn't support binary logging with the multi-master cluster as the binlog master or worker. You can't use binlog-based CDC tools with multi-master clusters.

- When migrating from non-MySQL-compatible servers, you can replicate into a multi-master cluster using the continuous change data capture (CDC) feature of AWS DMS. That type of replication transmits SQL statements to the destination cluster, thus the restriction on binlog replication doesn't apply.

For a detailed discussion of migration techniques and recommendations, see the Amazon Aurora migration handbook AWS whitepaper. Some of the migration methods listed in the handbook might not apply to Aurora multi-master clusters, but the document is a great overall source of knowledge about Aurora migration topics.

Exporting data from a multi-master cluster

You can save a snapshot of a multi-master cluster and restore it to another multi-master cluster. Currently, you can't restore a multi-master cluster snapshot into a single-master cluster.

To migrate data from a multi-master cluster to a single-master cluster, use a logical dump and restore with a tool such as `mysqldump`.

You can't use a multi-master cluster as the source or destination for binary log replication.
High availability considerations for Aurora multi-master clusters

In an Aurora multi-master cluster, any DB instance can restart without causing any other instance to restart. This behavior provides a higher level of availability for read/write and read-only connections than for Aurora single-master clusters. We refer to this availability level as continuous availability. In multi-master clusters, there is no downtime for write availability when a writer DB instance fails. Multi-master clusters don't use the failover mechanism, because all cluster instances are writable. If a DB instance fails in a multi-master cluster, your application can redirect the workload towards the remaining healthy instances.

In a single-master cluster, restarting the primary instance makes write operations unavailable until the failover mechanism promotes a new primary instance. Read-only operations also experience a brief downtime because all the Aurora Replicas in the cluster restart.

To minimize downtime for applications in a multi-master cluster, implement frequent SQL-level health checks. If a DB instance in a multi-master cluster becomes unavailable, you can decide what to do based on the expected length of the outage and the urgency of write operations in the workload. If you expect the outage to be brief and the write operations aren't urgent, you can wait for the DB instance to recover before resuming the workload that is normally handled by that DB instance. Alternatively, you can redirect that workload to a different DB instance. The underlying data remains available at all time to all DB instances in the cluster. The highly distributed Aurora storage volume keeps the data continuously available even in the unlikely event of a failure affecting an entire AZ. For information about the timing considerations for switching write operations away from an unavailable DB instance, see Using a multi-master cluster as an active standby (p. 792).

Replication between multi-master clusters and other clusters

Multi-master clusters don't support incoming or outgoing binary log replication.

Upgrading a multi-master cluster

Aurora multi-master clusters use the same version numbering scheme, with major and minor version numbers, as other kinds of Aurora clusters. However, the Enable auto minor version upgrade setting doesn't apply for multi-master clusters.

When you upgrade an Aurora multi-master cluster, typically the upgrade procedure moves the database engine from the current version to the next higher version. If you upgrade to an Aurora version that increments the version number by more than one, the upgrade uses a multi-step approach. Each DB instance is upgraded to the next higher version, then the next one after that, and so on until it reaches the specified upgrade version.

The approach is different depending on whether there are any backwards-incompatible changes between the old and new versions. For example, updates to the system schema are considered backwards-incompatible changes. You can check whether a specific version contains any backwards-incompatible changes by consulting the release notes.

If there aren't any incompatible changes between the old and new versions, each DB instance is upgraded and restarted individually. The upgrades are staggered so that the overall cluster doesn't experience any downtime. At least one DB instance is available at any time during the upgrade process.

If there are incompatible changes between the old and new versions, Aurora performs the upgrade in offline mode. All cluster nodes are upgraded and restarted at the same time. The cluster experiences some downtime, to avoid an older engine writing to newer system tables.

Zero-downtime patching (ZDP) isn't currently supported for Aurora multi-master clusters.
Application considerations for Aurora multi-master clusters

Following, you can learn any changes that might be required in your applications due to differences in feature support or behavior between multi-master and single-master clusters.

Topics
- SQL considerations for multi-master clusters (p. 780)
- Connection management for multi-master clusters (p. 781)
- Consistency model for multi-master clusters (p. 782)
- Multi-master clusters and transactions (p. 783)
- Write conflicts and deadlocks in multi-master clusters (p. 783)
- Multi-master clusters and locking reads (p. 784)
- Performing DDL operations on a multi-master cluster (p. 785)
- Using autoincrement columns (p. 786)
- Multi-master clusters feature reference (p. 787)

SQL considerations for multi-master clusters

The following are the major limitations that apply to the SQL language features you can use with a multi-master cluster:

- In a multi-master cluster, you can't use certain settings or column types that change the row layout. You can't enable the innodb_large_prefix configuration option. You can't use the column types MEDIUMTEXT, MEDIUMBLOB, LONGTEXT, or LONGBLOB.
- You can't use the CASCADE clause with any foreign key columns in a multi-master cluster.
- Multi-master clusters can't contain any tables with full-text search (FTS) indexes. Such tables can't be created on or imported into multi-master clusters.
- DDL works differently on multi-master and single-master clusters. For example, the fast DDL mechanism isn't available for multi-master clusters. You can't write to a table in a multi-master cluster while the table is undergoing DDL. For full details on DDL differences, see Performing DDL operations on a multi-master cluster (p. 785).
- You can't use the SERIALIZABLE transaction isolation level on multi-master clusters. On Aurora single-master clusters, you can use this isolation level on the primary instance.
- Autoincrement columns are handled using the auto_increment_increment and auto_increment_offset parameters. Parameter values are predetermined and not configurable. The parameter auto_increment_increment is set to 16, which is the maximum number of instances in any Aurora cluster. However, multi-master clusters currently have a lower limit on the number of DB instances. For details, see Using autoincrement columns (p. 786).

When adapting an application for an Aurora multi-master cluster, approach that activity the same as a migration. You might have to stop using certain SQL features, and change your application logic for other SQL features:

- In your CREATE TABLE statements, change any columns defined as MEDIUMTEXT, MEDIUMBLOB, LONGTEXT, or LONGBLOB to shorter types that don't require off-page storage.
- In your CREATE TABLE statements, remove the CASCADE clause from any foreign key declarations. Add application logic if necessary to emulate the CASCADE effects through INSERT or DELETE statements.
• Remove any use of InnoDB fulltext search (FTS) indexes. Check your source code for \texttt{MATCH()} operators in \texttt{SELECT} statements, and \texttt{FULLTEXT} keywords in DDL statements. Check if any table names from the \texttt{INFORMATION_SCHEMA.INNODB_SYS_TABLES} system table contain the string \texttt{FTS_}.

• Check the frequency of DDL operations such as \texttt{CREATE TABLE} and \texttt{DROP TABLE} in your application. Because DDL operations have more overhead in multi-master clusters, avoid running many small DDL statements. For example, look for opportunities to create needed tables ahead of time. For information about DDL differences with multi-master clusters, see Performing DDL operations on a multi-master cluster (p. 785).

• Examine your use of autoincrement columns. The sequences of values for autoincrement columns are different for multi-master clusters than other kinds of Aurora clusters. Check for the \texttt{AUTO_INCREMENT} keyword in DDL statements, the function name \texttt{last_insert_id()} in \texttt{SELECT} statements, and the name \texttt{innodb_autoinc_lock_mode} in your custom configuration settings. For details about the differences and how to handle them, see Using autoincrement columns (p. 786).

• Check your code for the \texttt{SERIALIZABLE} keyword. You can't use this transaction isolation level with a multi-master cluster.

Connection management for multi-master clusters

The main connectivity consideration for multi-master clusters is the number and type of the available DNS endpoints. With multi-master clusters, you often use the instance endpoints, which you rarely use in other kinds of Aurora clusters.

Aurora multi-master clusters have the following kinds of endpoints:

Cluster endpoint

This type of endpoint always points to a DB instance with read/write capability. Each multi-master cluster has one cluster endpoint.

Because applications in multi-master clusters typically include logic to manage connections to specific DB instances, you rarely need to use this endpoint. It's mostly useful for connecting to a multi-master cluster to perform administration.

You can also connect to this endpoint to examine the cluster topology when you don't know the status of the DB instances in the cluster. To learn that procedure, see Describing cluster topology (p. 788).

DB instance endpoint

This type of endpoint connects to specific named DB instances. For Aurora multi-master clusters, your application typically uses the DB instance endpoints for all or nearly all connections. You decide which DB instance to use for each SQL statement based on the mapping between your shards and the DB instances in the cluster. Each DB instance has one such endpoint. Thus the multi-master cluster has one or more of these endpoints, and the number changes as DB instances are added to or removed from a multi-master cluster.

The way you use DB instance endpoints is different between single-master and multi-master clusters. For single-master clusters, you typically don't use this endpoint often.

Custom endpoint

This type of endpoint is optional. You can create one or more custom endpoints to group together DB instances for a specific purpose. When you connect to the endpoint, Aurora returns the IP address of a different DB instance each time. In multi-master clusters, you typically use custom endpoints to designate a set of DB instances to use mostly for read operations. We recommend not using custom endpoints with multi-master clusters to load-balance write operations, because doing so increases the chance of write conflicts.
Multi-master clusters don't have reader endpoints. Where practical, issue `SELECT` queries using the same DB instance endpoint that normally writes to the same table. Doing so makes more effective use of cached data from the buffer pool, and avoids potential issues with stale data due to replication lag within the cluster. If you don’t locate `SELECT` statements on the same DB instances that write to the same tables, and you require strict read after write guarantee for certain queries, consider running those queries using the global read-after-write (GRAW) mechanism described in Consistency model for multi-master clusters (p. 782).

For general best practices of Aurora and MySQL connection management, see the Amazon Aurora migration handbook AWS whitepaper.

For information about how to emulate read-only DB instances in multi-master DB clusters, see Using instance read-only mode (p. 788).

Follow these guidelines when creating custom DNS endpoints and designing drivers and connectors for Aurora multi-master clusters:

- For DDL, DML, and DCL statements, don’t use endpoints or connection routing techniques that operate in round-robin or random fashion.
- Avoid long-running write queries and long write transactions unless these transactions are guaranteed not to conflict with other write traffic in the cluster.
- Prefer to use autocommitted transactions. Where practical, avoid `autocommit=0` settings at global or session level. When you use a database connector or database framework for your programming language, check that `autocommit` is turned on for applications that use the connector or framework. If needed, add `COMMIT` statements at logical points throughout your code to ensure that transactions are brief.
- When global read consistency or read-after-write guarantee is required, follow recommendations for global read-after-write (GRAW) described in Consistency model for multi-master clusters (p. 782).
- Use the cluster endpoint for DDL and DCL statements where practical. The cluster endpoint helps to minimize the dependency on the hostnames of the individual DB instances. You don’t need to divide DDL and DCL statements by table or database, as you do with DML statements.

**Consistency model for multi-master clusters**

Aurora multi-master clusters support a global read-after-write (GRAW) mode that is configurable at the session level. This setting introduces extra synchronization to create a consistent read view for each query. That way, queries always see the very latest data. By default, the replication lag in a multi-master cluster means that a DB instance might see old data for a few milliseconds after the data was updated. Enable this feature if your application depends on queries seeing the latest data changes made by any other DB instance, even if the query has to wait as a result.

**Note**

Replication lag doesn't affect your query results if you write and then read the data using the same DB instance. Thus, the GRAW feature applies mainly to applications that issue multiple concurrent write operations through different DB instances.

When using the GRAW mode, don’t enable it for all queries by default. Globally consistent reads are noticeably slower than local reads. Therefore, use GRAW selectively for queries that require it.

Be aware of these considerations for using GRAW:

- GRAW involves performance overhead due to the cost of establishing a cluster-wide consistent read view. The transaction must first determine a cluster-wide consistent point in time, then replication must catch up to that time. The total delay depends on the workload, but it's typically in the range of tens of milliseconds.
- You can't change GRAW mode within a transaction.
• When using GRAW without explicit transactions, each individual query incurs the performance overhead of establishing a globally consistent read view.
• With GRAW enabled, the performance penalty applies to both reads and writes.
• When you use GRAW with explicit transactions, the overhead of establishing a globally consistent view applies once for each transaction, when the transaction starts. Queries performed later in the transaction are as fast as if run without GRAW. If multiple successive statements can all use the same read view, you can wrap them in a single transaction for a better overall performance. That way, the penalty is only paid once per transaction instead of per query.

Multi-master clusters and transactions

Standard Aurora MySQL guidance applies to Aurora multi-master clusters. The Aurora MySQL database engine is optimized for short-lived SQL statements. These are the types of statements typically associated with online transaction processing (OLTP) applications.

In particular, make your write transactions as short as possible. Doing so reduces the window of opportunity for write conflicts. The conflict resolution mechanism is optimistic, meaning that it performs best when write conflicts are rare. The tradeoff is that when conflicts occur, they incur substantial overhead.

There are certain workloads that benefit from large transactions. For example, bulk data imports are significantly faster when run using multi-megabyte transactions rather than single-statement transactions. If you observe an unacceptable number of conflicts while running such workloads, consider the following options:

• Reduce transaction size.
• Reschedule or rearrange batch jobs so that they don't overlap and don't provoke conflicts with other workloads. If practical, reschedule the batch jobs so that they run during off-peak hours.
• Refactor the batch jobs so that they run on the same writer instance as the other transactions causing conflicts. When conflicting transactions are run on the same instance, the transactional engine manages access to the rows. In that case, storage-level write conflicts don't occur.

Write conflicts and deadlocks in multi-master clusters

One important performance aspect for multi-master clusters is the frequency of write conflicts. When such a problem condition occurs in the Aurora storage subsystem, your application receives a deadlock error and performs the usual error handling for deadlock conditions. Aurora uses a lock-free optimistic algorithm that performs best when such conflicts are rare.

In a multi-master cluster, all the DB instances can write to the shared storage volume. For every data page you modify, Aurora automatically distributes several copies across multiple Availability Zones (AZs). A write conflict can occur when multiple DB instances try to modify the same data page within a very short time. The Aurora storage subsystem detects that the changes overlap and performs conflict resolution before finalizing the write operation.

Aurora detects write conflicts at the level of the physical data pages, which have a fixed size of 16 KiB. Thus, a conflict can occur even for changes that affect different rows, if the rows are both within the same data page.

When conflicts do occur, the cleanup operation requires extra work to undo the changes from one of the DB instances. From the point of view of your application, the transaction that caused the conflict encounters a deadlock and Aurora rolls back that whole transaction. Your application receives error code 1213.

Undoing the transaction might require modifying many other data pages whose changes were already applied to the Aurora storage subsystem. Depending on how much data was changed by the transaction,
undoing it might involve substantial overhead. Therefore, minimizing the potential for write conflicts is a crucial design consideration for an Aurora multi-master cluster.

Some conflicts result from changes that you initiate. These changes include SQL statements, transactions, and transaction rollbacks. You can minimize these kinds of conflicts through your schema design and the connection management logic in your application.

Other conflicts happen because of simultaneous changes from both a SQL statement and an internal server thread. These conflicts are hard to predict because they depend on internal server activity that you might not be aware of. The two major kinds of internal activity that cause these conflicts are garbage collection (known as purge), and transaction rollbacks performed automatically by Aurora. For example, Aurora performs rollbacks automatically during crash recovery or if a client connection is lost.

A transaction rollback physically reverts page changes that were already made. A rollback produces page changes just like the original transaction does. A rollback takes time, potentially several times as long as the original transaction. While the rollback is proceeding, the changes it produces can come into conflict with your transactions.

Garbage collection has to do with multi-version concurrency control (MVCC), which is the concurrency control method used by the Aurora MySQL transactional engine. With MVCC, data mutations create new row versions, and the database keeps multiple versions of rows to achieve transaction isolation while permitting concurrent access to data. Row versions are removed (purged) when they're no longer needed. Here again, the process of purging produces page changes, which might conflict with your transactions. Depending on the workload, the database can develop a purge lag: a queue of changes waiting to be garbage collected. If the lag grows substantially, the database might need a considerable amount of time to complete the purge, even if you stop submitting SQL statements.

If an internal server thread encounters a write conflict, Aurora retries automatically. In contrast, your application must handle the retry logic for any transactions that encounter conflicts.

When multiple transactions from the same DB instance cause these kinds of overlapping changes, Aurora uses the standard transaction concurrency rules. For example, if two transactions on the same DB instance modify the same row, one of them waits. If the wait is longer than the configured timeout (innodb_lock_wait_timeout, by default 50 seconds), the waiting transaction aborts with a “Lock wait timeout exceeded” message.

Multi-master clusters and locking reads

Aurora multi-master clusters support locking reads in the following forms.

```
SELECT ... FOR UPDATE
SELECT ... LOCK IN SHARE MODE
```

For more information about locking reads, see the MySQL reference manual.

Locking read operations are supported on all nodes, but the lock scope is local to the node on which the command was run. A locking read performed on one writer doesn't prevent other writers from accessing or modifying the locked rows. Despite this limitation, you can still work with locking reads in use cases that guarantee strict workload scope separation between writers, such as in sharded or multitenant databases.

Consider the following guidelines:

- Remember that a node can always see its own changes immediately and without delay. When possible, you can colocate reads and writes on the same node to eliminate the GRAW requirement.
- If read-only queries must be run with globally consistent results, use GRAW.
- If read-only queries care about data visibility but not global consistency, use GRAW or introduce a timed wait before each read. For example, a single application thread might maintain connections C1 and C2 to two different nodes. The application writes on C1 and reads on C2. In such case, the
application can issue a read immediately using GRAW, or it can sleep before issuing a read. The sleep time should be equal to or longer than the replication lag (usually approximately 20–30 ms).

The read-after-write feature is controlled using the `aurora_mm_session_consistency_level` session variable. The valid values are `INSTANCE_RAW` for local consistency mode (default) and `REGIONAL_RAW` for cluster-wide consistency:

**Performing DDL operations on a multi-master cluster**

The SQL data definition language (DDL) statements have special considerations for multi-master clusters. These statements sometimes cause substantial reorganization of the underlying data. Such large-scale changes potentially affect many data pages in the shared storage volume. The definitions of tables and other schema objects are held in the `INFORMATION_SCHEMA` tables. Aurora handles changes to those tables specially to avoid write conflicts when multiple DB instances run DDL statements at the same time.

For DDL statements, Aurora automatically delegates the statement processing to a special server process in the cluster. Because Aurora centralizes the changes to the `INFORMATION_SCHEMA` tables, this mechanism avoids the potential for write conflicts between DDL statements.

DDL operations prevent concurrent writes to that table. During a DDL operation on a table, all DB instances in the multi-master cluster are limited to read-only access to that table until the DDL statement finishes.

The following DDL behaviors are the same in Aurora single-master and multi-master clusters:

- A DDL performed on one DB instance causes other instances to terminate any connections actively using the table.
- Session-level temporary tables can be created on any node using the `MyISAM` or `MEMORY` storage engines.
- DDL operations on very large tables might fail if the DB instance doesn't have sufficient local temporary storage.

Note the following DDL performance considerations in multi-master clusters:

- Try to avoid issuing large numbers of short DDL statements in your application. Create databases, tables, partitions, columns, and so on, in advance where practical. Replication overhead can impose significant performance overhead for simple DDL statements that are typically very quick. The statement doesn't finish until the changes are replicated to all DB instances in the cluster. For example, multi-master clusters take longer than other Aurora clusters to create empty tables, drop tables, or drop schemas containing many tables.

  If you do need to perform a large set of DDL operations, you can reduce the network and coordination overhead by issuing the statements in parallel through multiple threads.

  Long-running DDL statements are less affected, because the replication delay is only a small fraction of the total time for the DDL statement.

  Performance of DDLs on session-level temporary tables should be roughly equivalent on Aurora single-master and multi-master clusters. Operations on temporary tables happen locally and are not subject to synchronous replication overhead.

**Using Percona online schema change with multi-master clusters**

The `pt-online-schema-change` tool works with multi-master clusters. You can use it if your priority is to run table modifications in the most nonblocking manner. However, be aware of the write conflict implications of the schema change process.
At a high level, the `pt-online-schema-change` tool works as follows:

1. It creates a new, empty table with the desired structure.
2. It creates `DELETE`, `INSERT` and `UPDATE` triggers on the original table to redo any data changes on the original table on top of the new table.
3. It moves existing rows into the new table using small chunks while ongoing table changes are automatically handled using the triggers.
4. After all the data is moved, it drops the triggers and switches the tables by renaming them.

The potential contention point occurs while the data is being transferred to the new table. When the new table is initially created, it's completely empty and therefore can become a locking hot point. The same is true in other kinds of database systems. Because triggers are synchronous, the impact from the hot point can propagate back to your queries.

In multi-master clusters, the impact can be more visible. This visibility is because the new table not only provokes lock contention, but also increases the likelihood of write conflicts. The table initially has very few pages in it, which means that writes are highly localized and therefore prone to conflicts. After the table grows, writes should spread out and write conflicts should no longer be a problem.

You can use the online schema change tool with multi-master clusters. However, it might require more careful testing and its effects on the ongoing workload might be slightly more visible in the first minutes of the operation.

### Using autoincrement columns

Aurora multi-master clusters handle autoincrement columns using the existing configuration parameters `auto_increment_increment` and `auto_increment_offset`. For more information, see the MySQL reference manual.

Parameter values are predetermined and you can't change them. Specifically, the `auto_increment_increment` parameter is hardcoded to 16, which is the maximum number of DB instances in any kind of Aurora cluster.

Due to the hard-coded increment setting, autoincrement values are consumed much more quickly than in single-master clusters. This is true even if a given table is only ever modified by a single DB instance. For best results, always use a `BIGINT` data type instead of `INT` for your autoincrement columns.

In a multi-master cluster, your application logic must be prepared to tolerate autoincrement columns that have the following properties:

- The values are noncontiguous.
- The values might not start from 1 on an empty table.
- The values increase by increments greater than 1.
- The values are consumed significantly more quickly than in a single-master cluster.

The following example shows how the sequence of autoincrement values in a multi-master cluster can be different from what you might expect.

```sql
mysql> create table autoinc (id bigint not null auto_increment, s varchar(64), primary key (id));

mysql> insert into autoinc (s) values ('row 1'), ('row 2'), ('row 3');
Query OK, 3 rows affected (0.02 sec)

mysql> select * from autoinc order by id;
```

786
You can change the `AUTO_INCREMENT` table property. Using a nondefault value only works reliably if that value is larger than any of the primary key values already in the table. You can't use smaller values to fill in an empty interval in the table. If you do, the change takes effect either temporarily or not at all. This behavior is inherited from MySQL 5.6 and is not specific to the Aurora implementation.

**Multi-master clusters feature reference**

Following, you can find a quick reference of the commands, procedures, and status variables specific to Aurora multi-master clusters.

**Using read-after-write**

The read-after-write feature is controlled using the `aurora_mm_session_consistency_level` session variable. The valid values are `INSTANCE_RAW` for local consistency mode (default) and `REGIONAL_RAW` for cluster-wide consistency.

An example follows.

```sql
mysql> select @@aurora_mm_session_consistency_level;
+---------------------------------------+
| @@aurora_mm_session_consistency_level |
+---------------------------------------+
| INSTANCE_RAW                           |
+---------------------------------------+
1 row in set (0.01 sec)
mysql> set session aurora_mm_session_consistency_level = 'REGIONAL_RAW';
Query OK, 0 rows affected (0.00 sec)
mysql> select @@aurora_mm_session_consistency_level;
+---------------------------------------+
| @@aurora_mm_session_consistency_level |
+---------------------------------------+
| REGIONAL_RAW                          |
+---------------------------------------+
1 row in set (0.03 sec)
```

**Checking DB instance read-write mode**

In multi-master clusters, all nodes operate in read/write mode. The `innodb_read_only` variable always returns zero. The following example shows that when you connect to any DB instance in a multi-master cluster, the DB instance reports that it has read/write capability.

```sql
mysql> select @@innodb_read_only;
+--------------------+
| @@innodb_read_only |
+--------------------+
|                  0 |
+--------------------+
```

Bye
Checking the node name and role

You can check the name of the DB instance you’re currently connected to by using the `aurora_server_id` status variable. The following example shows how.

```sql
mysql> select @@aurora_server_id;
+----------------------+
| @@aurora_server_id   |
+----------------------+
| mmr-demo-test-mm-3-1 |
+----------------------+
1 row in set (0.00 sec)
```

To find this information for all the DB instances in a multi-master cluster, see Describing cluster topology (p. 788).

Describing cluster topology

You can describe multi-master cluster topology by selecting from the `information_schema.replica_host_status` table. Multi-master clusters have the following differences from single-master clusters:

- The `has_primary` column identifies the role of the node. For multi-master clusters, this value is true for the DB instance that handles all DDL and DCL statements. Aurora forwards such requests to one of the DB instances in a multi-master cluster.
- The `replica_lag_in_milliseconds` column reports replication lag on all DB instances.
- The `last_reported_status` column reports the status of the DB instance. It can be Online, Recovery, or Offline.

An example follows.

```sql
mysql> select server_id, has_primary, replica_lag_in_milliseconds, last_reported_status
    -> from information_schema.replica_host_status;
+----------------------+-------------+-----------------------------+----------------------+
| server_id            | has_primary | replica_lag_in_milliseconds | last_reported_status |
+----------------------+------------------+------------------------+----------------------+
| mmr-demo-test-mm-3-1 | true        | 37.302             | Online               |
| mmr-demo-test-mm-3-2 | false       | 39.907             | Online               |
+----------------------+-------------+-----------------------------+----------------------+
```

Using instance read-only mode

In Aurora multi-master clusters, you usually issue `SELECT` statements to the specific DB instance that performs write operations on the associated tables. Doing so avoids consistency issues due to replication lag and maximizes reuse for table and index data from the buffer pool.

If you need to run a query-intensive workload across multiple tables, you might designate one of more DB instances within a multi-master cluster as read-only.
To put an entire DB instance into read-only mode at runtime, call the `mysql.rds_set_read_only` stored procedure.

```sql
mysql> select @@read_only;
+-------------+
| @@read_only |
+-------------+
| 0           |
+-------------+
1 row in set (0.00 sec)
mysql> call mysql.rds_set_read_only(1);
Query OK, 0 rows affected (0.00 sec)
mysql> select @@read_only;
+-------------+
| @@read_only |
+-------------+
| 1           |
+-------------+
1 row in set (0.00 sec)
mysql> call mysql.rds_set_read_only(0);
Query OK, 0 rows affected (0.00 sec)
mysql> select @@read_only;
+-------------+
| @@read_only |
+-------------+
| 0           |
+-------------+
1 row in set (0.00 sec)
```

Calling the stored procedure is equivalent to running `SET GLOBAL read_only = 0|1`. That setting is runtime only and doesn’t survive an engine restart. You can permanently set the DB instance to read-only by setting the `read_only` parameter to `true` in the parameter group for your DB instance.

**Performance considerations for Aurora multi-master clusters**

For both single-master and multi-master clusters, the Aurora engine is optimized for OLTP workloads. OLTP applications consist mostly of short-lived transactions with highly selective, random-access queries. You get the most advantage from Aurora with workloads that run many such operations concurrently.

Avoid running all the time at 100 percent utilization. Doing so lets Aurora keep up with internal maintenance work. To learn how to measure how busy a multi-master cluster is and how much maintenance work is needed, see Monitoring an Aurora multi-master cluster (p. 777).

**Topics**

- Query performance for multi-master clusters (p. 789)
- Conflict resolution for multi-master clusters (p. 790)
- Optimizing buffer pool and dictionary cache usage (p. 790)

**Query performance for multi-master clusters**

Multi-master clusters don’t provide dedicated read-only nodes or read-only DNS endpoints, but it’s possible to create groups of read-only DB instances and use them for the intended purpose. For more information, see Using instance read-only mode (p. 788).

You can use the following approaches to optimize query performance for a multi-master cluster:
- Perform `SELECT` statements on the DB instance that handles the shard containing the associated table, database, or other schema objects involved in the query. This technique maximizes reuse of data in the buffer pool. It also avoids the same data being cached on more than one DB instance. For more details about this technique, see Optimizing buffer pool and dictionary cache usage (p. 790).

- If you need read/write workload isolation, designate one or more DB instances as read-only, as described in Using instance read-only mode (p. 788). You can direct read-only sessions to those DB instances by connecting to the corresponding instance endpoints, or by defining a custom endpoint that is associated with all the read-only instances.

- Spread read-only queries across all DB instances. This approach is the least efficient. Use one of the other approaches where practical, especially as you move from the development and test phase towards production.

### Conflict resolution for multi-master clusters

Many best practices for multi-master clusters focus on reducing the chance of write conflicts. Resolving write conflicts involves network overhead. Your applications must also handle error conditions and retry transactions. Wherever possible, try to minimize these unwanted consequences:

- Wherever practical, make all changes to a particular table and its associated indexes using the same DB instance. If only one DB instance ever modifies a data page, changing that page cannot trigger any write conflicts. This access pattern is common in sharded or multitenant database deployments. Thus, it's relatively easy to switch such deployments to use multi-master clusters.

- A multi-master cluster doesn’t have a reader endpoint. The reader endpoint load-balances incoming connections, freeing you from knowing which DB instance is handling a particular connection. In a multi-master cluster, managing connections involves being aware which DB instance is used for each connection. That way, modifications to a particular database or table can always be routed to the same DB instance.

- A write conflict for a small amount of data (one 16-KB page) can trigger a substantial amount of work to roll back the entire transaction. Thus, ideally you keep the transactions for a multi-master cluster relatively brief and small. This best practice for OLTP applications is especially important for Aurora multi-master clusters.

Conflicts are detected at page level. A conflict could occur because proposed changes from different DB instances modify different rows within the page. All page changes introduced in the system are subject to conflict detection. This rule applies regardless of whether the source is a user transaction or a server background process. It also applies whether the data page is from a table, secondary index, undo space, and so on.

You can divide the write operations so that each DB instance handles all write operations for a set of schema objects. In this case, all the changes to each data page are made by one specific instance.

### Optimizing buffer pool and dictionary cache usage

Each DB instance in a multi-master cluster maintains separate in-memory buffers and caches such as the buffer pool, table handler cache, and table dictionary cache. For each DB instance, the contents and amount of turnover for the buffers and caches depends on the SQL statements processed by that instance.

Using memory efficiently can help the performance of multi-master clusters and reduce I/O cost. Use a sharded design to physically separate the data and write to each shard from a particular DB instance. Doing so makes the most efficient use of the buffer cache on each DB instance. Try to assign `SELECT` statements for a table to the same DB instance that performs write operations for that table. Doing so helps those queries to reuse the cached data on that DB instance. If you have a large number of tables or partitions, this technique also reduces the number of unique table handlers and dictionary objects held in memory by each DB instance.
Approaches to Aurora multi-master clusters

In the following sections, you can find approaches to take for particular deployments that are suitable for multi-master clusters. These approaches involve ways to divide the workload so that the DB instances perform write operations for portions of the data that don't overlap. Doing so minimizes the chances of write conflicts. Write conflicts are the main focus of performance tuning and troubleshooting for a multi-master cluster.

Topics
- Using a multi-master cluster for a sharded database (p. 791)
- Using a multi-master cluster without sharding (p. 791)
- Using a multi-master cluster as an active standby (p. 792)

Using a multi-master cluster for a sharded database

Sharding is a popular type of schema design that works well with Aurora multi-master clusters. In a sharded architecture, each DB instance is assigned to update a specific group of schema objects. That way, multiple DB instances can write to the same shared storage volume without conflicts from concurrent changes. Each DB instance can handle write operations for multiple shards. You can change the mapping of DB instances to shards at any time by updating your application configuration. You don't need to reorganize your database storage or reconfigure DB instances when you do so.

Applications that use a sharded schema design are good candidates to use with Aurora multi-master clusters. The way the data is physically divided in a sharded system helps to avoid write conflicts. You map each shard to a schema object such as a partition, a table, or a database. Your application directs all write operations for a particular shard to the appropriate DB instance.

Bring-your-own-shard (BYOS) describes a use case where you already have a sharded/partitioned database and an application capable of accessing it. The shards are already physically separated. Thus, you can easily move the workload to Aurora multi-master clusters without changing your schema design. The same simple migration path applies to multitenant databases, where each tenant uses a dedicated table, a set of tables, or an entire database.

You map shards or tenants to DB instances in a one-to-one or many-to-one fashion. Each DB instance handles one or more shards. The sharded design primarily applies to write operations. You can issue SELECT queries for any shard from any DB instance with equivalent performance.

Suppose you used a multi-master cluster for a sharded gaming application. You might distribute the work so that database updates are performed by specific DB instances, depending on the player's user name. Your application handles the logic of mapping each player to the appropriate DB instance and connecting to the endpoint for that instance. Each DB instance can handle write operations for many different shards. You can submit queries to any DB instance, because conflicts can only arise during write operations. You might designate one DB instance to perform all SELECT queries to minimize the overhead on the DB instances that perform write operations.

Suppose that as time goes on, one of the shards becomes much more active. To rebalance the workload, you can switch which DB instance is responsible for that shard. In a non-Aurora system, you might have to physically move the data to a different server. With an Aurora multi-master cluster, you can reshard like this by directing all write operations for the shard to some other DB instance that has unused compute capacity. The Aurora shared storage model avoids the need to physically reorganize the data.

Using a multi-master cluster without sharding

If your schema design doesn't subdivide the data into physically separate containers such as databases, tables, or partitions, you can still divide write operations such as DML statements among the DB instances in a multi-master cluster.
You might see some performance overhead, and your application might have to deal with occasional transaction rollbacks when write conflicts are treated as deadlock conditions. Write conflicts are more likely during write operations for small tables. If a table contains few data pages, rows from different parts of the primary key range might be in the same data page. This overlap might lead to write conflicts if those rows are changed simultaneously by different DB instances.

You should also minimize the number of secondary indexes in this case. When you make a change to indexed columns in a table, Aurora makes corresponding changes in the associated secondary indexes. A change to an index could cause a write conflict because the order and grouping of rows is different between a secondary index and the associated table.

Because you might still experience some write conflicts when using this technique, Amazon recommends using a different approach if practical. See if you can use an alternative database design that subdivides the data into different schema objects.

**Using a multi-master cluster as an active standby**

An *active standby* is a DB instance that is kept synchronized with another DB instance, and is ready to take over for it very quickly. This configuration helps with high availability in situations where a single DB instance can handle the full workload.

You can use multi-master clusters in an active standby configuration by directing all traffic, both read/write and read-only, to a single DB instance. If that DB instance becomes unavailable, your application must detect the problem and switch all connections to a different DB instance. In this case, Aurora doesn’t perform any failover because the other DB instance is already available to accept read/write connections. By only writing to a single DB instance at any one time, you avoid write conflicts. Thus, you don’t need to have a sharded database schema to use multi-master clusters in this way.

**Tip**

If your application can tolerate a brief pause, you can wait several seconds after a DB instance becomes unavailable before redirecting write traffic to another instance. When an instance becomes unavailable because of a restart, it becomes available again after approximately 10–20 seconds. If the instance can’t restart quickly, Aurora might initiate recovery for that instance. When an instance is shut down, it performs some additional cleanup activities as part of the shutdown. If you begin writing to a different instance while the instance is restarting, undergoing recovery, or being shut down, you can encounter write conflicts. The conflicts can occur between SQL statements on the new instance, and recovery operations such as rollback and purge on the instance that was restarted or shut down.

**Integrating Amazon Aurora MySQL with other AWS services**

Amazon Aurora MySQL integrates with other AWS services so that you can extend your Aurora MySQL DB cluster to use additional capabilities in the AWS Cloud. Your Aurora MySQL DB cluster can use AWS services to do the following:

- Synchronously or asynchronously invoke an AWS Lambda function using the native functions `lambda_sync` or `lambda_async`. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Load data from text or XML files stored in an Amazon Simple Storage Service (Amazon S3) bucket into your DB cluster using the `LOAD DATA FROM S3` or `LOAD XML FROM S3` command. For more information, see Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804).
- Save data to text files stored in an Amazon S3 bucket from your DB cluster using the `SELECT INTO OUTFILE S3` command. For more information, see Saving data from an Amazon Aurora MySQL DB cluster into text files in an Amazon S3 bucket (p. 812).
Automatically add or remove Aurora Replicas with Application Auto Scaling. For more information, see Using Amazon Aurora Auto Scaling with Aurora replicas (p. 372).

Perform sentiment analysis with Amazon Comprehend, or a wide variety of machine learning algorithms with SageMaker. For more information, see Using machine learning (ML) capabilities with Amazon Aurora (p. 387).

Aurora secures the ability to access other AWS services by using AWS Identity and Access Management (IAM). You grant permission to access other AWS services by creating an IAM role with the necessary permissions, and then associating the role with your DB cluster. For details and instructions on how to permit your Aurora MySQL DB cluster to access other AWS services on your behalf, see Authorizing Amazon Aurora MySQL to access other AWS services on your behalf (p. 793).

Authorizing Amazon Aurora MySQL to access other AWS services on your behalf

Note
Integration with other AWS services is available for Amazon Aurora MySQL version 1.8 and later. Some integration features are only available for later versions of Aurora MySQL. For more information on Aurora versions, see Database engine updates for Amazon Aurora MySQL (p. 874).

For your Aurora MySQL DB cluster to access other services on your behalf, create and configure an AWS Identity and Access Management (IAM) role. This role authorizes database users in your DB cluster to access other AWS services. For more information, see Setting up IAM roles to access AWS services (p. 793).

You must also configure your Aurora DB cluster to allow outbound connections to the target AWS service. For more information, see Enabling network communication from Amazon Aurora MySQL to other AWS services (p. 803).

If you do so, your database users can perform these actions using other AWS services:

- Synchronously or asynchronously invoke an AWS Lambda function using the native functions `lambda_sync` or `lambda_async`. Or, asynchronously invoke an AWS Lambda function using the `mysql.lambda_async` procedure. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).

- Load data from text or XML files stored in an Amazon S3 bucket into your DB cluster by using the `LOAD DATA FROM S3` or `LOAD XML FROM S3` statement. For more information, see Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804).

- Save data from your DB cluster into text files stored in an Amazon S3 bucket by using the `SELECT INTO OUTFILE S3` statement. For more information, see Saving data from an Amazon Aurora MySQL DB cluster into text files in an Amazon S3 bucket (p. 812).

- Export log data to Amazon CloudWatch Logs MySQL. For more information, see Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs (p. 824).

- Automatically add or remove Aurora Replicas with Application Auto Scaling. For more information, see Using Amazon Aurora Auto Scaling with Aurora replicas (p. 372).

Setting up IAM roles to access AWS services

To permit your Aurora DB cluster to access another AWS service, do the following:

1. Create an IAM policy that grants permission to the AWS service. For more information, see:
   - Creating an IAM policy to access Amazon S3 resources (p. 794)
• Creating an IAM policy to access AWS Lambda resources (p. 796)
• Creating an IAM policy to access CloudWatch Logs resources (p. 797)
• Creating an IAM policy to access AWS KMS resources (p. 798)

2. Create an IAM role and attach the policy that you created. For more information, see Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).

3. Associate that IAM role with your Aurora DB cluster. For more information, see Associating an IAM role with an Amazon Aurora MySQL DB cluster (p. 800).

Creating an IAM policy to access Amazon S3 resources

Aurora can access Amazon S3 resources to either load data to or save data from an Aurora DB cluster. However, you must first create an IAM policy that provides the bucket and object permissions that allow Aurora to access Amazon S3.

The following table lists the Aurora features that can access an Amazon S3 bucket on your behalf, and the minimum required bucket and object permissions required by each feature.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Bucket permissions</th>
<th>Object permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOAD DATA FROM S3</td>
<td>ListBucket</td>
<td>GetObject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetObjectVersion</td>
</tr>
<tr>
<td>LOAD XML FROM S3</td>
<td>ListBucket</td>
<td>GetObject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetObjectVersion</td>
</tr>
<tr>
<td>SELECT INTO OUTFILE S3</td>
<td>ListBucket</td>
<td>AbortMultipartUpload</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteObject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetObject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListMultipartUploadParts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PutObject</td>
</tr>
</tbody>
</table>

The following policy adds the permissions that might be required by Aurora to access an Amazon S3 bucket on your behalf.

```json
{
   "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:::example-bucket/*",
            "arn:aws:s3:::example-bucket/*",
         ]
      }
   ]
}
```
Amazon Aurora User Guide for Aurora
Authorizing Aurora MySQL to access AWS services

```
"arn:aws:s3:::example-bucket"
```  

Note
Based on your use case, you might not need to add all of the permissions in the sample policy. Also, other permissions might be required. For example, if your Amazon S3 bucket is encrypted, you need to add kms:Decrypt permissions.

You can use the following steps to create an IAM policy that provides the minimum required permissions for Aurora to access an Amazon S3 bucket on your behalf. To allow Aurora to access all of your Amazon S3 buckets, you can skip these steps and use either the AmazonS3ReadOnlyAccess or AmazonS3FullAccess predefined IAM policy instead of creating your own.

To create an IAM policy to grant access to your Amazon S3 resources

1. Open the IAM Management Console.
2. In the navigation pane, choose Policies.
3. Choose Create policy.
4. On the Visual editor tab, choose Choose a service, and then choose S3.
5. For Actions, choose Expand all, and then choose the bucket permissions and object permissions needed for the IAM policy.

Object permissions are permissions for object operations in Amazon S3, and need to be granted for objects in a bucket, not the bucket itself. For more information about permissions for object operations in Amazon S3, see Permissions for object operations.

6. Choose Resources, and choose Add ARN for bucket.
7. In the Add ARN(s) dialog box, provide the details about your resource, and choose Add.

Specify the Amazon S3 bucket to allow access to. For instance, if you want to allow Aurora to access the Amazon S3 bucket named example-bucket, then set the Amazon Resource Name (ARN) value to arn:aws:s3:::example-bucket.

8. If the object resource is listed, choose Add ARN for object.
9. In the Add ARN(s) dialog box, provide the details about your resource.

For the Amazon S3 bucket, specify the Amazon S3 bucket to allow access to. For the object, you can choose Any to grant permissions to any object in the bucket.

Note
You can set Amazon Resource Name (ARN) to a more specific ARN value in order to allow Aurora to access only specific files or folders in an Amazon S3 bucket. For more information about how to define an access policy for Amazon S3, see Managing access permissions to your Amazon S3 resources.

10. (Optional) Choose Add ARN for bucket to add another Amazon S3 bucket to the policy, and repeat the previous steps for the bucket.

Note
You can repeat this to add corresponding bucket permission statements to your policy for each Amazon S3 bucket that you want Aurora to access. Optionally, you can also grant access to all buckets and objects in Amazon S3.

12. For Name, enter a name for your IAM policy, for example AllowAuroraToExampleBucket. You use this name when you create an IAM role to associate with your Aurora DB cluster. You can also add an optional Description value.

795
13. Choose **Create policy**.
14. Complete the steps in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).

### Creating an IAM policy to access AWS Lambda resources

You can create an IAM policy that provides the minimum required permissions for Aurora to invoke an AWS Lambda function on your behalf.

The following policy adds the permissions required by Aurora to invoke an AWS Lambda function on your behalf.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAuroraToExampleFunction",
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:<region>:<123456789012>:function:<example_function>"
    }
  ]
}
```

You can use the following steps to create an IAM policy that provides the minimum required permissions for Aurora to invoke an AWS Lambda function on your behalf. To allow Aurora to invoke all of your AWS Lambda functions, you can skip these steps and use the predefined **AWSLambdaRole** policy instead of creating your own.

**To create an IAM policy to grant invoke to your AWS Lambda functions**

1. Open the IAM console.
2. In the navigation pane, choose Policies.
3. Choose **Create policy**.
4. On the Visual editor tab, choose **Choose a service**, and then choose Lambda.
5. For Actions, choose **Expand all**, and then choose the AWS Lambda permissions needed for the IAM policy.
   
   Ensure that InvokeFunction is selected. It is the minimum required permission to enable Amazon Aurora to invoke an AWS Lambda function.
6. Choose Resources and choose **Add ARN for function**.
7. In the **Add ARN(s)** dialog box, provide the details about your resource.

   Specify the Lambda function to allow access to. For instance, if you want to allow Aurora to access a Lambda function named example_function, then set the ARN value to `arn:aws:lambda:::function:example_function`.

   For more information on how to define an access policy for AWS Lambda, see Authentication and access control for AWS Lambda.
8. Optionally, choose **Add additional permissions** to add another AWS Lambda function to the policy, and repeat the previous steps for the function.

**Note**

You can repeat this to add corresponding function permission statements to your policy for each AWS Lambda function that you want Aurora to access.

10. Set Name to a name for your IAM policy, for example AllowAuroraToExampleFunction. You use this name when you create an IAM role to associate with your Aurora DB cluster. You can also add an optional Description value.

11. Choose Create policy.

12. Complete the steps in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).

Creating an IAM policy to access CloudWatch Logs resources

Aurora can access CloudWatch Logs to export audit log data from an Aurora DB cluster. However, you must first create an IAM policy that provides the log group and log stream permissions that allow Aurora to access CloudWatch Logs.

The following policy adds the permissions required by Aurora to access Amazon CloudWatch Logs on your behalf, and the minimum required permissions to create log groups and export data.

```json
{
   "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/*"
      }
   ]
}
```

You can modify the ARNs in the policy to restrict access to a specific AWS Region and account.

You can use the following steps to create an IAM policy that provides the minimum required permissions for Aurora to access CloudWatch Logs on your behalf. To allow Aurora full access to CloudWatch Logs, you can skip these steps and use the CloudWatchLogsFullAccess predefined IAM policy instead of creating your own. For more information, see Using identity-based policies (IAM policies) for CloudWatch Logs in the Amazon CloudWatch User Guide.

To create an IAM policy to grant access to your CloudWatch Logs resources

1. Open the IAM console.
2. In the navigation pane, choose Policies.
3. Choose Create policy.
4. On the Visual editor tab, choose Choose a service, and then choose CloudWatch Logs.
5. For **Actions**, choose **Expand all** (on the right), and then choose the Amazon CloudWatch Logs permissions needed for the IAM policy.

   Ensure that the following permissions are selected:
   - CreateLogGroup
   - CreateLogStream
   - DescribeLogStreams
   - GetLogEvents
   - PutLogEvents
   - PutRetentionPolicy

6. Choose **Resources** and choose **Add ARN** for log-group.

7. In the **Add ARN(s)** dialog box, enter the following values:
   - **Region** – An AWS Region or *
   - **Account** – An account number or *
   - **Log Group Name** – `/aws/rds/*`

8. In the **Add ARN(s)** dialog box, choose **Add**.

9. Choose **Add ARN** for log-stream.

10. In the **Add ARN(s)** dialog box, enter the following values:
   - **Region** – An AWS Region or *
   - **Account** – An account number or *
   - **Log Group Name** – `/aws/rds/*`
   - **Log Stream Name** – *

11. In the **Add ARN(s)** dialog box, choose **Add**.

12. Choose **Review policy**.

13. Set **Name** to a name for your IAM policy, for example **AmazonRDSCloudWatchLogs**. You use this name when you create an IAM role to associate with your Aurora DB cluster. You can also add an optional **Description** value.

14. Choose **Create policy**.

15. Complete the steps in **Creating an IAM role to allow Amazon Aurora to access AWS services** (p. 799).

### Creating an IAM policy to access AWS KMS resources

Aurora can access AWS Key Management Service customer master keys (CMKs) used for encrypting their database backups. However, you must first create an IAM policy that provides the permissions that allow Aurora to access AWS KMS CMKs.

The following policy adds the permissions required by Aurora to access AWS KMS CMKs on your behalf.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:<region>:<123456789012>:key/<key-ID>"
        }
    ]
}
```
You can use the following steps to create an IAM policy that provides the minimum required permissions for Aurora to access AWS KMS CMKs on your behalf.

**To create an IAM policy to grant access to your AWS KMS CMKs**

1. Open the IAM console.
2. In the navigation pane, choose Policies.
3. Choose Create policy.
4. On the Visual editor tab, choose Choose a service, and then choose KMS.
5. For Actions, choose Write, and then choose Decrypt.
6. Choose Resources, and choose Add ARN.
7. In the Add ARN(s) dialog box, enter the following values:
   - Region – Type the AWS Region, such as us-west-2.
   - Account – Type the user account number.
   - Log Stream Name – Type the AWS KMS key identifier.
8. In the Add ARN(s) dialog box, choose Add.
10. Set Name to a name for your IAM policy, for example AmazonRDSKMSKey. You use this name when you create an IAM role to associate with your Aurora DB cluster. You can also add an optional Description value.
11. Choose Create policy.
12. Complete the steps in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).

**Creating an IAM role to allow Amazon Aurora to access AWS services**

After creating an IAM policy to allow Aurora to access AWS resources, you must create an IAM role and attach the IAM policy to the new IAM role.

To create an IAM role to permit your Amazon RDS cluster to communicate with other AWS services on your behalf, take the following steps.

**To create an IAM role to allow Amazon RDS to access AWS services**

1. Open the IAM console.
2. In the navigation pane, choose Roles.
3. Choose Create role.
4. Under AWS service, choose RDS.
5. Under Select your use case, choose RDS – Add Role to Database.
6. Choose Next: Permissions.
7. On the Attach permissions policies page, enter the name of your policy in the Search field.
8. When it appears in the list, select the policy that you defined earlier using the instructions in one of the following sections:
   - Creating an IAM policy to access Amazon S3 resources (p. 794)
   - Creating an IAM policy to access AWS Lambda resources (p. 796)
   - Creating an IAM policy to access CloudWatch Logs resources (p. 797)
   - Creating an IAM policy to access AWS KMS resources (p. 798)
9. Choose **Next: Tags**, and then choose **Next: Review**.
10. In **Role name**, enter a name for your IAM role, for example **RDSLoadFromS3**. You can also add an optional **Role description** value.
11. Choose **Create Role**.
12. Complete the steps in **Associating an IAM role with an Amazon Aurora MySQL DB cluster (p. 800)**.

**Associating an IAM role with an Amazon Aurora MySQL DB cluster**

To permit database users in an Amazon Aurora DB cluster to access other AWS services, you associate the role that you created in **Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799)** with that DB cluster.

**Note**

You can't associate an IAM role with an Aurora Serverless DB cluster. For more information, see **Using Amazon Aurora Serverless v1 (p. 134)**.

To associate an IAM role with a DB cluster you do two things:

- Add the role to the list of associated roles for a DB cluster by using the RDS console, the **add-role-to-db-cluster** AWS CLI command, or the **AddRoleToDBCluster** RDS API operation.

You can add a maximum of five IAM roles for each Aurora DB cluster.

- Set the cluster-level parameter for the related AWS service to the ARN for the associated IAM role.

The following table describes the cluster-level parameter names for the IAM roles used to access other AWS services.

<table>
<thead>
<tr>
<th>Cluster-level parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aws_default_lambda_role</td>
<td>Used when invoking a Lambda function from your DB cluster.</td>
</tr>
<tr>
<td>aws_default_logs_role</td>
<td>This parameter is no longer required for exporting log data from your DB cluster to Amazon CloudWatch Logs. Aurora MySQL now uses a service-linked role for the required permissions. For more information about service-linked roles, see <strong>Using service-linked roles for Amazon Aurora (p. 1277)</strong>.</td>
</tr>
<tr>
<td>aws_default_s3_role</td>
<td>Used when invoking the LOAD DATA FROM S3, LOAD XML FROM S3, or SELECT INTO OUTFILE S3 statement from your DB cluster. The IAM role specified in this parameter is used only if an IAM role isn't specified for aurora_load_from_s3_role or aurora_select_into_s3_role for the appropriate statement. For earlier versions of Aurora, the IAM role specified for this parameter is always used.</td>
</tr>
<tr>
<td>aurora_load_from_s3_role</td>
<td>Used when invoking the LOAD DATA FROM S3 or LOAD XML FROM S3 statement from your DB cluster. If an IAM role is not specified</td>
</tr>
<tr>
<td>Cluster-level parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>for this parameter, the IAM role specified in aws_default_s3_role is used. For earlier versions of Aurora, this parameter is not available.</td>
</tr>
<tr>
<td>aurora_select_into_s3_role</td>
<td>Used when invoking the SELECT INTO OUTFILE S3 statement from your DB cluster. If an IAM role is not specified for this parameter, the IAM role specified in aws_default_s3_role is used. For earlier versions of Aurora, this parameter is not available.</td>
</tr>
</tbody>
</table>

To associate an IAM role to permit your Amazon RDS cluster to communicate with other AWS services on your behalf, take the following steps.

**To associate an IAM role with an Aurora DB cluster using the console**

2. Choose **Databases**.
3. Choose the name of the Aurora DB cluster that you want to associate an IAM role with to show its details.
4. On the **Connectivity & security** tab, in the **Manage IAM roles** section, choose the role to add under **Add IAM roles to this cluster**.

5. Choose **Add role**.
6. (Optional) To stop associating an IAM role with a DB cluster and remove the related permission, choose the role and choose **Delete**.
7. In the RDS console, choose **Parameter groups** in the navigation pane.
8. If you are already using a custom DB parameter group, you can select that group to use instead of creating a new DB cluster parameter group. If you are using the default DB cluster parameter group, create a new DB cluster parameter group, as described in the following steps:
   a. Choose **Create parameter group**.
b. For **Parameter group family**, choose `aurora5.6` for an Aurora MySQL 5.6-compatible DB cluster, or choose `aurora-mysql5.7` for an Aurora MySQL 5.7-compatible DB cluster.

c. For **Type**, choose **DB Cluster Parameter Group**.

d. For **Group name**, type the name of your new DB cluster parameter group.

e. For **Description**, type a description for your new DB cluster parameter group.

f. Choose **Create**.

9. On the **Parameter groups** page, select your DB cluster parameter group and choose **Edit** for **Parameter group actions**.

10. Set the appropriate cluster-level parameters to the related IAM role ARN values. For example, you can set just the `aws_default_s3_role` parameter to `arn:aws:iam::123456789012:role/AllowAuroraS3Role`.

11. Choose **Save changes**.

12. To change the DB cluster parameter group for your DB cluster, complete the following steps:

   a. Choose **Databases**, and then choose your Aurora DB cluster.

   b. Choose **Modify**.

   c. Scroll to **Database options** and set **DB cluster parameter group** to the DB cluster parameter group.

   d. Choose **Continue**.

   e. Verify your changes and then choose **Apply immediately**.

   f. Choose **Modify cluster**.

   g. Choose **Databases**, and then choose the primary instance for your DB cluster.

   h. For **Actions**, choose **Reboot**.

   When the instance has rebooted, your IAM role is associated with your DB cluster.

For more information about cluster parameter groups, see [Aurora MySQL parameters](p. 848).
To associate an IAM role with a DB cluster by using the AWS CLI

1. Call the add-role-to-db-cluster command from the AWS CLI to add the ARNs for your IAM roles to the DB cluster, as shown following.

   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. If you are using the default DB cluster parameter group, create a new DB cluster parameter group. If you are already using a custom DB parameter group, you can use that group instead of creating a new DB cluster parameter group.

   To create a new DB cluster parameter group, call the create-db-cluster-parameter-group command from the AWS CLI, as shown following.

   PROMPT> aws rds create-db-cluster-parameter-group --db-cluster-parameter-group-name AllowAWSAccess --db-parameter-group-family aurora5.6 --description "Allow access to Amazon S3 and AWS Lambda"

   For an Aurora MySQL 5.7-compatible DB cluster, specify aurora-mysql5.7 for --db-parameter-group-family.

3. Set the appropriate cluster-level parameter or parameters and the related IAM role ARN values in your DB cluster parameter group, as shown following.

   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. Modify the DB cluster to use the new DB cluster parameter group and then reboot the cluster, as shown following.

   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

   When the instance has rebooted, your IAM roles are associated with your DB cluster.

   For more information about cluster parameter groups, see Aurora MySQL parameters (p. 848).

Enabling network communication from Amazon Aurora MySQL to other AWS services

To use certain other AWS services with Amazon Aurora, the network configuration of your Aurora DB cluster must allow outbound connections to endpoints for those services. The following operations require this network configuration.

- Invoking AWS Lambda functions. To learn about this feature, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
• Accessing files from Amazon S3. To learn about this feature, see Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804) and Saving data from an Amazon Aurora MySQL DB cluster into text files in an Amazon S3 bucket (p. 812).

• Accessing AWS KMS endpoints. AWS KMS access is required to use database activity streams with Aurora MySQL. To learn about this feature, see Using Database Activity Streams with Amazon Aurora (p. 565).

Aurora returns the following error messages if it can't connect to a service endpoint.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR 1871 (HY000)</td>
<td>S3 API returned error: Network Connection</td>
</tr>
<tr>
<td>ERROR 1873 (HY000)</td>
<td>Lambda API returned error: Network Connection. Unable to connect to endpoint</td>
</tr>
<tr>
<td>ERROR 1815 (HY000)</td>
<td>Internal error: Unable to initialize S3Stream</td>
</tr>
</tbody>
</table>

For database activity streams using Aurora MySQL, the activity stream stops functioning if the DB cluster can't access the AWS KMS endpoint. Aurora notifies you about this issue using RDS Events.

If you encounter these messages while using the corresponding AWS services, check if your Aurora DB cluster is public or private. If your Aurora DB cluster is private, you must configure it to enable connections.

For an Aurora DB cluster to be public, it must be marked as publicly accessible. If you look at the details for the DB cluster in the AWS Management Console, Publicly Accessible is Yes if this is the case. The DB cluster must also be in an Amazon VPC public subnet. For more information about publicly accessible DB instances, see Working with a DB instance in a VPC (p. 1291). For more information about public Amazon VPC subnets, see Your VPC and subnets.

If your Aurora DB cluster isn't publicly accessible and in a VPC public subnet, it is private. You might have a DB cluster that is private and want to use one of the features that requires this network configuration. If so, configure the cluster so that it can connect to Internet addresses through Network Address Translation (NAT). As an alternative for Amazon S3, you can instead configure the VPC to have a VPC endpoint for Amazon S3 associated with the DB cluster's route table. For more information about configuring NAT in your VPC, see NAT gateways. For more information about configuring VPC endpoints, see VPC endpoints.

Related topics
• Integrating Aurora with other AWS services (p. 371)
• Managing an Amazon Aurora DB cluster (p. 322)

Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket

You can use the LOAD DATA FROM S3 or LOAD XML FROM S3 statement to load data from files stored in an Amazon S3 bucket.

Note
Loading data into a table from text files in an Amazon S3 bucket is available for Amazon Aurora MySQL version 1.8 and later. For more information about Aurora MySQL versions, see Database engine updates for Amazon Aurora MySQL (p. 874).
Giving Aurora access to Amazon S3

Before you can load data from an Amazon S3 bucket, you must first give your Aurora MySQL DB cluster permission to access Amazon S3.

To give Aurora MySQL access to Amazon S3

1. Create an AWS Identity and Access Management (IAM) policy that provides the bucket and object permissions that allow your Aurora MySQL DB cluster to access Amazon S3. For instructions, see Creating an IAM policy to access Amazon S3 resources (p. 794).

2. Create an IAM role, and attach the IAM policy you created in Creating an IAM policy to access Amazon S3 resources (p. 794) to the new IAM role. For instructions, see Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).

3. Make sure the DB cluster is using a custom DB cluster parameter group.

   For more information about creating a custom DB cluster parameter group, see Creating a DB cluster parameter group (p. 302).

4. Set either the aurora_load_from_s3_role or aws_default_s3_role DB cluster parameter to the Amazon Resource Name (ARN) of the new IAM role. If an IAM role isn't specified for aurora_load_from_s3_role, Aurora uses the IAM role specified in aws_default_s3_role.

   If the cluster is part of an Aurora global database, set this parameter for each Aurora cluster in the global database. Although only the primary cluster in an Aurora global database can load data, another cluster might be promoted by the failover mechanism and become the primary cluster.

   For more information about DB cluster parameters, see Amazon Aurora DB cluster and DB instance parameters (p. 300).

5. To permit database users in an Aurora MySQL DB cluster to access Amazon S3, associate the role that you created in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799) with the DB cluster. For an Aurora global database, associate the role with each Aurora cluster in the global database. For information about associating an IAM role with a DB cluster, see Associating an IAM role with an Amazon Aurora MySQL DB cluster (p. 800).

6. Configure your Aurora MySQL DB cluster to allow outbound connections to Amazon S3. For instructions, see Enabling network communication from Amazon Aurora MySQL to other AWS services (p. 803).

   For an Aurora global database, enable outbound connections for each Aurora cluster in the global database.

Granting privileges to load data in Amazon Aurora MySQL

The database user that issues the LOAD DATA FROM S3 or LOAD XML FROM S3 statement must be granted the LOAD FROM S3 privilege to issue either statement. The master user name for a DB cluster is granted the LOAD FROM S3 privilege by default. You can grant the privilege to another user by using the following statement.

```
GRANT LOAD FROM S3 ON *.* TO 'user'@'domain-or-ip-address'
```

The LOAD FROM S3 privilege is specific to Amazon Aurora and is not available for MySQL databases or RDS MySQL DB instances. If you have set up replication between an Aurora DB cluster as the replication master and a MySQL database as the replication client, then the GRANT LOAD FROM S3 statement causes replication to stop with an error. You can safely skip the error to resume replication. To skip the
error on an RDS MySQL DB instance, use the `mysql_rds_skip_repl_error` procedure. To skip the error on an external MySQL database, use the `SET GLOBAL sql_slave_skip_counter` statement.

## Specifying a path to an Amazon S3 bucket

The syntax for specifying a path to files stored on an Amazon S3 bucket is as follows.

```
s3-region://bucket-name/file-name-or-prefix
```

The path includes the following values:

- **region** (optional) – The AWS Region that contains the Amazon S3 bucket to load from. This value is optional. If you don’t specify a `region` value, then Aurora loads your file from Amazon S3 in the same region as your DB cluster.
- **bucket-name** – The name of the Amazon S3 bucket that contains the data to load. Object prefixes that identify a virtual folder path are supported.
- **file-name-or-prefix** – The name of the Amazon S3 text file or XML file, or a prefix that identifies one or more text or XML files to load. You can also specify a manifest file that identifies one or more text files to load. For more information about using a manifest file to load text files from Amazon S3, see Using a manifest to specify data files to load (p. 807).

## LOAD DATA FROM S3

You can use the `LOAD DATA FROM S3` statement to load data from any text file format that is supported by the MySQL `LOAD DATA INFILE` statement, such as text data that is comma-delimited. Compressed files are not supported.

### 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']
]
[STARTING BY 'string']
[TERMINATED BY 'string']

[IGNORE number {LINES | ROWS}]
[(col_name_or_user_var,...)]
[SET col_name = expr,...]
```

### Parameters

Following, you can find a list of the required and optional parameters used by the `LOAD DATA FROM S3` statement. You can find more details about some of these parameters in `LOAD DATA INFILE` syntax in the MySQL documentation.

- **FILE | PREFIX | MANIFEST** – Identifies whether to load the data from a single file, from all files that match a given prefix, or from all files in a specified manifest. `FILE` is the default.
- **S3-URI** – Specifies the URI for a text or manifest file to load, or an Amazon S3 prefix to use. Specify the URI using the syntax described in Specifying a path to an Amazon S3 bucket (p. 806).
• REPLACE | IGNORE – Determines what action to take if an input row as the same unique key values as an existing row in the database table.
  • Specify REPLACE if you want the input row to replace the existing row in the table.
  • Specify IGNORE if you want to discard the input row.
• INTO TABLE – Identifies the name of the database table to load the input rows into.
• PARTITION – Requires that all input rows be inserted into the partitions identified by the specified list of comma-separated partition names. If an input row cannot be inserted into one of the specified partitions, then the statement fails and an error is returned.
• CHARACTER SET – Identifies the character set of the data in the input file.
• FIELDS | COLUMNS – Identifies how the fields or columns in the input file are delimited. Fields are tab-delimited by default.
• LINES – Identifies how the lines in the input file are delimited. Lines are delimited by a newline character ('\n') by default.
• IGNORE number LINES | ROWS – Specifies to ignore a certain number of lines or rows at the start of the input file. For example, you can use IGNORE 1 LINES to skip over an initial header line containing column names, or IGNORE 2 ROWS to skip over the first two rows of data in the input file. If you also use PREFIX, IGNORE skips a certain number of lines or rows at the start of the first input file.
• col_name_or_user_var, ... – Specifies a comma-separated list of one or more column names or user variables that identify which columns to load by name. The name of a user variable used for this purpose must match the name of an element from the text file, prefixed with @. You can employ user variables to store the corresponding field values for subsequent reuse.

For example, the following statement loads the first column from the input file into the first column of table1, and sets the value of the table_column2 column in table1 to the input value of the second column divided by 100.

```sql
LOAD DATA FROM S3 's3://mybucket/data.txt'
  INTO TABLE table1
    (column1, @var1)
  SET table_column2 = @var1/100;
```

• SET – Specifies a comma-separated list of assignment operations that set the values of columns in the table to values not included in the input file.

For example, the following statement sets the first two columns of table1 to the values in the first two columns from the input file, and then sets the value of the column3 in table1 to the current time stamp.

```sql
LOAD DATA FROM S3 's3://mybucket/data.txt'
  INTO TABLE table1
    (column1, column2)
  SET column3 = CURRENT_TIMESTAMP;
```

You can use subqueries in the right side of SET assignments. For a subquery that returns a value to be assigned to a column, you can use only a scalar subquery. Also, you cannot use a subquery to select from the table that is being loaded.

You cannot use the LOCAL keyword of the LOAD DATA FROM S3 statement if you are loading data from an Amazon S3 bucket.

**Using a manifest to specify data files to load**

You can use the LOAD DATA FROM S3 statement with the MANIFEST keyword to specify a manifest file in JSON format that lists the text files to be loaded into a table in your DB cluster. You must be using Aurora 1.11 or greater to use the MANIFEST keyword with the LOAD DATA FROM S3 statement.
The following JSON schema describes the format and content of a manifest file.

```
{
   "$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"
   }
```

Each `url` in the manifest must specify a URL with the bucket name and full object path for the file, not just a prefix. You can use a manifest to load files from different buckets, different regions, or files that do not share the same prefix. If a region is not specified in the URL, the region of the target Aurora DB cluster is used. The following example shows a manifest file that loads four files from different buckets.

```
{
   "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"
      }
   ]
```
The optional `mandatory` flag specifies whether `LOAD DATA FROM S3` should return an error if the file is not found. The `mandatory` flag defaults to `false`. Regardless of how `mandatory` is set, `LOAD DATA FROM S3` terminates if no files are found.

Manifest files can have any extension. The following example runs the `LOAD DATA FROM S3` statement with the manifest in the previous example, which is named `customer.manifest`.

```sql
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);
```

After the statement completes, an entry for each successfully loaded file is written to the `aurora_s3_load_history` table.

### Verifying loaded files using the `aurora_s3_load_history` table

Every successful `LOAD DATA FROM S3` statement updates the `aurora_s3_load_history` table in the `mysql` schema with an entry for each file that was loaded.

After you run the `LOAD DATA FROM S3` statement, you can verify which files were loaded by querying the `aurora_s3_load_history` table. To see the files that were loaded from one iteration of the statement, use the `WHERE` clause to filter the records on the Amazon S3 URI for the manifest file used in the statement. If you have used the same manifest file before, filter the results using the `timestamp` field.

```sql
select * from mysql.aurora_s3_load_history where load_prefix = 'S3_URI';
```

The following table describes the fields in the `aurora_s3_load_history` table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>load_prefix</code></td>
<td>The URI that was specified in the load statement. This URI can map to any of the following:</td>
</tr>
<tr>
<td></td>
<td>• A single data file for a <code>LOAD DATA FROM S3 FILE</code> statement</td>
</tr>
<tr>
<td></td>
<td>• An Amazon S3 prefix that maps to multiple data files for a <code>LOAD DATA FROM S3 PREFIX</code> statement</td>
</tr>
<tr>
<td></td>
<td>• A single manifest file that contains the names of files to be loaded for a <code>LOAD DATA FROM S3 MANIFEST</code> statement</td>
</tr>
<tr>
<td><code>file_name</code></td>
<td>The name of a file that was loaded into Aurora from Amazon S3 using the URI identified in the <code>load_prefix</code> field.</td>
</tr>
<tr>
<td><code>version_number</code></td>
<td>The version number of the file identified by the <code>file_name</code> field</td>
</tr>
<tr>
<td><code>bytes_loaded</code></td>
<td>The size of the file loaded, in bytes.</td>
</tr>
<tr>
<td><code>load_timestamp</code></td>
<td>The timestamp when the <code>LOAD DATA FROM S3</code> statement completed.</td>
</tr>
</tbody>
</table>
Examples

The following statement loads data from an Amazon S3 bucket that is in the same region as the Aurora DB cluster. The statement reads the comma-delimited data in the file `customerdata.txt` that is in the `dbbucket` Amazon S3 bucket, and then loads the data into the table `store-schema.customer-table`.

```
LOAD DATA FROM S3 's3://dbbucket/customerdata.csv'
  INTO TABLE store-schema.customer-table
  FIELDS TERMINATED BY ','
  LINES TERMINATED BY '\n'
  (ID, FIRSTNAME, LASTNAME, ADDRESS, EMAIL, PHONE);
```

The following statement loads data from an Amazon S3 bucket that is in a different region from the Aurora DB cluster. The statement reads the comma-delimited data from all files that match the `employee-data` object prefix in the `my-data` Amazon S3 bucket in the `us-west-2` region, and then loads the data into the `employees` table.

```
LOAD DATA FROM S3 PREFIX 's3-us-west-2://my-data/employee_data'
  INTO TABLE employees
  FIELDS TERMINATED BY ','
  LINES TERMINATED BY '\n'
  (ID, FIRSTNAME, LASTNAME, EMAIL, SALARY);
```

The following statement loads data from the files specified in a JSON manifest file named `q1_sales.json` into the `sales` table.

```
LOAD DATA FROM S3 MANIFEST 's3-us-west-2://aurora-bucket/q1_sales.json'
  INTO TABLE sales
  FIELDS TERMINATED BY ','
  LINES TERMINATED BY '\n'
  (MONTH, STORE, GROSS, NET);
```

LOAD XML FROM S3

You can use the `LOAD XML FROM S3` statement to load data from XML files stored on an Amazon S3 bucket in one of three different XML formats:

- Column names as attributes of a `<row>` element. The attribute value identifies the contents of the table field.

  ```
  <row column1="value1" column2="value2" .../>
  ```

- Column names as child elements of a `<row>` element. The value of the child element identifies the contents of the table field.

  ```
  <row>
  <column1>value1</column1>
  <column2>value2</column2>
  </row>
  ```

- Column names in the `name` attribute of `<field>` elements in a `<row>` element. The value of the `<field>` element identifies the contents of the table field.

  ```
  <row>
  <field name='column1'>value1</field>
  <field name='column2'>value2</field>
  ```
Loading data from text files in Amazon S3

Syntax

```sql
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,...]
```

Parameters

Following, you can find a list of the required and optional parameters used by the `LOAD DATA FROM S3` statement. You can find more details about some of these parameters in `LOAD XML syntax` in the MySQL documentation.

- **FILE | PREFIX** – Identifies whether to load the data from a single file, or from all files that match a given prefix. `FILE` is the default.
- **REPLACE | IGNORE** – Determines what action to take if an input row has the same unique key values as an existing row in the database table.
  - Specify `REPLACE` if you want the input row to replace the existing row in the table.
  - Specify `IGNORE` if you want to discard the input row. `IGNORE` is the default.
- **INTO TABLE** – Identifies the name of the database table to load the input rows into.
- **PARTITION** – Requires that all input rows be inserted into the partitions identified by the specified list of comma-separated partition names. If an input row cannot be inserted into one of the specified partitions, then the statement fails and an error is returned.
- **CHARACTER SET** – Identifies the character set of the data in the input file.
- **ROWS IDENTIFIED BY** – Identifies the element name that identifies a row in the input file. The default is `<row>`.
- **IGNORE number LINES | ROWS** – Specifies to ignore a certain number of lines or rows at the start of the input file. For example, you can use `IGNORE 1 LINES` to skip over the first line in the text file, or `IGNORE 2 ROWS` to skip over the first two rows of data in the input XML.
- **field_name_or_user_var, ...** – Specifies a comma-separated list of one or more XML element names or user variables that identify which elements to load by name. The name of a user variable used for this purpose must match the name of an element from the XML file, prefixed with `@`. You can employ user variables to store the corresponding field values for subsequent reuse.

For example, the following statement loads the first column from the input file into the first column of `table1`, and sets the value of the `table_column2` column in `table1` to the input value of the second column divided by 100.

```sql
LOAD XML FROM S3 's3://mybucket/data.xml'
INTO TABLE table1
(column1, @var1)
SET table_column2 = @var1/100;
```

- **SET** – Specifies a comma-separated list of assignment operations that set the values of columns in the table to values not included in the input file.
For example, the following statement sets the first two columns of `table1` to the values in the first two columns from the input file, and then sets the value of the `column3` in `table1` to the current time stamp.

```sql
LOAD XML FROM S3 's3://mybucket/data.xml'
INTO TABLE table1
(column1, column2)
SET column3 = CURRENT_TIMESTAMP;
```

You can use subqueries in the right side of `SET` assignments. For a subquery that returns a value to be assigned to a column, you can use only a scalar subquery. Also, you cannot use a subquery to select from the table that is being loaded.

Related topics

- Integrating Amazon Aurora MySQL with other AWS services (p. 792)
- Saving data from an Amazon Aurora MySQL DB cluster into text files in an Amazon S3 bucket (p. 812)
- Managing an Amazon Aurora DB cluster (p. 322)
- Migrating data to an Amazon Aurora DB cluster (p. 321)

Saving data from an Amazon Aurora MySQL DB cluster into text files in an Amazon S3 bucket

You can use the `SELECT INTO OUTFILE S3` statement to query data from an Amazon Aurora MySQL DB cluster and save it directly into text files stored in an Amazon S3 bucket. You can use this functionality to skip bringing the data down to the client first, and then copying it from the client to Amazon S3. The `LOAD DATA FROM S3` statement can use the files created by this statement to load data into an Aurora DB cluster. For more information, see Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804).

**Note**
This feature currently isn't available for Aurora Serverless clusters.

Giving Aurora MySQL access to Amazon S3

Before you can save data into an Amazon S3 bucket, you must first give your Aurora MySQL DB cluster permission to access Amazon S3.

**To give Aurora MySQL access to Amazon S3**

1. Create an AWS Identity and Access Management (IAM) policy that provides the bucket and object permissions that allow your Aurora MySQL DB cluster to access Amazon S3. For instructions, see Creating an IAM policy to access Amazon S3 resources (p. 794).
2. Create an IAM role, and attach the IAM policy you created in Creating an IAM policy to access Amazon S3 resources (p. 794) to the new IAM role. For instructions, see Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).
3. Set either the `aurora_select_into_s3_role` or `aws_default_s3_role` DB cluster parameter to the Amazon Resource Name (ARN) of the new IAM role. If an IAM role isn't specified for `aurora_select_into_s3_role`, Aurora uses the IAM role specified in `aws_default_s3_role`. 
If the cluster is part of an Aurora global database, set this parameter for each Aurora cluster in the global database.

For more information about DB cluster parameters, see Amazon Aurora DB cluster and DB instance parameters (p. 300).

4. To permit database users in an Aurora MySQL DB cluster to access Amazon S3, associate the role that you created in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799) with the DB cluster.

For an Aurora global database, associate the role with each Aurora cluster in the global database.

For information about associating an IAM role with a DB cluster, see Associating an IAM role with an Amazon Aurora MySQL DB cluster (p. 800).

5. Configure your Aurora MySQL DB cluster to allow outbound connections to Amazon S3. For instructions, see Enabling network communication from Amazon Aurora MySQL to other AWS services (p. 803).

For an Aurora global database, enable outbound connections for each Aurora cluster in the global database.

Granting privileges to save data in Aurora MySQL

The database user that issues the SELECT INTO OUTFILE S3 statement must be granted the SELECT INTO S3 privilege to issue the statement. The master user name for a DB cluster is granted the SELECT INTO S3 privilege by default. You can grant the privilege to another user by using the following statement.

```sql
GRANT SELECT INTO S3 ON *.* TO 'user'@'domain-or-ip-address'
```

The SELECT INTO S3 privilege is specific to Amazon Aurora MySQL and is not available for MySQL databases or RDS MySQL DB instances. If you have set up replication between an Aurora MySQL DB cluster as the replication master and a MySQL database as the replication client, then the GRANT SELECT INTO S3 statement causes replication to stop with an error. You can safely skip the error to resume replication. To skip the error on an RDS MySQL DB instance, use the mysql_rds_skip_repl_error procedure. To skip the error on an external MySQL database, use the SET GLOBAL sql_slave_skip_counter statement.

Specifying a path to an Amazon S3 bucket

The syntax for specifying a path to store the data and manifest files on an Amazon S3 bucket is similar to that used in the LOAD DATA FROM S3 PREFIX statement, as shown following.

```sql
s3-region://bucket-name/file-prefix
```

The path includes the following values:

- **region** (optional) – The AWS Region that contains the Amazon S3 bucket to save the data into. This value is optional. If you don't specify a region value, then Aurora saves your files into Amazon S3 in the same region as your DB cluster.
- **bucket-name** – The name of the Amazon S3 bucket to save the data into. Object prefixes that identify a virtual folder path are supported.
- **file-prefix** – The Amazon S3 object prefix that identifies the files to be saved in Amazon S3.
The data files created by the `SELECT INTO OUTFILE S3` statement use the following path, in which `00000` represents a 5-digit, zero-based integer number.

`s3-region://bucket-name/file-prefix.part_00000`

For example, suppose that a `SELECT INTO OUTFILE S3` statement specifies `s3-us-west-2://bucket/prefix` as the path in which to store data files and creates three data files. The specified Amazon S3 bucket contains the following data files.

- s3-us-west-2://bucket/prefix.part_00000
- s3-us-west-2://bucket/prefix.part_00001
- s3-us-west-2://bucket/prefix.part_00002

Creating a manifest to list data files

You can use the `SELECT INTO OUTFILE S3` statement with the `MANIFEST ON` option to create a manifest file in JSON format that lists the text files created by the statement. The `LOAD DATA FROM S3` statement can use the manifest file to load the data files back into an Aurora MySQL DB cluster. For more information about using a manifest to load data files from Amazon S3 into an Aurora MySQL DB cluster, see Using a manifest to specify data files to load (p. 807).

The data files included in the manifest created by the `SELECT INTO OUTFILE S3` statement are listed in the order that they're created by the statement. For example, suppose that a `SELECT INTO OUTFILE S3` statement specified `s3-us-west-2://bucket/prefix` as the path in which to store data files and creates three data files and a manifest file. The specified Amazon S3 bucket contains a manifest file named `s3-us-west-2://bucket/prefix.manifest`, that contains the following information.

```json
{
  "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**

You can use the `SELECT INTO OUTFILE S3` statement to query data from a DB cluster and save it directly into delimited text files stored in an Amazon S3 bucket. Compressed files are not supported. Encrypted files are supported starting in Aurora MySQL 2.09.0.

**Syntax**

```sql
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}]
[PROCEDURE procedure_name(argument_list)]
INTO OUTFILE S3 's3_uri'
[CHARACTER SET charset_name]
[export_options]
[MANIFEST {ON | OFF}]
[OVERWRITE {ON | OFF}]

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']
]

Parameters

Following, you can find a list of the required and optional parameters used by the `SELECT INTO OUTFILE S3` statement that are specific to Aurora.

- **s3-uri** – Specifies the URI for an Amazon S3 prefix to use. Specify the URI using the syntax described in `Specifying a path to an Amazon S3 bucket (p. 813)`.

- **FORMAT {CSV|TEXT} [HEADER]** – Optionally saves the data in CSV format. This syntax is available in Aurora MySQL version 2.07.0 and later.

  The **TEXT** option is the default and produces the existing MySQL export format.

  The **CSV** option produces comma-separated data values. The CSV format follows the specification in `RFC-4180`. If you specify the optional keyword **HEADER**, the output file contains one header line. The labels in the header line correspond to the column names from the `SELECT` statement. You can use the CSV files for training data models for use with AWS ML services. For more information about using exported Aurora data with AWS ML services, see `Exporting data to Amazon S3 for SageMaker model training (p. 833)`.

- **MANIFEST {ON | OFF}** – Indicates whether a manifest file is created in Amazon S3. The manifest file is a JavaScript Object Notation (JSON) file that can be used to load data into an Aurora DB cluster with the `LOAD DATA FROM S3 MANIFEST` statement. For more information about `LOAD DATA FROM S3 MANIFEST`, see `Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804)`.

  If **MANIFEST ON** is specified in the query, the manifest file is created in Amazon S3 after all data files have been created and uploaded. The manifest file is created using the following path:

  `s3-region://bucket-name/file-prefix.manifest`

  For more information about the format of the manifest file's contents, see `Creating a manifest to list data files (p. 814)`.


815
• **OVERWRITE (ON | OFF)** – Indicates whether existing files in the specified Amazon S3 bucket are overwritten. If OVERWRITE ON is specified, existing files that match the file prefix in the URI specified in `s3-uri` are overwitten. Otherwise, an error occurs.

You can find more details about other parameters in **SELECT syntax** and **LOAD DATA INFILE syntax**, in the MySQL documentation.

**Considerations**

The number of files written to the Amazon S3 bucket depends on the amount of data selected by the `SELECT INTO OUTFILE S3` statement and the file size threshold for Aurora MySQL. The default file size threshold is 6 gigabytes (GB). If the data selected by the statement is less than the file size threshold, a single file is created; otherwise, multiple files are created. Other considerations for files created by this statement include the following:

- Aurora MySQL guarantees that rows in data files are not split across file boundaries. For multiple files, the size of every data file except the last is typically close to the file size threshold. However, occasionally staying under the file size threshold results in a row being split across two data files. In this case, Aurora MySQL creates a data file that keeps the row intact, but might be larger than the file size threshold.

- Because each `SELECT` statement in Aurora MySQL runs as an atomic transaction, a `SELECT INTO OUTFILE S3` statement that selects a large data set might run for some time. If the statement fails for any reason, you might need to start over and issue the statement again. If the statement fails, however, files already uploaded to Amazon S3 remain in the specified Amazon S3 bucket. You can use another statement to upload the remaining data instead of starting over again.

- If the amount of data to be selected is large (more than 25 GB), we recommend that you use multiple `SELECT INTO OUTFILE S3` statements to save the data to Amazon S3. Each statement should select a different portion of the data to be saved, and also specify a different `file_prefix` in the `s3-uri` parameter to use when saving the data files. Partitioning the data to be selected with multiple statements makes it easier to recover from an error in one statement. If an error occurs for one statement, only a portion of data needs to be re-selected and uploaded to Amazon S3. Using multiple statements also helps to avoid a single long-running transaction, which can improve performance.

- If multiple `SELECT INTO OUTFILE S3` statements that use the same `file_prefix` in the `s3-uri` parameter run in parallel to select data into Amazon S3, the behavior is undefined.

- Metadata, such as table schema or file metadata, is not uploaded by Aurora MySQL to Amazon S3.

- In some cases, you might re-run a `SELECT INTO OUTFILE S3` query, such as to recover from a failure. In these cases, you must either remove any existing data files in the Amazon S3 bucket with the same file prefix specified in `s3-uri`, or include OVERWRITE ON in the `SELECT INTO OUTFILE S3` query.

The `SELECT INTO OUTFILE S3` statement returns a typical MySQL error number and response on success or failure. If you don't have access to the MySQL error number and response, the easiest way to determine when it's done is by specifying MANIFEST ON in the statement. The manifest file is the last file written by the statement. In other words, if you have a manifest file, the statement has completed.

Currently, there's no way to directly monitor the progress of the `SELECT INTO OUTFILE S3` statement while it runs. However, suppose that you're writing a large amount of data from Aurora MySQL to Amazon S3 using this statement, and you know the size of the data selected by the statement. In this case, you can estimate progress by monitoring the creation of data files in Amazon S3.

To do so, you can use the fact that a data file is created in the specified Amazon S3 bucket for about every 6 GB of data selected by the statement. Divide the size of the data selected by 6 GB to get the estimated number of data files to create. You can then estimate the progress of the statement by monitoring the number of files uploaded to Amazon S3 while the statement runs.
Examples

The following statement selects all of the data in the `employees` table and saves the data into an Amazon S3 bucket that is in a different region from the Aurora MySQL DB cluster. The statement creates data files in which each field is terminated by a comma (,) character and each row is terminated by a newline (\n) character. The statement returns an error if files that match the `sample_employee_data` file prefix exist in the specified Amazon S3 bucket.

```sql
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';
```

The following statement selects all of the data in the `employees` table and saves the data into an Amazon S3 bucket that is in the same region as the Aurora MySQL DB cluster. The statement creates data files in which each field is terminated by a comma (,) character and each row is terminated by a newline (\n) character, and also a manifest file. The statement returns an error if files that match the `sample_employee_data` file prefix exist in the specified Amazon S3 bucket.

```sql
SELECT * FROM employees INTO OUTFILE S3 's3://aurora-select-into-s3-pdx/sample_employee_data'
    FIELDS TERMINATED BY ',
    LINES TERMINATED BY '\n'
    MANIFEST ON;
```

The following statement selects all of the data in the `employees` table and saves the data into an Amazon S3 bucket that is in a different region from the Aurora DB cluster. The statement creates data files in which each field is terminated by a comma (,) character and each row is terminated by a newline (\n) character. The statement overwrites any existing files that match the `sample_employee_data` file prefix in the specified Amazon S3 bucket.

```sql
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;
```

The following statement selects all of the data in the `employees` table and saves the data into an Amazon S3 bucket that is in the same region as the Aurora MySQL DB cluster. The statement creates data files in which each field is terminated by a comma (,) character and each row is terminated by a newline (\n) character, and also a manifest file. The statement overwrites any existing files that match the `sample_employee_data` file prefix in the specified Amazon S3 bucket.

```sql
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;
```

Related topics

- Integrating Aurora with other AWS services (p. 371)
- Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804)
- Managing an Amazon Aurora DB cluster (p. 322)
Invoking a Lambda function from an Amazon Aurora MySQL DB cluster

You can invoke an AWS Lambda function from an Amazon Aurora with MySQL compatibility DB cluster with a native function or a stored procedure. Before invoking a Lambda function from an Aurora MySQL, the Aurora DB cluster must have access to Lambda.

In recent Aurora MySQL versions, using a stored procedure is deprecated. We strongly recommend using an Aurora MySQL native function if you are using one of the following Aurora MySQL versions:

- Aurora MySQL version 1.16 and later, for MySQL 5.6-compatible clusters.
- Aurora MySQL version 2.06 and later, for MySQL 5.7-compatible clusters.

Topics

- Giving Aurora access to Lambda (p. 818)
- Invoking a Lambda function with an Aurora MySQL native function (p. 819)
- Invoking a Lambda function with an Aurora MySQL stored procedure (p. 821)

Giving Aurora access to Lambda

Before you can invoke Lambda functions from an Aurora MySQL, you must first give your Aurora MySQL DB cluster permission to access Lambda.

To give Aurora MySQL access to Lambda

1. Create an AWS Identity and Access Management (IAM) policy that provides the permissions that allow your Aurora MySQL DB cluster to invoke Lambda functions. For instructions, see Creating an IAM policy to access AWS Lambda resources (p. 796).

2. Create an IAM role, and attach the IAM policy you created in Creating an IAM policy to access AWS Lambda resources (p. 796) to the new IAM role. For instructions, see Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).

3. Set the `aws_default_lambda_role` DB cluster parameter to the Amazon Resource Name (ARN) of the new IAM role.

   If the cluster is part of an Aurora global database, apply the same setting for each Aurora cluster in the global database.

   For more information about DB cluster parameters, see Amazon Aurora DB cluster and DB instance parameters (p. 300).

4. To permit database users in an Aurora MySQL DB cluster to invoke Lambda functions, associate the role that you created in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799) with the DB cluster. For information about associating an IAM role with a DB cluster, see Associating an IAM role with an Amazon Aurora MySQL DB cluster (p. 800).

   If the cluster is part of an Aurora global database, associate the role with each Aurora cluster in the global database.

5. Configure your Aurora MySQL DB cluster to allow outbound connections to Lambda. For instructions, see Enabling network communication from Amazon Aurora MySQL to other AWS services (p. 803).
If the cluster is part of an Aurora global database, enable outbound connections for each Aurora cluster in the global database.

## Invoking a Lambda function with an Aurora MySQL native function

**Note**
You can call the native functions `lambda_sync` and `lambda_async` when you use Aurora MySQL version 1.16 and later, or Aurora MySQL 2.06 and later. For more information about Aurora MySQL versions, see Database engine updates for Amazon Aurora MySQL (p. 874).

You can invoke an AWS Lambda function from an Aurora MySQL DB cluster by calling the native functions `lambda_sync` and `lambda_async`. This approach can be useful when you want to integrate your database running on Aurora MySQL with other AWS services. For example, you might want to send a notification using Amazon Simple Notification Service (Amazon SNS) whenever a row is inserted into a specific table in your database.

### Working with native functions to invoke a Lambda function

The `lambda_sync` and `lambda_async` functions are built-in, native functions that invoke a Lambda function synchronously or asynchronously. When you must know the result of the Lambda function before moving on to another action, use the synchronous function `lambda_sync`. When you don't need to know the result of the Lambda function before moving on to another action, use the asynchronous function `lambda_async`.

The user invoking a native function must be granted the `INVOKE LAMBDA` privilege. To grant this privilege to a user, connect to the DB instance as the master user, and run the following statement.

```sql
GRANT INVOKE LAMBDA ON *.* TO user@domain-or-ip-address
```

You can revoke this privilege by running the following statement.

```sql
REVOKE INVOKE LAMBDA ON *.* FROM user@domain-or-ip-address
```

### Syntax for the `lambda_sync` function

You invoke the `lambda_sync` function synchronously with the RequestResponse invocation type. The function returns the result of the Lambda invocation in a JSON payload. The function has the following syntax.

```sql
lambda_sync (lambda_function_ARN, JSON_payload)
```

**Note**
You can use triggers to call Lambda on data-modifying statements. Remember that triggers are not run once per SQL statement, but once per row modified, one row at a time. When a trigger runs, the process is synchronous. The data-modifying statement only returns when the trigger completes.

Be careful when invoking an AWS Lambda function from triggers on tables that experience high write traffic. `INSERT`, `UPDATE`, and `DELETE` triggers are activated per row. A write-heavy
workload on a table with INSERT, UPDATE, or DELETE triggers results in a large number of calls to your AWS Lambda function.

Parameters for the lambda_sync function

The lambda_sync function has the following parameters.

lambda_function_ARN

The Amazon Resource Name (ARN) of the Lambda function to invoke.

JSON_payload

The payload for the invoked Lambda function, in JSON format.

Note

Aurora MySQL doesn't support JSON parsing. JSON parsing isn't required when a Lambda function returns an atomic value, such as a number or a string.

Example for the lambda_sync function

The following query based on lambda_sync invokes the Lambda function BasicTestLambda synchronously using the function ARN. The payload for the function is {"operation": "ping"}.

```
SELECT lambda_sync(
    'arn:aws:lambda:us-east-1:868710585169:function:BasicTestLambda',
    '{"operation": "ping"}');
```

Syntax for the lambda_async function

You invoke the lambda_async function asynchronously with the Event invocation type. The function returns the result of the Lambda invocation in a JSON payload. The function has the following syntax.

```
lambda_async(
    lambda_function_ARN,
    JSON_payload
)
```

Parameters for the lambda_async function

The lambda_async function has the following parameters.

lambda_function_ARN

The Amazon Resource Name (ARN) of the Lambda function to invoke.

JSON_payload

The payload for the invoked Lambda function, in JSON format.

Note

Aurora MySQL doesn't support JSON parsing. JSON parsing isn't required when a Lambda function returns an atomic value, such as a number or a string.

Example for the lambda_async function

The following query based on lambda_async invokes the Lambda function BasicTestLambda asynchronously using the function ARN. The payload for the function is {"operation": "ping"}.

```
lambda_async (  
    lambda_function_ARN,  
    JSON_payload  
)
```
SELECT lambda_async(
    'arn:aws:lambda:us-east-1:868710585169:function:BasicTestLambda',
    "{"operation": "ping"}");

Related topics
• Integrating Aurora with other AWS services (p. 371)
• Managing an Amazon Aurora DB cluster (p. 322)
• AWS Lambda Developer Guide

Invoking a Lambda function with an Aurora MySQL stored procedure
You can invoke an AWS Lambda function from an Aurora MySQL DB cluster by calling the `mysql.lambda_async` procedure. This approach can be useful when you want to integrate your database running on Aurora MySQL with other AWS services. For example, you might want to send a notification using Amazon Simple Notification Service (Amazon SNS) whenever a row is inserted into a specific table in your database.

Aurora MySQL version considerations
Starting in Aurora MySQL version 1.8 and Aurora MySQL version 2.06, you can use the native function method instead of these stored procedures to invoke a Lambda function. For more information about the native functions, see Working with native functions to invoke a Lambda function (p. 819).

Starting with Amazon Aurora version 1.16 and 2.06, the stored procedure `mysql.lambda_async` is deprecated. If you are using an Aurora version that's higher than 1.16 or 2.06, we strongly recommend that you work with native Lambda functions instead.

Working with the `mysql.lambda_async` procedure to invoke a Lambda function
The `mysql.lambda_async` procedure is a built-in stored procedure that invokes a Lambda function asynchronously. To use this procedure, your database user must have `EXECUTE` privilege on the `mysql.lambda_async` stored procedure.

Syntax
The `mysql.lambda_async` procedure has the following syntax.

```sql
CALL mysql.lambda_async (
    lambda_function_ARN,
    lambda_function_input
)
```

Parameters
The `mysql.lambda_async` procedure has the following parameters.

`lambda_function_ARN`
The Amazon Resource Name (ARN) of the Lambda function to invoke.

`lambda_function_input`
The input string, in JSON format, for the invoked Lambda function.
Examples

As a best practice, we recommend that you wrap calls to the `mysql.lambda_async` procedure in a stored procedure that can be called from different sources such as triggers or client code. This approach can help to avoid impedance mismatch issues and make it easier to invoke Lambda functions.

**Note**

Be careful when invoking an AWS Lambda function from triggers on tables that experience high write traffic. `INSERT`, `UPDATE`, and `DELETE` triggers are activated per row. A write-heavy workload on a table with `INSERT`, `UPDATE`, or `DELETE` triggers results in a large number of calls to your AWS Lambda function.

Although calls to the `mysql.lambda_async` procedure are asynchronous, triggers are synchronous. A statement that results in a large number of trigger activations doesn't wait for the call to the AWS Lambda function to complete, but it does wait for the triggers to complete before returning control to the client.

**Example Example: Invoke an AWS Lambda function to send email**

The following example creates a stored procedure that you can call in your database code to send an email using a Lambda function.

**AWS Lambda Function**

```python
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']
                }
            }
        }
    )
```

**Stored Procedure**

```sql
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(
        CONCAT({"email_to": ": ", email_to,
```
Call the Stored Procedure to Invoke the AWS Lambda Function

```sql
mysql> call SES_send_email('example_from@amazon.com', 'example_to@amazon.com', 'Email subject', 'Email content');
```

Example Example: Invoke an AWS Lambda function to publish an event from a trigger

The following example creates a stored procedure that publishes an event by using Amazon SNS. The code calls the procedure from a trigger when a row is added to a table.

**AWS Lambda Function**

```python
import boto3

sns = boto3.client('sns')

def SNS_publish_message(event, context):
    return sns.publish(
        Message=event['message'],
        Subject=event['subject'],
        MessageStructure='string'
    )
```

**Stored Procedure**

```sql
DROP PROCEDURE IF EXISTS SNS_Publish_Message;
DELIMITER ;
CREATE PROCEDURE SNS_Publish_Message (IN subject VARCHAR(255),
IN message TEXT) LANGUAGE SQL
BEGIN
        CONCAT('{ "subject" : ", subject,
                "message" : ", message, "}')
    );
END
DELIMITER ;
```

**Table**

```sql
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;
```
Trigger

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 ;

Insert a Row into the Table to Trigger the Notification

mysql> insert into Customer_Feedback (customer_name, customer_feedback) VALUES ('Sample Customer', 'Good job guys!');

Related topics

- Integrating Aurora with other AWS services (p. 371)
- Managing an Amazon Aurora DB cluster (p. 322)
- AWS Lambda Developer Guide

Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs

You can configure your Aurora MySQL DB cluster to publish general, slow, audit, and error log data to a log group in Amazon CloudWatch Logs. With CloudWatch Logs, you can perform real-time analysis of the log data, and use CloudWatch to create alarms and view metrics. You can use CloudWatch Logs to store your log records in highly durable storage.

To publish logs to CloudWatch Logs, the respective logs must be enabled. Error logs are enabled by default, but you must enable the other types of logs explicitly. For information about enabling logs in MySQL, see Selecting general query and slow query log output destinations in the MySQL documentation. For more information about enabling Aurora MySQL audit logs, see Enabling advanced auditing (p. 727).

Note

Be aware of the following:

- You can't publish logs to CloudWatch Logs for the China (Ningxia) region.
- If exporting log data is disabled, Aurora doesn't delete existing log groups or log streams. If exporting log data is disabled, existing log data remains available in CloudWatch Logs, depending on log retention, and you still incur charges for stored audit log data. You can delete log streams and log groups using the CloudWatch Logs console, the AWS CLI, or the CloudWatch Logs API.
- An alternative way to publish audit logs to CloudWatch Logs is by enabling advanced auditing and setting the cluster-level DB parameter server_audit_logs_upload to 1. The default for the server_audit_logs_upload parameter is 0.

    If you use this alternative method, you must have an IAM role to access CloudWatch Logs and set the aws_default_logs_role cluster-level parameter to the ARN for this
role. For information about creating the role, see Setting up IAM roles to access AWS services (p. 793). However, if you have the AWSServiceRoleForRDS service-linked role, it provides access to CloudWatch Logs and overrides any custom-defined roles. For information service-linked roles for Amazon RDS, see Using service-linked roles for Amazon Aurora (p. 1277).

- If you don't want to export audit logs to CloudWatch Logs, make sure that all methods of exporting audit logs are disabled. These methods are the AWS Management Console, the AWS CLI, the RDS API, and the server_audit_logs_upload parameter.

- The procedure is slightly different for Aurora Serverless clusters than for provisioned clusters. Serverless clusters automatically upload all the kinds of logs that you enable through the configuration parameters. Therefore, you enable or disable log upload for Serverless clusters by turning different log types on and off in the DB cluster parameter group. You don't modify the settings of the cluster itself through the AWS Management Console, AWS CLI, or RDS API. For information about enabling MySQL logs for Serverless clusters, see Aurora Serverless v1 and parameter groups (p. 142).

**Console**

You can publish Aurora MySQL logs for provisioned clusters to CloudWatch Logs with the console.

**To publish Aurora MySQL logs from the console**

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the Aurora MySQL DB cluster that you want to publish the log data for.
4. Choose Modify.
5. In the Log exports section, choose the logs that you want to start publishing to CloudWatch Logs.
6. Choose Continue, and then choose Modify DB Cluster on the summary page.

**AWS CLI**

You can publish Aurora MySQL logs for provisioned clusters with the AWS CLI. To do so, you run the `modify-db-cluster` AWS CLI command with the following options:

- `--db-cluster-identifier`—The DB cluster identifier.
- `--cloudwatch-logs-export-configuration`—The configuration setting for the log types to be enabled for export to CloudWatch Logs for the DB cluster.

You can also publish Aurora MySQL logs by running one of the following AWS CLI commands:

- `create-db-cluster`
- `restore-db-cluster-from-s3`
- `restore-db-cluster-from-snapshot`
- `restore-db-cluster-to-point-in-time`

Run one of these AWS CLI commands with the following options:

- `--db-cluster-identifier`—The DB cluster identifier.
- `--engine`—The database engine.
- `--enable-cloudwatch-logs-exports`—The configuration setting for the log types to be enabled for export to CloudWatch Logs for the DB cluster.
Other options might be required depending on the AWS CLI command that you run.

Example

The following command modifies an existing Aurora MySQL DB cluster to publish log files to CloudWatch Logs.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster \
  --db-cluster-identifier mydbcluster \
  --cloudwatch-logs-export-configuration '{"EnableLogTypes": ["error","general","slowquery","audit"]}'
```

For Windows:

```bash
aws rds modify-db-cluster ^
  --db-cluster-identifier mydbcluster ^
  --cloudwatch-logs-export-configuration '{"EnableLogTypes": ["error","general","slowquery","audit"]}'
```

Example

The following command creates an Aurora MySQL DB cluster to publish log files to CloudWatch Logs.

For Linux, macOS, or Unix:

```bash
aws rds create-db-cluster \
  --db-cluster-identifier mydbcluster \
  --engine aurora \
  --enable-cloudwatch-logs-exports '["error","general","slowquery","audit"]'
```

For Windows:

```bash
aws rds create-db-cluster ^
  --db-cluster-identifier mydbcluster ^
  --engine aurora ^
  --enable-cloudwatch-logs-exports '["error","general","slowquery","audit"]'
```

RDS API

You can publish Aurora MySQL logs for provisioned clusters with the RDS API. To do so, you run the `ModifyDBCluster` operation with the following options:

- `DBClusterIdentifier`—The DB cluster identifier.
- `CloudWatchLogsExportConfiguration`—The configuration setting for the log types to be enabled for export to CloudWatch Logs for the DB cluster.

You can also publish Aurora MySQL logs with the RDS API by running one of the following RDS API operations:

- `CreateDBCluster`
Run the RDS API operation with the following parameters:

- **DBClusterIdentifier**—The DB cluster identifier.
- **Engine**—The database engine.
- **EnableCloudwatchLogsExports**—The configuration setting for the log types to be enabled for export to CloudWatch Logs for the DB cluster.

Other parameters might be required depending on the AWS CLI command that you run.

### Monitoring log events in Amazon CloudWatch

After enabling Aurora MySQL log events, you can monitor the events in Amazon CloudWatch Logs. A new log group is automatically created for the Aurora DB cluster under the following prefix, in which `cluster-name` represents the DB cluster name, and `log_type` represents the log type.

```
/aws/rds/cluster/cluster-name/log_type
```

For example, if you configure the export function to include the slow query log for a DB cluster named `mydbcluster`, slow query data is stored in the `/aws/rds/cluster/mydbcluster/slowquery` log group.

All of the events from all of the DB instances in a DB cluster are pushed to a log group using different log streams.

If a log group with the specified name exists, Aurora uses that log group to export log data for the Aurora DB cluster. You can use automated configuration, such as AWS CloudFormation, to create log groups with predefined log retention periods, metric filters, and customer access. Otherwise, a new log group is automatically created using the default log retention period, **Never Expire**, in CloudWatch Logs. You can use the CloudWatch Logs console, the AWS CLI, or the CloudWatch Logs API to change the log retention period. For more information about changing log retention periods in CloudWatch Logs, see [Change log data retention in CloudWatch Logs](#).

You can use the CloudWatch Logs console, the AWS CLI, or the CloudWatch Logs API to search for information within the log events for a DB cluster. For more information about searching and filtering log data, see [Searching and filtering log data](#).

### Using machine learning (ML) with Aurora MySQL

Aurora machine learning enables you to add machine learning-based predictions to database applications using the SQL language. Aurora machine learning makes use of a highly optimized integration between the Aurora database and AWS machine learning (ML) services SageMaker and Amazon Comprehend.

**Benefits of Aurora Machine Learning** include the following:

- You can add ML-based predictions to your existing database applications. You don't need to build custom integrations or learn separate tools. You can embed machine learning processing directly into your SQL query as calls to stored functions.
- The ML integration is a fast way to enable ML services to work with transactional data. You don't have to move the data out of the database to perform the machine learning operations. You don't have
to convert or reimport the results of the machine learning operations to use them in your database application.

- You can use your existing governance policies to control who has access to the underlying data and to the generated insights.

AWS ML Services are managed services that are set up and run in their own production environments. Currently, Aurora Machine Learning integrates with Amazon Comprehend for sentiment analysis and SageMaker for a wide variety of ML algorithms.

For details about using Aurora and Amazon Comprehend together, see Using Amazon Comprehend for sentiment detection (p. 836). For general information about Amazon Comprehend, see Amazon Comprehend.

For details about using Aurora and SageMaker together, see Using SageMaker to run your own ML models (p. 834). For general information about SageMaker, see SageMaker.

Topics
- Prerequisites for Aurora Machine Learning (p. 828)
- Enabling Aurora Machine Learning (p. 828)
- Exporting data to Amazon S3 for SageMaker model training (p. 833)
- Using SageMaker to run your own ML models (p. 834)
- Using Amazon Comprehend for sentiment detection (p. 836)
- Performance considerations for Aurora Machine Learning (p. 837)
- Monitoring Aurora Machine Learning (p. 838)
- Limitations of Aurora Machine Learning (p. 839)

Prerequisites for Aurora Machine Learning

Aurora machine learning is available for any Aurora cluster running Aurora MySQL 2.07.0 and newer versions in AWS Regions that support Aurora machine learning. You can upgrade an Aurora cluster running an older version of Aurora MySQL to a newer version if you want to use Aurora machine learning with that cluster. For more information, see Database engine updates for Amazon Aurora MySQL (p. 874).

For more information about Regions and Aurora version availability, see Aurora machine learning (p. 16).

Enabling Aurora Machine Learning

Enabling the ML capabilities involves the following steps:

- You enable the Aurora cluster to access the Amazon machine learning services SageMaker or Amazon Comprehend, depending the kinds of ML algorithms you want for your application.
- For SageMaker, then you use the Aurora CREATE FUNCTION statement to set up stored functions that access inference features.

  **Note**
  Aurora machine learning includes built-in functions that call Amazon Comprehend for sentiment analysis. You don't need to run any CREATE FUNCTION statements if you only use Amazon Comprehend.

Topics
- Setting up IAM access to Amazon Comprehend and SageMaker (p. 829)
• Granting SQL privileges for invoking Aurora Machine Learning services (p. 833)
• Enabling network communication from Aurora MySQL to other AWS services (p. 833)

Setting up IAM access to Amazon Comprehend and SageMaker

Before you can access SageMaker and Amazon Comprehend services, enable the Aurora MySQL cluster
to access AWS ML services. For your Aurora MySQL DB cluster to access AWS ML services on your behalf,
create and configure AWS Identity and Access Management (IAM) roles. These roles authorize the users
of your Aurora MySQL database to access AWS ML services.

When you use the AWS Management Console, AWS does the IAM setup for you automatically. You can
skip the following information and follow the procedure in Connecting an Aurora DB cluster to Amazon
S3, SageMaker, or Amazon Comprehend using the console (p. 829).

Setting up the IAM roles for SageMaker or Amazon Comprehend using the AWS CLI or the RDS API
consists of the following steps:

1. Create an IAM policy to specify which SageMaker endpoints can be invoked by your Aurora MySQL
cluster or to enable access to Amazon Comprehend.
2. Create an IAM role to permit your Aurora MySQL database cluster to access AWS ML services. The IAM
policy created above is attached to the IAM role.
3. To permit the Aurora MySQL database cluster to access AWS ML services, you associate the IAM role
that you created above to the database cluster.
4. To permit database applications to invoke AWS ML services, you must also grant privileges to specific
database users. For SageMaker, because the calls to the endpoints are wrapped inside a stored
function, you also grant EXECUTE privileges on the stored functions to any database users that call
them.

For general information about how to permit your Aurora MySQL DB cluster to access other AWS
services on your behalf, see Authorizing Amazon Aurora MySQL to access other AWS services on your
behalf (p. 793).

Connecting an Aurora DB cluster to Amazon S3, SageMaker, or Amazon Comprehend using the
console

Aurora machine learning requires that your DB cluster use some combination of Amazon S3, SageMaker,
and Amazon Comprehend. Amazon Comprehend is for sentiment analysis. SageMaker is for a wide
variety of machine learning algorithms. For Aurora Machine Learning, Amazon S3 is only for training
SageMaker models. You only need to use Amazon S3 with Aurora machine learning if you don’t already
have a trained model available and the training is your responsibility. To connect a DB cluster to these
services requires that you set up an AWS Identity and Access Management (IAM) role for each Amazon
service. The IAM role enables users of your DB cluster to authenticate with the corresponding service.

To generate the IAM roles for Amazon S3, SageMaker, or Amazon Comprehend, repeat the following
steps for each service that you need.

To connect a DB cluster to an Amazon service

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://
console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases, and then choose the Aurora MySQL DB cluster that you
want to use.
3. Choose the Connectivity & security tab.
4. Choose Select a service to connect to this cluster in the Manage IAM roles section, and choose the
service that you want to connect to:
Using machine learning with Aurora MySQL

- Amazon S3
- Amazon Comprehend
- SageMaker

5. Choose **Connect service**.
6. Enter the required information for the specific service on the **Connect cluster** window:
   - For SageMaker, enter the Amazon Resource Name (ARN) of a SageMaker endpoint. For details about what the endpoint represents, see [Deploy a model on Amazon SageMaker hosting services](#). In the navigation pane of the SageMaker console, choose **Endpoints** and copy the ARN of the endpoint you want to use.
   - For Amazon Comprehend, don’t specify any additional parameter.
   - For Amazon S3, enter the ARN of an Amazon S3 bucket to use.

   The format of an Amazon S3 bucket ARN is `arn:aws:s3:::bucket_name`. Ensure that the Amazon S3 bucket that you use is set up with the requirements for training SageMaker models. When you train a model, your Aurora DB cluster requires permission to export data to the Amazon S3 bucket, and also to import data from the bucket.

   To learn more about Amazon S3 bucket ARNs, see **Specifying resources in a policy** in the *Amazon Simple Storage Service Developer Guide*. For more about using an Amazon S3 bucket with SageMaker, see **Step 1: Create an Amazon Amazon S3 bucket** in the *Amazon SageMaker Developer Guide*.

7. Choose **Connect service**.
8. Aurora creates a new IAM role and adds it to the DB cluster's list of **Current IAM roles for this cluster**. The IAM role's status is initially **In progress**. The IAM role name is autogenerated with the following pattern for each connected service:
   - The Amazon S3 IAM role name pattern is `rds-cluster_ID-S3-policy-timestamp`.
   - The SageMaker IAM role name pattern is `rds-cluster_ID-SageMaker-policy-timestamp`.
   - The Amazon Comprehend IAM role name pattern is `rds-cluster_ID-Comprehend-policy-timestamp`.

   Aurora also creates a new IAM policy and attaches it to the role. The policy name follows a similar naming convention and also has a timestamp.

**Creating an IAM policy to access SageMaker (AWS CLI only)**

**Note**
When you use the AWS Management Console, Aurora creates the IAM policy automatically. In that case, you can skip this section.

The following policy adds the permissions required by Aurora MySQL to invoke an SageMaker function on your behalf. You can specify all of your SageMaker endpoints that you need your database applications to access from your Aurora MySQL cluster in a single policy. The policy allows you to specify the AWS Region for an SageMaker endpoint. However, an Aurora MySQL cluster can only invoke SageMaker models deployed in the same AWS Region as the cluster.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAuroraToInvokeRCFEndPoint",
      "Effect": "Allow",
```
Using machine learning with Aurora MySQL

The following command performs the same operation through the AWS CLI.

```
aws iam put-role-policy --role-name role_name --policy-name policy_name
}
```

Creating an IAM policy to access Amazon Comprehend (AWS CLI only)

**Note**

When you use the AWS Management Console, Aurora creates the IAM policy automatically. In that case, you can skip this section.

The following policy adds the permissions required by Aurora MySQL to invoke AWS Amazon Comprehend on your behalf.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAuroraToInvokeComprehendDetectSentiment",
      "Effect": "Allow",
      "Action": [
        "comprehend:DetectSentiment",
        "comprehend:BatchDetectSentiment"
      ],
      "Resource": "*"
    }
  ]
}
```

The following command performs the same operation through the AWS CLI.

```
aws iam put-role-policy --role-name role_name --policy-name policy_name
}
```

To create an IAM policy to grant access to Amazon Comprehend

1. Open the IAM Management Console.
2. In the navigation pane, choose Policies.
3. Choose Create policy.
4. On the Visual editor tab, choose Choose a service, and then choose Comprehend.
5. For Actions, choose Detect Sentiment and BatchDetectSentiment.
7. For Name, enter a name for your IAM policy. You use this name when you create an IAM role to associate with your Aurora DB cluster. You can also add an optional Description value.
8. Choose Create policy.
9. Complete the procedure in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799).
Creating an IAM role to access SageMaker and Amazon Comprehend

After you create the IAM policies, create an IAM role that the Aurora MySQL cluster can assume on behalf of your database users to access ML services. To create an IAM role, you can use the AWS Management Console or the AWS CLI. To create an IAM role and attach the preceding policies to the role, follow the steps described in Creating an IAM role to allow Amazon Aurora to access AWS services (p. 799). For more information about IAM roles, see IAM roles in the AWS Identity and Access Management User Guide.

You can only use a global IAM role for authentication. You can't use an IAM role associated with a database user or a session. This requirement is the same as for Aurora integration with the Lambda and Amazon S3 services.

Associating an IAM role with an Aurora MySQL DB cluster (AWS CLI only)

Note
When you use the AWS Management Console, Aurora creates the IAM policy automatically. In that case, you can skip this section.

The last step is to associate the IAM role with the attached IAM policy with your Aurora MySQL DB cluster. To associate an IAM role with an Aurora DB cluster, you do two things:

1. Add the role to the list of associated roles for a DB cluster by using the AWS Management Console, the add-role-to-db-cluster AWS CLI command, or the AddRoleToDBCluster RDS API operation.
2. Set the cluster-level parameter for the related AWS ML service to the ARN for the associated IAM role. Use the aws_default_sagemaker_role, aws_default_comprehend_role, or both parameters depending on which AWS ML services you intend to use with your Aurora cluster.

Cluster-level parameters are grouped into DB cluster parameter groups. To set the preceding cluster parameters, use an existing custom DB cluster group or create an new one. To create a new DB cluster parameter group, call the create-db-cluster-parameter-group command from the AWS CLI, as shown following.

```
PROMPT> aws rds create-db-cluster-parameter-group  --db-cluster-parameter-group-name AllowAWSAccessToExternalServices  
  --db-parameter-group-family aurora-mysql5.7 --description "Allow access to Amazon S3, AWS Lambda, AWS SageMaker, and AWS Comprehend"
```

Set the appropriate cluster-level parameter or parameters and the related IAM role ARN values in your DB cluster parameter group, as shown in the following.

```
PROMPT> aws rds modify-db-cluster-parameter-group  
  --db-cluster-parameter-group-name AllowAWSAccessToExternalServices  
  --parameters  
  "ParameterName=aws_default_s3_role,ParameterValue=arn:aws:iam::123456789012:role/AllowAuroraS3Role,ApplyMethod=pending-reboot"  
  "ParameterName=aws_default_sagemaker_role,ParameterValue=arn:aws:iam::123456789012:role/AllowAuroraSageMakerRole,ApplyMethod=pending-reboot"  
  "ParameterName=aws_default_comprehend_role,ParameterValue=arn:aws:iam::123456789012:role/AllowAuroraComprehendRole,ApplyMethod=pending-reboot"
```

Modify the DB cluster to use the new DB cluster parameter group. Then, reboot the cluster. The following shows how.

```
PROMPT> aws rds modify-db-cluster --db-cluster-identifier your_cluster_id  
  --db-cluster-parameter-group-name AllowAWSAccessToExternalServices
```

832
When the instance has rebooted, your IAM roles are associated with your DB cluster.

**Granting SQL privileges for invoking Aurora Machine Learning services**

After you create the required IAM policies and roles and associating the role to the Aurora MySQL DB cluster, you authorize individual database users to invoke the Aurora Machine Learning stored functions for SageMaker and built-in functions for Amazon Comprehend.

The database user invoking a native function must be granted the `INVOKE SAGEMAKER` or `INVOKE COMPREHEND` privilege. To grant this privilege to a user, connect to the DB instance as the master user, and run the following statements. Substitute the appropriate details for the database user.

```
GRANT INVOKE SAGEMAKER ON *.* TO user@domain-or-ip-address
GRANT INVOKE COMPREHEND ON *.* TO user@domain-or-ip-address
```

For SageMaker, user-defined functions define the parameters to be sent to the model for producing the inference and to configure the endpoint name to be invoked. You grant `EXECUTE` permission to the stored functions configured for SageMaker for each of the database users who intend to invoke the endpoint.

```
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
```

**Enabling network communication from Aurora MySQL to other AWS services**

Since SageMaker and Amazon Comprehend are external AWS services, you must also configure your Aurora DB cluster to allow outbound connections to the target AWS service. For more information, see Enabling network communication from Amazon Aurora MySQL to other AWS services (p. 803).

You can use VPC endpoints to connect to Amazon S3. AWS PrivateLink can't be used to connect Aurora to AWS machine learning services or Amazon S3 at this time.

**Exporting data to Amazon S3 for SageMaker model training**

Depending on how your team divides the machine learning tasks, you might not perform this task. If someone else provides the SageMaker model for you, you can skip this section.

To train SageMaker models, you export data to an Amazon S3 bucket. The Amazon S3 bucket is used by a Jupyter SageMaker notebook instance to train your model before it is deployed. You can use the `SELECT INTO OUTFILE S3` statement to query data from an Aurora MySQL DB cluster and save it directly into text files stored in an Amazon S3 bucket. Then the notebook instance consumes the data from the Amazon S3 bucket for training.

Aurora Machine Learning extends the existing `SELECT INTO OUTFILE` syntax in Aurora MySQL to export data to CSV format. The generated CSV file can be directly consumed by models that need this format for training purposes.

```
SELECT * INTO OUTFILE S3 's3_uri' [FORMAT {CSV|TEXT} [HEADER]] FROM table_name;
```

The extension supports the standard CSV format.

- **Format TEXT** is the same as the existing MySQL export format. This is the default format.
- **Format CSV** is a newly introduced format that follows the specification in RFC-4180.
• If you specify the optional keyword HEADER, the output file contains one header line. The labels in the header line correspond to the column names from the SELECT statement.

• You can still use the keywords CSV and HEADER as identifiers.

The extended syntax and grammar of SELECT INTO is now as follows:

```
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']
]
```

Using SageMaker to run your own ML models

SageMaker is a fully managed machine learning service. With SageMaker, data scientists and developers can quickly and easily build and train machine learning models. Then they can directly deploy the models into a production-ready hosted environment. SageMaker provides an integrated Jupyter authoring notebook instance for easy access to your data sources. That way, you can perform exploration and analysis without managing the hardware infrastructure for servers. It also provides common machine learning algorithms that are optimized to run efficiently against extremely large datasets in a distributed environment. With native support for bring-your-own-algorithms and frameworks, SageMaker offers flexible distributed training options that adjust to your specific workflows.

Currently, Aurora Machine Learning supports any SageMaker endpoint that can read and write comma-separated value format, through a Content-Type of text/csv. The built-in SageMaker algorithms that currently accept this format are Random Cut Forest, Linear Learner, 1P, XGBoost, and 3P. If the algorithms return multiple outputs per item, the Aurora Machine Learning function returns only the first item. This first item is expected to be a representative result.

Aurora machine learning always invokes SageMaker endpoints in the same AWS Region as your Aurora cluster. Therefore, for a single-region Aurora cluster, always deploy the model in the same AWS Region as your Aurora MySQL cluster.

If you are using an Aurora global database, you set up the same integration between the services for each AWS Region that's part of the global database. In particular, make sure the following conditions are satisfied for all AWS Regions in the global database:

• Configure the appropriate IAM roles for accessing external services such as SageMaker, Amazon Comprehend, or Lambda for the global database cluster in each AWS Region.

• Ensure that all AWS Regions have the same trained SageMaker models deployed with the same endpoint names. Do so before running the CREATE FUNCTION statement for your Aurora Machine Learning function in the primary AWS Region. In a global database, all CREATE FUNCTION statements you run in the primary AWS Region are immediately run in all the secondary regions also.

To use models deployed in SageMaker for inference, you create user-defined functions using the familiar MySQL data definition language (DDL) statements for stored functions. Each stored function represents the SageMaker endpoint hosting the model. When you define such a function, you specify the input parameters to the model, the specific SageMaker endpoint to invoke, and the return type. The function returns the inference computed by the SageMaker endpoint after applying the model to the input parameters. All Aurora Machine Learning stored functions return numeric types or VARCHAR. You can use
any numeric type except BIT. Other types, such as JSON, BLOB, TEXT, and DATE are not allowed. Use model input parameters that are the same as the input parameters that you exported to Amazon S3 for model training.

```sql
CREATE FUNCTION function_name (arg1 type1, arg2 type2, ...) -- variable number of arguments
[DEFINER = user]
CREATE FUNCTION
  RETURNS mysql_type -- For example, INTEGER, REAL, ...
  [SQL SECURITY { DEFINER | INVOKER }] -- same as existing MySQL
  CREATE FUNCTION
  ALIAS AWS_SAGEMAKER_INVOKE_ENDPOINT   -- ALIAS replaces the stored function body. Only
  ENDPOINT NAME 'endpoint_name'
  [MAX_BATCH_SIZE max_batch_size];     -- default is 10,000
```

This is a variation of the existing CREATE FUNCTION DDL statement. In the CREATE FUNCTION statement that defines the SageMaker function, you don't specify a function body. Instead, you specify the new keyword ALIAS where the function body usually goes. Currently, Aurora Machine Learning only supports aws_sagemaker_invoke_endpoint for this extended syntax. You must specify the endpoint_name parameter. The optional parameter max_batch_size restricts the maximum number of inputs processed in an actual batched request to SageMaker. An SageMaker endpoint can have different characteristics for each model. The max_batch_size parameter can help to avoid an error caused by inputs that are too large, or to make SageMaker return a response more quickly. The max_batch_size parameter affects the size of an internal buffer used for ML request processing. Specifying too large a value for max_batch_size might cause substantial memory overhead on your DB instance.

We recommend leaving the MANIFEST setting at its default value of OFF. Although you can use the MANIFEST ON option, some SageMaker features can't directly use the CSV exported with this option. The manifest format is not compatible with the expected manifest format from SageMaker.

You create a separate stored function for each of your SageMaker models. This mapping of functions to models is required because an endpoint is associated with a specific model, and each model accepts different parameters. Using SQL types for the model inputs and the model output type helps to avoid type conversion errors passing data back and forth between the AWS services. You can control who can apply the model. You can also control the runtime characteristics by specifying a parameter representing the maximum batch size.

Currently, all Aurora Machine Learning functions have the NOT DETERMINISTIC property. If you don't specify that property explicitly, Aurora sets NOT DETERMINISTIC automatically. This requirement is because the ML model can be changed without any notification to the database. If that happens, calls to an Aurora Machine Learning function might return different results for the same input within a single transaction.

You can't use the characteristics CONTAINS SQL, NO SQL, READS SQL DATA, or MODIFIES SQL DATA in your CREATE FUNCTION statement.

Following is an example usage of invoking an SageMaker endpoint to detect anomalies. There is an SageMaker endpoint random-cut-forest-model. The corresponding model is already trained by the random-cut-forest algorithm. For each input, the model returns an anomaly score. This example shows the data points whose score is greater than 3 standard deviations (approximately the 99.9th percentile) from the mean score.

```sql
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;

**Character set requirement for SageMaker functions that return strings**

We recommend specifying a character set of `utf8mb4` as the return type for your SageMaker functions that return string values. If that isn’t practical, use a large enough string length for the return type to hold a value represented in the `utf8mb4` character set. The following example shows how to declare the `utf8mb4` character set for your function.

```sql
CREATE FUNCTION my_ml_func(...) RETURNS VARCHAR(5) CHARSET utf8mb4 ALIAS ... 
```

Currently, each SageMaker function that returns a string uses the character set `utf8mb4` for the return value. The return value uses this character set even if your ML function declares a different character set for its return type implicitly or explicitly. If your ML function declares a different character set for the return value, the returned data might be silently truncated if you store it in a table column that isn’t long enough. For example, a query with a `DISTINCT` clause creates a temporary table. Thus, the ML function result might be truncated due to the way strings are handled internally during a query.

**Using Amazon Comprehend for sentiment detection**

Amazon Comprehend uses machine learning to find insights and relationships in textual data. You can use this AWS machine learning service even if you don’t have any machine learning experience or expertise. Aurora machine learning uses Amazon Comprehend for sentiment analysis of text that is stored in your database. For example, using Amazon Comprehend you can analyze contact center call-in documents to detect sentiment and better understand caller-agent dynamics. You can find a further description in the post [Analyzing contact center calls](https://aws.amazon.com/blogs/machine-learning/analyzing-contact-center-calls/) on the AWS Machine Learning blog.

You can also combine sentiment analysis with analysis of other information in your database using a single query. For example, you can detect the average sentiment of call-in center documents for issues that combine the following:

- Open for more than 30 days.
- About a specific product or feature.
- Made by the customers who have the greatest social media influence.

Using Amazon Comprehend from Aurora Machine Learning is as easy as calling a SQL function. Aurora machine learning provides two built-in Amazon Comprehend functions, `aws_comprehend_detect_sentiment()` and `aws_comprehend_detect_sentiment_confidence()` to perform sentiment analysis through Amazon Comprehend. For each text fragment that you analyze, these functions help you to determine the sentiment and the confidence level.

```sql
-- Returns one of 'POSITIVE', 'NEGATIVE', 'NEUTRAL', 'MIXED'
aws_comprehend_detect_sentiment(
  input_text
  ,language_code
  [,max_batch_size]  -- default is 25. should be greater than 0
)

-- Returns a double value that indicates confidence of the result of
aws_comprehend_detect_sentiment.
aws_comprehend_detect_sentiment_confidence(
  input_text
  ,language_code
  [,max_batch_size]  -- default is 25. should be greater than 0.
) 
```
The `max_batch_size` helps you to tune the performance of the Amazon Comprehend function calls. A large batch size trades off faster performance for greater memory usage on the Aurora cluster. For more information, see Performance considerations for Aurora Machine Learning (p. 837).

For information about parameters and return types for the sentiment detection functions in Amazon Comprehend, see DetectSentiment

A typical Amazon Comprehend query looks for rows where the sentiment is a certain value, with a confidence level greater than a certain number. For example, the following query shows how you can determine the average sentiment of documents in your database. The query considers only documents where the confidence of the assessment is at least 80%.

```sql
SELECT AVG(CASE awc.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
    awc.detect_sentiment_confidence(productTable.document, 'en') >= 0.80;
```

**Note**

Amazon Comprehend is currently available only in some AWS Regions. To check in which AWS Regions you can use Amazon Comprehend, see the AWS Region table page.

Performance considerations for Aurora Machine Learning

Most of the work in an Aurora Machine Learning function call happens within the external ML service. This separation enables you to scale the resources for the machine learning service independent of your Aurora cluster. Within Aurora, you mostly focus on making the function calls themselves as efficient as possible.

**Query cache**

The Aurora MySQL query cache doesn't work for ML functions. Aurora MySQL doesn't store query results in the query cache for any SQL statements that call ML functions.

**Batch optimization for Aurora Machine Learning function calls**

The main Aurora Machine Learning performance aspect that you can influence from your Aurora cluster is the batch mode setting for calls to the Aurora Machine Learning stored functions. Machine learning functions typically require substantial overhead, making it impractical to call an external service separately for each row. Aurora Machine Learning can minimize this overhead by combining the calls to the external Aurora Machine Learning service for many rows into a single batch. Aurora Machine Learning receives the responses for all the input rows, and delivers the responses, one row at a time, to the query as it runs. This optimization improves the throughput and latency of your Aurora queries without changing the results.

When you create an Aurora stored function that's connected to an SageMaker endpoint, you define the batch size parameter. This parameter influences how many rows are transferred for every underlying call to SageMaker. For queries that process large numbers of rows, the overhead to make a separate SageMaker call for each row can be substantial. The larger the data set processed by the stored procedure, the larger you can make the batch size.

If the batch mode optimization can be applied to an SageMaker function, you can tell by checking the query plan produced by the `EXPLAIN PLAN` statement. In this case, the `extra` column in the execution plan includes `Batched machine learning`. The following example shows a call to an SageMaker function that uses batch mode.

```sql
mysql> create function anomaly_score(val real) returns real alias
    > aws_sagemaker_invoke_endpoint endpoint name 'my-rcf-model-20191126';
```
When you call one of the built-in Amazon Comprehend functions, you can control the batch size by specifying the optional `max_batch_size` parameter. This parameter restricts the maximum number of `input_text` values processed in each batch. By sending multiple items at once, it reduces the number of round trips between Aurora and Amazon Comprehend. Limiting the batch size is useful in situations such as a query with a `LIMIT` clause. By using a small value for `max_batch_size`, you can avoid invoking Amazon Comprehend more times than you have input texts.

The batch optimization for evaluating Aurora Machine Learning functions applies in the following cases:

- Function calls within the select list or the `WHERE` clause of `SELECT` statements. There are some exceptions, as described following.
- Function calls in the `VALUES` list of `INSERT` and `REPLACE` statements.
- ML functions in `SET` values in `UPDATE` statements.

```
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 ...;
```

### Monitoring Aurora Machine Learning

To monitor the performance of Aurora Machine Learning batch operations, Aurora MySQL includes several global variables that you can query as follows.

```
show status like 'Aurora_ml%';
```

You can reset these status variables by using a `FLUSH STATUS` statement. Thus, all of the figures represent totals, averages, and so on, since the last time the variable was reset.

**Aurora_ml_logical_response_cnt**

The aggregate response count that Aurora MySQL receives from the ML services across all queries run by users of the DB instance.

**Aurora_ml_actual_request_cnt**

The aggregate request count that Aurora MySQL receives from the ML services across all queries run by users of the DB instance.

**Aurora_ml_actual_response_cnt**

The aggregate response count that Aurora MySQL receives from the ML services across all queries run by users of the DB instance.
Aurora_ml_cache_hit_cnt

The aggregate internal cache hit count that Aurora MySQL receives from the ML services across all queries run by users of the DB instance.

Aurora_ml_single_request_cnt

The aggregate count of ML functions that are evaluated by non-batch mode across all queries run by users of the DB instance.

For information about monitoring the performance of the SageMaker operations called from Aurora Machine Learning functions, see Monitor Amazon SageMaker.

Limitations of Aurora Machine Learning

The following limitations apply to Aurora machine learning.

You can't use an Aurora machine learning function for a generated-always column. The same limitation applies to any Aurora MySQL stored function. Functions aren't compatible with this binary log (binlog) format. For information about generated columns, see the MySQL documentation.

The setting `--binlog-format=STATEMENT` throws an exception for calls to Aurora machine learning functions. The reason for the error is that Aurora Machine Learning considers all ML functions to be nondeterministic, and nondeterministic stored functions aren't compatible with this binlog format. For information about this binlog format, see the MySQL documentation.

Amazon Aurora MySQL lab mode

Aurora lab mode is used to enable Aurora features that are available in the current Aurora database version, but are not enabled by default. While Aurora lab mode features are not recommended for use in production DB clusters, you can use Aurora lab mode to enable these features for DB clusters in your development and test environments. For more information about Aurora features available when Aurora lab mode is enabled, see Aurora lab mode features (p. 839).

The `aurora_lab_mode` parameter is an instance-level parameter that is in the default parameter group. The parameter is set to 0 (disabled) in the default parameter group. To enable Aurora lab mode, create a custom parameter group, set the `aurora_lab_mode` parameter to 1 (enabled) in the custom parameter group, and modify one or more DB instances in your Aurora cluster to use the custom parameter group. Then connect to the appropriate instance endpoint to try the lab mode features. For information on modifying a DB parameter group, see Modifying parameters in a DB parameter group (p. 303). For information on parameter groups and Amazon Aurora, see Aurora MySQL parameters (p. 848).

Aurora lab mode features

The following table lists the Aurora features currently available when Aurora lab mode is enabled. You must enable Aurora lab mode before any of these features can be used.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Batching</td>
<td>Aurora MySQL scan batching speeds up in-memory, scan-oriented queries significantly. The feature boosts the performance of table full scans, index full scans, and index range scans by batch processing.</td>
</tr>
</tbody>
</table>
### Best practices with Amazon Aurora MySQL

This topic includes information on best practices and options for using or migrating data to an Amazon Aurora MySQL DB cluster.

**Topics**
- Determining which DB instance you are connected to (p. 840)
- Using T2 and T3 instances (p. 841)
- Invoking an AWS Lambda function (p. 842)
- Working with asynchronous key prefetch in Amazon Aurora (p. 842)
- Working with multi-threaded replication in Amazon Aurora MySQL (p. 844)
- Using Amazon Aurora to scale reads for your MySQL database (p. 844)
- Using Amazon Aurora for Disaster Recovery with your MySQL databases (p. 845)
- Migrating from MySQL to Amazon Aurora MySQL with reduced downtime (p. 845)
- Using XA transactions with Amazon Aurora MySQL (p. 845)
- Working with hash joins in Aurora MySQL (p. 845)
- Working with foreign keys in Aurora MySQL (p. 847)
- Related topics (p. 847)

**Determining which DB instance you are connected to**

To determine which DB instance in an Aurora MySQL DB cluster a connection is connected to, check the `innodb_read_only` global variable, as shown in the following example.

```sql
SHOW GLOBAL VARIABLES LIKE 'innodb_read_only';
```
The `innodb_read_only` variable is set to `ON` if you are connected to an Aurora Replica and `OFF` if you are connected to the primary instance.

This approach can be helpful if you want to add logic to your application code to balance the workload or to ensure that a write operation is using the correct connection. This technique only applies to Aurora clusters using single-master replication. For multi-master clusters, all the DB instances have the setting `innodb_read_only=OFF`.

**Using T2 and T3 instances**

Amazon Aurora MySQL instances that use the `db.t2.small` or `db.t2.medium` DB instance classes are best suited for applications that do not support a high workload for an extended amount of time. T2 instances are designed to provide moderate baseline performance and the capability to burst to significantly higher performance as required by your workload. They are intended for workloads that don't use the full CPU often or consistently, but occasionally need to burst. We recommend only using the `db.t2.small` and `db.t2.medium` DB instance classes for development and test servers, or other non-production servers. For more details on T2 instances, see **T2 instances**.

If your Aurora cluster is larger than 40 TB, don't use `db.t2` or `db.t3` instance classes.

Don't enable the MySQL Performance Schema on Amazon Aurora MySQL T2 instances. If the Performance Schema is enabled, the T2 instance might run out of memory.

When you use a T2 instance as a DB instance in an Aurora MySQL DB cluster, we recommend the following:

- If you use a T2 instance as a DB instance class in your DB cluster, then we recommend that all instances in your DB cluster use the same DB instance class. For example, if you use `db.t2.medium` for your primary instance, then we recommend that you use `db.t2.medium` for your Aurora Replicas as well.

- Monitor your CPU Credit Balance (`CPUCreditBalance`) to ensure that it is at a sustainable level. That is, CPU credits are being accumulated at the same rate as they are being used.

When you have exhausted the CPU credits for an instance, you see an immediate drop in the available CPU and an increase in the read and write latency for the instance. This situation results in a severe decrease in the overall performance of the instance.

If your CPU credit balance is not at a sustainable level, then we recommend that you modify your DB instance to use one of the supported R3 DB instance classes (scale compute).

For more information on monitoring metrics, see **Monitoring Amazon Aurora DB cluster metrics** (p. 489).

- For your Aurora MySQL DB clusters using single-master replication, monitor the replica lag (AuroraReplicaLag) between the primary instance and the Aurora Replicas.

  If an Aurora Replica runs out of CPU credits before the primary instance, the lag behind the primary instance results in the Aurora Replica frequently restarting. This result is common when an application has a heavy load of read operations distributed among Aurora Replicas in an Aurora MySQL DB cluster, at the same time that the primary instance has a minimal load of write operations.

  If you see a sustained increase in replica lag, make sure that your CPU credit balance for the Aurora Replicas in your DB cluster is not being exhausted.

  If your CPU credit balance is not at a sustainable level, then we recommend that you modify your DB instance to use one of the supported R3 DB instance classes (scale compute).

- Keep the number of inserts per transaction below 1 million for DB clusters that have binary logging enabled.

  If the DB cluster parameter group for your DB cluster has the `binlog_format` parameter set to a value other than `OFF`, then your DB cluster might experience out-of-memory conditions if the DB
cluster receives transactions that contain over 1 million rows to insert. You can monitor the freeable memory (FreeableMemory) metric to determine if your DB cluster is running out of available memory. You then check the write operations (VolumeWriteIOPS) metric to see if a writer instance is receiving a heavy load of write operations. If this is the case, then we recommend that you update your application to limit the number of inserts in a transaction to less than 1 million. Alternatively, you can modify your instance to use one of the supported R3 DB instance classes (scale compute).

Invoking an AWS Lambda function

If you are using Amazon Aurora version 1.16 or later, we recommend using the native functions lambda_sync and lambda_async to invoke Lambda functions.

If you are using the deprecated mysql.lambda_async procedure, we recommend that you wrap calls to the mysql.lambda_async procedure in a stored procedure. You can call this stored procedure from different sources, such as triggers or client code. This approach can help to avoid impedance mismatch issues and make it easier for your database programmers to invoke Lambda functions.

For more information on invoking Lambda functions from Amazon Aurora, see Invoking a Lambda function from an Amazon Aurora MySQL DB cluster (p. 818).

Working with asynchronous key prefetch in Amazon Aurora

**Note**
The asynchronous key prefetch (AKP) feature is available for Amazon Aurora MySQL version 1.15 and later. For more information about Aurora MySQL versions, see Database engine updates for Amazon Aurora MySQL (p. 874).

Amazon Aurora can use AKP to improve the performance of queries that join tables across indexes. This feature improves performance by anticipating the rows needed to run queries in which a JOIN query requires use of the Batched Key Access (BKA) Join algorithm and Multi-Range Read (MRR) optimization features. For more information about BKA and MRR, see Block nested-loop and batched key access joins and Multi-range read optimization in the MySQL documentation.

To take advantage of the AKP feature, a query must use both BKA and MRR. Typically, such a query occurs when the JOIN clause of a query uses a secondary index, but also needs some columns from the primary index. For example, you can use AKP when a JOIN clause represents an equijoin on index values between a small outer and large inner table, and the index is highly selective on the larger table.

AKP works in concert with BKA and MRR to perform a secondary to primary index lookup during the evaluation of the JOIN clause. AKP identifies the rows required to run the query during the evaluation of the JOIN clause. It then uses a background thread to asynchronously load the pages containing those rows into memory before running the query.

Enabling asynchronous key prefetch

You can enable the AKP feature by setting aurora_use_key_prefetch, a MySQL server variable, to on. By default, this value is set to on. However, AKP cannot be enabled until you also enable the BKA Join algorithm and disable cost-based MRR functionality. To do so, you must set the following values for optimizer_switch, a MySQL server variable:

- Set batched_key_access to on. This value controls the use of the BKA Join algorithm. By default, this value is set to off.
- Set mrr_cost_based to off. This value controls the use of cost-based MRR functionality. By default, this value is set to on.
Currently, you can set these values only at the session level. The following example illustrates how to set these values to enable AKP for the current session by executing SET statements.

```sql
mysql> set @@session.aurora_use_key_prefetch=on;
mysql> set @@session.optimizer_switch='batched_key_access=on,mrr_cost_based=off';
```

Similarly, you can use SET statements to disable AKP and the BKA Join algorithm and re-enable cost-based MRR functionality for the current session, as shown in the following example.

```sql
mysql> set @@session.aurora_use_key_prefetch=off;
mysql> set @@session.optimizer_switch='batched_key_access=off,mrr_cost_based=on';
```

For more information about the `batched_key_access` and `mrr_cost_based` optimizer switches, see [Switchable optimizations](#) in the MySQL documentation.

### Optimizing queries for asynchronous key prefetch

You can confirm whether a query can take advantage of the AKP feature. To do so, use the EXPLAIN statement with the EXTENDED keyword to profile the query before running it. The `EXPLAIN statement` provides information about the execution plan to use for a specified query.

In the output for the EXPLAIN statement, the `Extra` column describes additional information included with the execution plan. If the AKP feature applies to a table used in the query, this column includes one of the following values:

- Using Key Prefetching
- Using join buffer (Batched Key Access with Key Prefetching)

The following example shows use of EXPLAIN with EXTENDED to view the execution plan for a query that can take advantage of AKP.

```sql
mysql> explain extended 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'
    -> )
```
Working with multi-threaded replication in Amazon Aurora MySQL

By default, Aurora uses single-threaded replication when an Aurora MySQL DB cluster is used as a read replica for binary log replication. While Amazon Aurora doesn't prohibit multithreaded replication, Aurora MySQL has inherited several issues regarding multithreaded replication from MySQL. We recommend that you do not use multithreaded replication in production. If you do use multithreaded replication, we recommend that you test any use thoroughly.

For more information about using replication in Amazon Aurora, see Replication with Amazon Aurora (p. 57).

Using Amazon Aurora to scale reads for your MySQL database

You can use Amazon Aurora with your MySQL DB instance to take advantage of the read scaling capabilities of Amazon Aurora and expand the read workload for your MySQL DB instance. To use Aurora to read scale your MySQL DB instance, create an Aurora MySQL DB cluster and make it a read replica of your MySQL DB instance. Then connect to the Aurora MySQL cluster to process the read queries. The source database can be an Amazon RDS MySQL DB instance, or a MySQL database running external to Amazon RDS. For more information, see Using Amazon Aurora to scale reads for your MySQL database (p. 755).
Using Amazon Aurora for Disaster Recovery with your MySQL databases

You can use Amazon Aurora with your MySQL DB instance to create an offsite backup for disaster recovery. To use Aurora for disaster recovery of your MySQL DB instance, create an Amazon Aurora DB cluster and make it a read replica of your MySQL DB instance. This applies to an Amazon RDS MySQL DB instance, or a MySQL database running external to Amazon RDS.

**Important**
When you set up replication between a MySQL DB instance and an Amazon Aurora MySQL DB cluster, you should monitor the replication to ensure that it remains healthy and repair it if necessary.

For instructions on how to create an Amazon Aurora MySQL DB cluster and make it a read replica of your MySQL DB instance, follow the procedure in Using Amazon Aurora to scale reads for your MySQL database (p. 844).

### Migrating from MySQL to Amazon Aurora MySQL with reduced downtime

When importing data from a MySQL database that supports a live application to an Amazon Aurora MySQL DB cluster, you might want to reduce the time that service is interrupted while you migrate. To do so, you can use the procedure documented in Importing data to an Amazon RDS MySQL or MariaDB DB instance with reduced downtime in the Amazon Relational Database Service User Guide. This procedure can especially help if you are working with a very large database. You can use the procedure to reduce the cost of the import by minimizing the amount of data that is passed across the network to AWS.

The procedure lists steps to transfer a copy of your database data to an Amazon EC2 instance and import the data into a new Amazon RDS MySQL DB instance. Because Amazon Aurora is compatible with MySQL, you can instead use an Amazon Aurora DB cluster for the target Amazon RDS MySQL DB instance.

### Using XA transactions with Amazon Aurora MySQL

We recommend that you don't use eXtended Architecture (XA) transactions with Aurora MySQL, because they can cause long recovery times if the XA was in the `PREPARED` state. If you must use XA transactions with Aurora MySQL, follow these best practices:

- Don't leave an XA transaction open in the `PREPARED` state.
- Keep XA transactions as small as possible.

For more information about using XA transactions with MySQL, see XA transactions in the MySQL documentation.

### Working with hash joins in Aurora MySQL

When you need to join a large amount of data by using an equijoin, a hash join can improve query performance. You can enable hash joins for Aurora MySQL.

A hash join column can be any complex expression. In a hash join column, you can compare across data types in the following ways:

- You can compare anything across the category of precise numeric data types, such as `int`, `bigint`, `numeric`, and `bit`.  

845
You can compare anything across the category of approximate numeric data types, such as `float` and `double`.

You can compare items across string types if the string types have the same character set and collation.

You can compare items with date and timestamp data types if the types are the same.

**Note**
Data types in different categories cannot compare.

The following restrictions apply to hash joins for Aurora MySQL:

- Left-right outer joins are not supported.
- Semijoins such as subqueries are not supported, unless the subqueries are materialized first.
- Multiple-table updates or deletes are not supported.

**Note**
Single-table updates or deletes are supported.

- BLOB and spatial data type columns cannot be join columns in a hash join.

### Enabling hash joins

To enable hash joins, set the MySQL server variable `optimizer_switch` to `hash_join=on`. The `optimizer_switch` parameter is set to `hash_join=off` by default. The following example illustrates how to enable hash joins.

```sql
mysql> SET optimizer_switch='hash_join=on';
```

With this setting, the optimizer chooses to use a hash join based on cost, query characteristics, and resource availability. If the cost estimation is incorrect, you can force the optimizer to choose a hash join. You do so by setting `hash_join_cost_based`, a MySQL server variable, to `off`. The following example illustrates how to force the optimizer to choose a hash join.

```sql
mysql> SET optimizer_switch='hash_join_cost_based=off';
```

**Note**
Prior to Aurora MySQL version 1.22, the way to enable hash joins in Aurora MySQL version 1 is by enabling the `aurora_lab_mode` session-level setting. In those Aurora MySQL versions, the `optimizer_switch` setting for hash joins is enabled by default and you only need to enable `aurora_lab_mode`.

For Aurora MySQL version 2, hash join support is available in version 2.06 and higher. In Aurora MySQL version 2, the hash join feature is always controlled by the `optimizer_switch` value.

### Optimizing queries for hash joins

To find out whether a query can take advantage of a hash join, use the `EXPLAIN` statement to profile the query first. The `EXPLAIN` statement provides information about the execution plan to use for a specified query.

In the output for the `EXPLAIN` statement, the `Extra` column describes additional information included with the execution plan. If a hash join applies to the tables used in the query, this column includes values similar to the following:

```plaintext
• Using where; Using join buffer (Hash Join Outer table `table1_name`)
```
• Using where; Using join buffer (Hash Join Inner table table2_name)

The following example shows the use of EXPLAIN to view the execution plan for a hash join query.

```sql
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 the output, the Hash Join Inner table is the table used to build hash table, and the Hash Join Outer table is the table that is used to probe the hash table.

For more information about the extended EXPLAIN output format, see Extended EXPLAIN output format in the MySQL product documentation.

In Aurora MySQL 2.08 and higher, you can use SQL hints to influence whether a query uses hash join or not, and which tables to use for the build and probe sides of the join. For details, see Aurora MySQL hints (p. 869).

**Working with foreign keys in Aurora MySQL**

We strongly recommend that you don't run any data definition language (DDL) statements when the foreign_key_checks variable is set to 0 (off).

If you need to insert or update rows that require a transient violation of foreign keys, follow these steps:

1. Set foreign_key_checks to 0.
2. Make your data manipulation language (DML) changes.
3. Make sure that your completed changes don't violate any foreign key constraints.
4. Set foreign_key_checks to 1 (on).

In addition, follow these other best practices for foreign key constraints:

- Make sure that your client applications don't set the foreign_key_checks variable to 0 as a part of the init_connect variable.
- If a restore from a logical backup such as mysqldump fails or is incomplete, make sure that foreign_key_checks is set to 1 before starting any other operations in the same session. A logical backup sets foreign_key_checks to 0 when it starts.

**Related topics**

- Managing an Amazon Aurora DB cluster (p. 322)
Amazon Aurora MySQL reference

This reference includes information about Aurora MySQL parameters, status variables, and general SQL extensions or differences from the community MySQL database engine.

Topics

- Aurora MySQL parameters (p. 848)
- Inapplicable MySQL parameters and status variables (p. 862)
- Aurora MySQL events (p. 863)
- Aurora MySQL isolation levels (p. 865)
- Aurora MySQL hints (p. 869)
- Aurora MySQL stored procedures (p. 871)

Aurora MySQL parameters

You manage your Amazon Aurora MySQL DB cluster in the same way that you manage other Amazon RDS DB instances, by using parameters in a DB parameter group. Amazon Aurora differs from other DB engines in that you have a DB cluster that contains multiple DB instances. As a result, some of the parameters that you use to manage your Aurora MySQL DB cluster apply to the entire cluster. Other parameters apply only to a particular DB instance in the DB cluster.

To manage cluster-level parameters, you use DB cluster parameter groups. To manage instance-level parameters, you use DB parameter groups. Each DB instance in an Aurora MySQL DB cluster is compatible with the MySQL database engine. However, you apply some of the MySQL database engine parameters at the cluster level, and you manage these parameters using DB cluster parameter groups. You can’t find cluster-level parameters in the DB parameter group for an instance in an Aurora DB cluster. A list of cluster-level parameters appears later in this topic.

You can manage both cluster-level and instance-level parameters using the AWS Management Console, the AWS CLI, or the Amazon RDS API. You use separate commands for managing cluster-level parameters and instance-level parameters. For example, you can use the modify-db-cluster-parameter-group CLI command to manage cluster-level parameters in a DB cluster parameter group. You can use the modify-db-parameter-group CLI command to manage instance-level parameters in a DB parameter group for a DB instance in a DB cluster.

You can view both cluster-level and instance-level parameters in the console, or by using the CLI or RDS API. For example, you can use the describe-db-cluster-parameters AWS CLI command to view cluster-level parameters in a DB cluster parameter group. You can use the describe-db-parameters CLI command to view instance-level parameters in a DB parameter group for a DB instance in a DB cluster.

For more information on DB parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298). For rules and restrictions for Aurora Serverless clusters, see Aurora Serverless v1 and parameter groups (p. 142).

Topics

- Cluster-level parameters (p. 848)
- Instance-level parameters (p. 852)

Cluster-level parameters

The following table shows all of the parameters that apply to the entire Aurora MySQL DB cluster.
<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>aurora_binlog_read_buffer_size</td>
<td>Yes</td>
<td>Only affects clusters that use binary log (binlog) replication. For information about binlog replication, see Replication between Aura and MySQL or between Aurora and another Aurora DB cluster (binary log replication) (p. 743).</td>
</tr>
<tr>
<td>aurora_binlog_replication_max_yiel Ministers</td>
<td>Yes</td>
<td>Only affects clusters that use binary log (binlog) replication. For information about binlog replication, see Replication between Aura and MySQL or between Aurora and another Aurora DB cluster (binary log replication) (p. 743).</td>
</tr>
<tr>
<td>aurora_binlog_use_large_read_buffer</td>
<td>Yes</td>
<td>Only affects clusters that use binary log (binlog) replication. For information about binlog replication, see Replication between Aura and MySQL or between Aurora and another Aurora DB cluster (binary log replication) (p. 743).</td>
</tr>
<tr>
<td>aurora_enable_replica_log_compress</td>
<td>Yes</td>
<td>For more information, see Performance considerations for Amazon Aurora MySQL replication (p. 732). Doesn't apply to clusters that are part of an Aurora global database.</td>
</tr>
<tr>
<td>aurora_enable_repl_bin_log_filtering</td>
<td>Yes</td>
<td>For more information, see Performance considerations for Amazon Aurora MySQL replication (p. 732). Doesn't apply to clusters that are part of an Aurora global database.</td>
</tr>
<tr>
<td>aurora_enable_zdr</td>
<td>Yes</td>
<td>For more information, see High availability considerations for Amazon Aurora MySQL replication (p. 732).</td>
</tr>
<tr>
<td>aurora_load_from_s3_role</td>
<td>Yes</td>
<td>For more information, see Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804).</td>
</tr>
<tr>
<td>aurora_select_into_s3_role</td>
<td>Yes</td>
<td>For more information, see Saving data from an Amazon Aurora MySQL DB cluster into text files in an Amazon S3 bucket (p. 812).</td>
</tr>
<tr>
<td>auto_increment increment</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>auto_increment offset</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>aws_default_lambda_role</td>
<td>Yes</td>
<td>For more information, see Invoking a Lambda function from an Amazon Aurora MySQL DB cluster (p. 818).</td>
</tr>
<tr>
<td>aws_default_s3_role</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>binlog_checksum</td>
<td>Yes</td>
<td>The AWS CLI and RDS API report a value of None if this parameter isn’t set. In that case, Aurora MySQL uses the engine default value, which is CRC32. This is different than the explicit setting of NONE, which turns off the checksum. See Aurora MySQL database engine updates 2020-09-02 (version 1.23.0) (p. 932) and Aurora MySQL database engine updates 2020-03-05 (version 1.22.2) (p. 937) for a bug fix related to this parameter.</td>
</tr>
<tr>
<td>binlog_format</td>
<td>Yes</td>
<td>For more information, see Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster (binary log replication) (p. 743).</td>
</tr>
<tr>
<td>binlog_row_image</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>binlog_rows_query_log_events</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>character_set-client-handshake</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>character_set_client</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>character_set_connection</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>character_set_database</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>character_set_filesystem</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>character_set_results</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>character_set_server</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>collation_connection</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>collation_server</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>completion_type</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>default_storage_engine</td>
<td>No</td>
<td>Aurora MySQL clusters use the InnoDB storage engine for all of your data.</td>
</tr>
<tr>
<td>innodb_autoinc_lock_mode</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_checksum</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_cmp_per_index_enabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_commit_concurrency</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_data_home_dir</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don’t access the filesystem directly.</td>
</tr>
<tr>
<td>innodb_file_per_table</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_flush_log_at_trx_commit</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>innodb_ft_max_token_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_ft_min_token_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_ft_num_word_optimize</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_ft_sort_pll_degree</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_onlineAlterLogMaxSize</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_optimizeFulltextOnly</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_page_size</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_purge_batch_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_purge_threads</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb rollback_on_timeout</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb rollback_segments</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_spin_wait_delay</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_strict_mode</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_support_xa</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_sync_array_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_sync_spin_loops</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_table_locks</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_undo_directory</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>innodb_undo_logs</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_undo_tablespaces</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>lc_time_names</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>lower_case_table_names</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>master-info-repository</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>master_verify_checksum</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>require_secure_transport</td>
<td>Yes</td>
<td>For more information, see Using SSL/TLS with Aurora MySQL DB clusters (p. 638).</td>
</tr>
<tr>
<td>server_audit_events</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>server_audit_excl_users</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>server_audit_incl_users</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Parameter name

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_audit.logging</td>
<td>Yes</td>
<td>For instructions on uploading the logs to Amazon CloudWatch Logs, see <a href="#">Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs</a>.</td>
</tr>
<tr>
<td>server_id</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>skip-character-set-client-handshake</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>skip_name_resolve</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>sync_frm</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>time_zone</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>tls_version</td>
<td>Yes</td>
<td>For more information, see <a href="#">TLS versions for Aurora MySQL</a>.</td>
</tr>
</tbody>
</table>

### Instance-level parameters

The following table shows all of the parameters that apply to a specific DB instance in an Aurora MySQL DB cluster.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-suspicious-udfs</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>aurora_lab_mode</td>
<td>Yes</td>
<td>For more information, see <a href="#">Amazon Aurora MySQL lab mode</a>.</td>
</tr>
<tr>
<td>aurora_oom_response</td>
<td>Yes</td>
<td>For more information, see <a href="#">Amazon Aurora MySQL out of memory issues</a>.</td>
</tr>
<tr>
<td>aurora_parallel_query</td>
<td>Yes</td>
<td>Set to ON to enable parallel query in Aurora MySQL versions 1.23 and 2.09 or higher. The old aurora_pq parameter isn't used in these versions. For more information, see <a href="#">Working with parallel query for Amazon Aurora MySQL</a>.</td>
</tr>
<tr>
<td>aurora_pq</td>
<td>Yes</td>
<td>Set to OFF to turn off parallel query for specific DB instances in Aurora MySQL versions before 1.23 and 2.09. In 1.23 and 2.09 or higher, turn parallel query on and off with aurora_parallel_query instead. For more information, see <a href="#">Working with parallel query for Amazon Aurora MySQL</a>.</td>
</tr>
<tr>
<td>autocommit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>automatic_sp_privileges</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>back_log</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>basedir</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>binlog_cache_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>binlog_max_flush_queue_time</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>binlog_order_commits</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>binlog_stmt_cache_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>bulk_insert_buffer_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>concurrent_insert</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>connect_timeout</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>core-file</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>datadir</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>default_time_zone</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>default_tmp_storage_engine</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>default_week_format</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>delay_key_write</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>delayed_insert_limit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>delayed_insert_timeout</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>delayed_queue_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>div_precision_increment</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>end_markers_in_json</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>enforce_gtid_consistency</td>
<td>Sometimes</td>
<td>Modifiable in Aurora MySQL version 2.04 and later.</td>
</tr>
<tr>
<td>eq_range_index_dive_limit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>event_scheduler</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>explicit_defaults_for_timestamp</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>flush</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>flush_time</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ft_boolean_syntax</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>ft_max_word_len</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ft_min_word_len</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ft_query_expansion_limit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ft_stopword_file</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>general_log</td>
<td>Yes</td>
<td>For instructions on uploading the logs to CloudWatch Logs, see Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs (p. 824).</td>
</tr>
<tr>
<td>general_log_file</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>group_concat_max_len</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>gtid-mode</td>
<td>Sometimes</td>
<td>Modifiable in Aurora MySQL version 2.04 and later.</td>
</tr>
<tr>
<td>host_cache_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>init_connect</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_adaptive_hash_index</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_adaptive_max_sleep_delay</td>
<td>Yes</td>
<td>Modifying this parameter has no effect, because innodb_thread_concurrency is always 0 for Aurora.</td>
</tr>
<tr>
<td>innodb_autoextend_increment</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_buffer_pool_dump_at_shutdown</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_buffer_pool_dump_now</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_buffer_pool_filename</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_buffer_pool_load_abort</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_buffer_pool_load_at_startup</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_buffer_pool_load_now</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_buffer_pool_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_change_buffer_max_size</td>
<td>No</td>
<td>Aurora MySQL doesn't use the InnoDB change buffer at all.</td>
</tr>
<tr>
<td>innodb_compression_failure_threshold</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_compression_level</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_compression_pad_pct_max</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_concurrency_tickets</td>
<td>Yes</td>
<td>Modifying this parameter has no effect, because innodb_thread_concurrency is always 0 for Aurora.</td>
</tr>
<tr>
<td>innodb_file_format</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Amazon Aurora User Guide for Aurora

**Parameters**

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>innodb_flush_log_at_timeout</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodbflushing_avg_loops</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_force_load_corrupted</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_ft_aux_table</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_ft_cache_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_ft_enable_stopword</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_ft_server_stopword_table</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_ft_user_stopword_table</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_large_prefix</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_lock_wait_timeout</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_log_compressed_pages</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_lru_scan_depth</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_max_purge_lag</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_max_purge_lag_delay</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_monitor_disable</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_monitor_enable</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_monitor_reset</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_monitor_reset_all</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_old_blocks_pct</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_old_blocks_time</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_open_files</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_print_all_deadlocks</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_random_read_ahead</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_read_ahead_threshold</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_read_io_threads</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>innodb_read_only</td>
<td>No</td>
<td>Aurora MySQL manages the read-only and read/write state of DB instances based on the type of cluster. For example, a provisioned cluster has one read/write DB instance (the <em>primary instance</em>) and any other instances in the cluster are read-only (the Aurora Replicas).</td>
</tr>
<tr>
<td>innodb_replication_delay</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>innodb_sort_buffer_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>innodb_stats_auto_recalc</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>innodb_stats_method</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>innodb_stats_on_metadata</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>innodb_stats_persistent</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>innodb_stats_persistent_sample_pages</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>innodb_stats_transient_sample_pages</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>innodb_thread_concurrency</code></td>
<td>No</td>
<td>Modifying this parameter has no effect, because <code>innodb_thread_concurrency</code> is always 0 for Aurora.</td>
</tr>
<tr>
<td><code>innodb_thread_sleep_delay</code></td>
<td>Yes</td>
<td>Modifying this parameter has no effect, because <code>innodb_thread_concurrency</code> is always 0 for Aurora.</td>
</tr>
<tr>
<td><code>interactive_timeout</code></td>
<td>Yes</td>
<td>Aurora evaluates the minimum value of <code>interactive_timeout</code> and <code>wait_timeout</code>, then uses that minimum as the timeout to end all idle sessions, both interactive and noninteractive.</td>
</tr>
<tr>
<td><code>join_buffer_size</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>keep_files_on_create</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>key_buffer_size</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>key_cache_age_threshold</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>key_cache_block_size</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>key_cache_division_limit</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>local_infile</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>lock_wait_timeout</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>log-bin</code></td>
<td>No</td>
<td>Setting <code>binlog_format</code> to <code>STATEMENT</code>, <code>MIXED</code>, or <code>ROW</code> automatically sets <code>log-bin</code> to <code>ON</code>. Setting <code>binlog_format</code> to <code>OFF</code> automatically sets <code>log-bin</code> to <code>OFF</code>. For more information, see Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster (binary log replication) (p. 743).</td>
</tr>
<tr>
<td><code>log_bin_trust_function_creators</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>log_bin_use_v1_row_events</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>log_error</code></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td><code>log_output</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>log_queries_not_using_indexes</code></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><code>log_slave_updates</code></td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>log_throttle_queries_not_using_indexes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>log_warnings</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>long_query_time</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>low_priority_updates</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_allowed_packet</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_binlog_cache_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_binlog_size</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>max_binlog_stmt_cache_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_connect_errors</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_connections</td>
<td>Yes</td>
<td>For more information, see Maximum connections to an Aurora MySQL DB instance (p. 675).</td>
</tr>
<tr>
<td>max_delayed_threads</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_error_count</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_heap_table_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_insert_delayed_threads</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_join_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_length_for_sort_data</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_prepared_stmt_count</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_seeks_for_key</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_sort_length</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_sp_recursion_depth</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_tmp_tables</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_user_connections</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>max_write_lock_count</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>metadata_locks_cache_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>min_examined_row_limit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>myisam_data_pointer_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>myisam_max_sort_file_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>myisam_mmap_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>myisam_sort_buffer_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>myisam_stats_method</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>myisam_use_mmap</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>net_buffer_length</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>net_read_timeout</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>net_retry_count</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>net_write_timeout</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>old-style-user-limits</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>old_passwords</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>optimizer_prune_level</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>optimizer_search_depth</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>optimizer_switch</td>
<td>Yes</td>
<td>For information about Aurora MySQL features that use this switch, see Best practices with Amazon Aurora MySQL (p. 840).</td>
</tr>
<tr>
<td>optimizer_trace</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>optimizer_trace_features</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>optimizer_trace_limit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>optimizer_trace_max_mem_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>optimizer_trace_offset</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance-schema-consumer-events-waits-current</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance-schema-instrument</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_accounts_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_consumer_global_instrumentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance_schema_consumer_thread_instrumentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance_schema_consumer_events_stages_current</td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance_schema_consumer_events_statements_current</td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance_schema_consumer_events_statements_history</td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance_schema_consumer_events_statements_history_long</td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance_schema_consumer_events_waits_history</td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance_schema_consumer_events_waits_history_long</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

858
<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>performance_schema_consumer_statements_digest</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_digests_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_events_stages_history_long_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_events_stages_history</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_events_statements_history_long_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_events_statements_history</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_events_transactions_history_long_size</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_events_transactions_history</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_events_waits_history_long_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_events_waits_history</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_hosts_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_cond_classes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_cond_instances</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_digest_length</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_file_classes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_file_handles</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_file_instances</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_index_stat</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_max_memory_classes</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_max_metadata_locks</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_max_mutex_classes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_mutex_instances</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_prepared_statements_instances</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_max_program_instances</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_max_rwlock_classes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_rwlock_instances</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_socket_classes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_socket_instances</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_sql_text_length</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_max_stage_classes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_statement_classes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>performance_schema_max_statement_stack</td>
<td>Yes</td>
<td>Aurora MySQL 2.x only</td>
</tr>
<tr>
<td>performance_schema_max_table_handles</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_table_instances</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_table_lock_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_thread_classes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_max_thread_instances</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_session_connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance_schema_setup_actors_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_setup_objects_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>performance_schema_users_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>pid_file</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>plugin_dir</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>port</td>
<td>No</td>
<td>Aurora MySQL manages the connection properties and enforces consistent settings for all DB instances in a cluster.</td>
</tr>
<tr>
<td>preload_buffer_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>profiling_history_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>query_alloc_block_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>query_cache_limit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>query_cache_min_res_unit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>query_cache_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>query_cache_type</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>query_cache_wlock_invalidate</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>query_prealloc_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>range_alloc_block_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>read_buffer_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>read_only</td>
<td>No</td>
<td>Aurora MySQL manages the read-only and read/write state of DB instances based on the type of cluster. For example, a provisioned cluster has one read/write DB instance (the primary instance) and any other instances in the cluster are read-only (the Aurora Replicas).</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>read_rnd_buffer_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>relay-log</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>relay_log_info_repository</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>relay_log_recovery</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>safe-user-create</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>secure_auth</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>secure_file_priv</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>skip-slave-start</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>skip_external_locking</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>skip_show_database</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>slave_checkpoint_group</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>slave_checkpoint_period</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>slave_parallel_workers</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>slave_pending_jobs_size_max</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>slave_sql_verify_checksum</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>slow_launch_time</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>slow_query_log</td>
<td>Yes</td>
<td>For instructions on uploading the logs to CloudWatch Logs, see Publishing Amazon Aurora MySQL logs to Amazon CloudWatch Logs (p. 824).</td>
</tr>
<tr>
<td>slow_query_log_file</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>socket</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>sort_buffer_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>sql_mode</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>sql_select_limit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>stored_program_cache</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>sync_binlog</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>sync_master_info</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>sync_relay_log</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>sync_relay_log_info</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Inapplicable MySQL parameters and status variables

Because of architectural differences between Aurora MySQL and MySQL, some MySQL parameters and status variables don't apply to Aurora MySQL.

The following MySQL parameters don't apply to Aurora MySQL:

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysdate-is-now</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>table_cache_element_entry_ttl</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>table_definition_cache</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>table_open_cache</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>table_open_cache_instances</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>temp_pool</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>thread_handling</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>thread_stack</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>timed_mutexes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>tmp_table_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>tmpdir</td>
<td>No</td>
<td>Aurora MySQL uses managed instances where you don't access the filesystem directly.</td>
</tr>
<tr>
<td>transaction_alloc_block_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>transaction_prealloc_size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>tx_isolation</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>updatable_views_with_limit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>validate_password</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>validate_password_dictionary_file</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>validate_password_length</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>validate_password_mixed_case_count</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>validate_password_number_count</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>validate_password_policy</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>validate_password_special_char_count</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>wait_timeout</td>
<td>Yes</td>
<td>Aurora evaluates the minimum value of interactive_timeout and wait_timeout, then uses that minimum as the timeout to end all idle sessions, both interactive and noninteractive.</td>
</tr>
</tbody>
</table>

Inapplicable MySQL parameters and status variables
• `innodb_adaptive_flushing`
• `innodb_adaptive_flushing_lwm`
• `innodb_change_buffering`
• `innodb_checksum_algorithm`
• `innodb_doublewrite`
• `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_max_dirty_pages_pct`
• `innodb_use_native_aio`
• `innodb_write_io_threads`
• `thread_cache_size`

The following MySQL status variables don't apply to Aurora MySQL:

• `innodb_buffer_pool_bytes_dirty`
• `innodb_buffer_pool_pages_dirty`
• `innodb_buffer_pool_pages_flushed`

**Note**
These lists are not exhaustive.

### Aurora MySQL events

The following are some common wait events for Aurora MySQL.

**Note**

**io/aurora_redo_log_flush**

In this wait event, a session is writing data to Aurora storage. Typically, this wait event is for a write I/O operation in Aurora MySQL.

**io/aurora_respond_to_client**

In this wait event, a thread is in the process of returning the result set to the client.

**io/file/csv/data**

In this wait event, there are threads writing to tables in comma-separated value (CSV) format. Check your CSV table usage. A typical cause of this event is setting `log_output` on a table.

**io/file/innodb/innodb_data_file**

In this wait event, there are threads waiting on I/O operations to storage. This event is more prevalent in I/O intensive workloads. SQL statements showing a comparatively large proportion of this wait event might be running disk intensive queries. Or they might be requesting data that can't be satisfied from the InnoDB buffer pool. To find out, check your query plans and cache hit ratios. For more information, see [Buffering and caching](https://dev.mysql.com/doc/refman/8.0/en/buffering.html) in the MySQL documentation.
**io/file/sql/binlog**

In this wait event, there is a thread waiting on a binlog file that is being written to disk.

**io/socket/sql/client_connection**

In this wait event, a thread is in the process of handling a new connection.

**io/table/sql/handler**

This is a table I/O wait event. Typically, these types of events can be followed by a nested event such as a file I/O event. For more information about 'atom' and 'molecule' events in the Performance Schema, see [Performance Schema atom and molecule events](https://dev.mysql.com/doc/refman/8.0/en/perfschema-atom-molecule-events.html) in the MySQL documentation.

**lock/table/sql/handler**

This wait event is a table lock wait event handler. For more information about 'atom' and 'molecule' events in the Performance Schema, see [Performance Schema atom and molecule events](https://dev.mysql.com/doc/refman/8.0/en/perfschema-atom-molecule-events.html) in the MySQL documentation.

**synch/cond/mysys/my_thread_var::suspend**

In this wait event, threads are suspended when they are waiting on a condition. For example, this event occurs when threads are waiting for table level lock. We recommend that you investigate your workload to see what threads might be acquiring table locks on your DB instance. For more information about table locking in MySQL, see [Table locking issues](https://dev.mysql.com/doc/refman/8.0/en/lock-tables.html) in the MySQL documentation.

**synch/cond/sql/MDL_context::COND_wait_status**

In this wait event, there are threads waiting on a table metadata lock. For more information, see [Optimizing locking operations](https://dev.mysql.com/doc/refman/8.0/en/lock-tables.html) in the MySQL documentation.

**synch/cond/sql/MYSQL_BIN_LOG::COND_done**

In this wait event, there is a thread waiting on a binlog file that is being written to disk. Binary logging contention can occur on databases with a very high change rate.

**synch/mutex/innodb/aurora_lock_thread_slot_futex**

In this wait event, there is a thread that is waiting on an InnoDB record lock. If you see this event, check your database for conflicting workloads. For more information, see [InnoDB locking](https://dev.mysql.com/doc/refman/8.0/en/innoDB-locking.html) in the MySQL documentation.

**synch/mutex/innodb/buf_pool_mutex**

In this wait event, a thread has acquired a lock on the InnoDB buffer pool.

**synch/mutex/sql/LOCK_open**

In this wait event, LOCK_open is being used to protect various objects in the data dictionary. This wait event indicates that there are threads waiting to acquire these locks. Typically, this event is caused by data dictionary contention.

**synch/mutex/sql/LOCK_table_cache**

In this wait event, there are threads waiting to acquire a lock on a table cache instance. For more information, see [How MySQL opens and closes tables](https://dev.mysql.com/doc/refman/8.0/en/innodb-locking-summary.html) in the MySQL documentation.

**synch/mutex/sql/LOG**

In this wait event, there are threads waiting on a log lock. For example, a thread might wait for a lock to write to the slow query log file.

**synch/mutex/sql/MYSQL_BIN_LOG::LOCK_commit**

In this wait event, there is a thread that is waiting to acquire a lock with the intention of committing to the binary log. Binary logging contention can occur on databases with a very high change rate. Depending on your version of MySQL, there are certain locks being used to protect the consistency and durability of the binary log. In RDS MySQL, binary logs are used for replication and the...
Aurora MySQL isolation levels

Following, you can learn how DB instances in an Aurora MySQL cluster implement the database property of isolation. Doing so helps you understand how the Aurora MySQL default behavior balances between strict consistency and high performance. You can also decide when to change the default settings based on the characteristics of your workload.

**Available isolation levels for writer instances**

You can use the isolation levels REPEATABLE READ, READ COMMITTED, READ UNCOMMITTED, and SERIALIZABLE on the primary instance of an Aurora MySQL single-master cluster, or any DB instance in an Aurora MySQL multi-master cluster. These isolation levels work the same in Aurora MySQL as in RDS MySQL.

**REPEATABLE READ isolation level for reader instances**

By default, Aurora MySQL DB instances configured as read-only Aurora Replicas always use the REPEATABLE READ isolation level. These DB instances ignore any SET TRANSACTION ISOLATION LEVEL statements and continue using the REPEATABLE READ isolation level.

**READ COMMITTED isolation level for reader instances**

If your application includes a write-intensive workload on the primary instance and long-running queries on the Aurora Replicas, you might experience substantial purge lag. Purge lag happens when internal garbage collection is blocked by long-running queries. The symptom that you see is a high value for history list length in output from the SHOW ENGINE INNODB STATUS command. You can monitor this value using the RollbackSegmentHistoryListLength metric in CloudWatch. This condition can reduce the effectiveness of secondary indexes and lead to reduced overall query performance and wasted storage space.

If you experience such issues, you can use an Aurora MySQL session-level configuration setting, aurora_read_replica_read_committed, to use the READ COMMITTED isolation level on Aurora Replicas. Using this setting can help reduce slowdowns and wasted space that can result from performing long-running queries at the same time as transactions that modify your tables.

We recommend making sure that you understand the specific Aurora MySQL behavior of the READ COMMITTED isolation before using this setting. The Aurora Replica READ COMMITTED behavior
complies with the ANSI SQL standard. However, the isolation is less strict than typical MySQL READ COMMITTED behavior that you might be familiar with. Thus, you might see different query results under READ COMMITTED on an Aurora MySQL read replica than for the same query under READ COMMITTED on the Aurora MySQL primary instance or on Amazon RDS MySQL. You might use the aurora_read_replica_read_committed setting for such use cases as a comprehensive report that scans a very large database. You might avoid it for short queries with small result sets, where precision and repeatability are important.

The READ COMMITTED isolation level isn’t available for sessions within a secondary cluster in an Aurora global database that use the write forwarding feature. For information about write forwarding, see Using write forwarding in an Amazon Aurora global database (p. 233).

Enabling READ COMMITTED for readers

To enable the READ COMMITTED isolation level for Aurora Replicas, enable the aurora_read_replica_read_committed configuration setting. Enable this setting at the session level while connected a specific Aurora Replica. To do so, run the following SQL commands.

```
set session aurora_read_replica_read_committed = ON;
set session transaction isolation level read committed;
```

You might enable this configuration setting temporarily to perform interactive ad hoc (one-time) queries. You might also want to run a reporting or data analysis application that benefits from the READ COMMITTED isolation level, while leaving the default unchanged for other applications.

When the aurora_read_replica_read_committed setting is enabled, use the SET TRANSACTION ISOLATION LEVEL command to specify the isolation level for the appropriate transactions.

```
set transaction isolation level read committed;
```

Differences in READ COMMITTED behavior on Aurora replicas

The aurora_read_replica_read_committed setting makes the READ COMMITTED isolation level available for an Aurora Replica, with consistency behavior that is optimized for long-running transactions. The READ COMMITTED isolation level on Aurora Replicas has less strict isolation than on Aurora primary instances or multi-master instances. For that reason, enable this setting only on Aurora Replicas where you know that your queries can accept the possibility of certain types of inconsistent results.

Your queries can experience certain kinds of read anomalies when the aurora_read_replica_read_committed setting is turned on. Two kinds of anomalies are especially important to understand and handle in your application code. A non-repeatable read occurs when another transaction commits while your query is running. A long-running query can see different data at the start of the query than it sees at the end. A phantom read occurs when other transactions cause existing rows to be reorganized while your query is running, and one or more rows are read twice by your query.

Your queries might experience inconsistent row counts as a result of phantom reads. Your queries might also return incomplete or inconsistent results due to non-repeatable reads. For example, suppose that a join operation refers to tables that are concurrently modified by SQL statements such as INSERT or DELETE. In this case, the join query might read a row from one table but not the corresponding row from another table.

The ANSI SQL standard allows both of these behaviors for the READ COMMITTED isolation level. However, those behaviors are different than the typical MySQL implementation of READ COMMITTED. Thus, before enabling the aurora_read_replica_read_committed setting, check any existing SQL code to verify if it operates as expected under the looser consistency model.
Row counts and other results might not be strongly consistent under the READ COMMITTED isolation level while this setting is enabled. Thus, you typically enable the setting only while running analytic queries that aggregate large amounts of data and don't require absolute precision. If you don't have these kinds of long-running queries alongside a write-intensive workload, you probably don't need the aurora_read_replica_read_committed setting. Without the combination of long-running queries and a write-intensive workload, you're unlikely to encounter issues with the length of the history list.

### Example Queries showing isolation behavior for READ COMMITTED on Aurora replicas

The following example shows how READ COMMITTED queries on an Aurora Replica might return non-repeatable results if transactions modify the associated tables at the same time. The table BIG_TABLE contains 1 million rows before any queries start. Other data manipulation language (DML) statements add, remove, or change rows while the are running.

The queries on the Aurora primary instance under the READ COMMITTED isolation level produce predictable results. However, the overhead of keeping the consistent read view for the lifetime of every long-running query can lead to expensive garbage collection later.

The queries on the Aurora Replica under the READ COMMITTED isolation level are optimized to minimize this garbage collection overhead. The tradeoff is that the results might vary depending on whether the queries retrieve rows that are added, removed, or reorganized by transactions that commit while the query is running. The queries are allowed to consider these rows but aren't required to. For demonstration purposes, the queries check only the number of rows in the table by using the COUNT(*) function.

<table>
<thead>
<tr>
<th>Time</th>
<th>DML statement on Aurora primary instance</th>
<th>Query on Aurora primary instance with READ COMMITTED</th>
<th>Query on Aurora replica with READ COMMITTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>INSERT INTO big_table SELECT * FROM other_table LIMIT 1000000; COMMIT;</td>
<td>Q1: SELECT COUNT(*) FROM big_table;</td>
<td>Q2: SELECT COUNT(*) FROM big_table;</td>
</tr>
<tr>
<td>T2</td>
<td>INSERT INTO big_table (c1, c2) VALUES (1, 'one more row'); COMMIT;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3</td>
<td>If Q1 finishes now, result is 1,000,000.</td>
<td>If Q2 finishes now, result is 1,000,000 or 1,000,001.</td>
<td></td>
</tr>
<tr>
<td>T4</td>
<td>DELETE FROM big_table LIMIT 2; COMMIT;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T5</td>
<td>UPDATE big_table SET c2 =</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If the queries finish quickly, before any other transactions perform DML statements and commit, the results are predictable and the same between the primary instance and the Aurora Replica.

The results for Q1 are highly predictable, because `READ COMMITTED` on the primary instance uses a strong consistency model similar to the `REPEATABLE READ` isolation level.

The results for Q2 might vary depending on what transactions commit while that query is running. For example, suppose that other transactions perform DML statements and commit while the queries are running. In this case, the query on the Aurora Replica with the `READ COMMITTED` isolation level might or might not take the changes into account. The row counts are not predictable in the same way as under the `REPEATABLE READ` isolation level. They also aren't as predictable as queries running under the `READ COMMITTED` isolation level on the primary instance, or on an RDS MySQL instance.

The `UPDATE` statement at T7 doesn't actually change the number of rows in the table. However, by changing the length of a variable-length column, this statement can cause rows to be reorganized internally. A long-running `READ COMMITTED` transaction might see the old version of a row, and later within the same query see the new version of the same row. The query can also skip both the old and new versions of the row. Thus, the row count might be different than expected.

The results of Q5 and Q6 might be identical or slightly different. Query Q6 on the Aurora Replica under `READ COMMITTED` is able to see, but is not required to see, the new rows that are committed while the query is running. It might also see the row from one table but not from the other table. If the join query

<table>
<thead>
<tr>
<th>Time</th>
<th>DML statement on Aurora primary instance</th>
<th>Query on Aurora primary instance with READ COMMITTED</th>
<th>Query on Aurora replica with READ COMMITTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>T8</td>
<td>CONCAT(c2,c2,c2); COMMIT;</td>
<td>If Q1 finishes now, result is 1,000,000.</td>
<td>If Q2 finishes now, result is 1,000,000 or 1,000,001 or 999,999, or possibly some higher number.</td>
</tr>
<tr>
<td>T9</td>
<td>Q3: SELECT COUNT(*) FROM big_table;</td>
<td>Q4: SELECT COUNT(*) FROM big_table;</td>
<td></td>
</tr>
<tr>
<td>T10</td>
<td>If Q3 finishes now, result is 999,999.</td>
<td>If Q4 finishes now, result is 999,999.</td>
<td></td>
</tr>
<tr>
<td>T11</td>
<td>Q5: SELECT COUNT(<em>) FROM parent_table p JOIN child_table c ON (p.id = c.id) WHERE p.id = 1000; Q6: SELECT COUNT(</em>) FROM parent_table p JOIN child_table c ON (p.id = c.id) WHERE p.id = 1000;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T12</td>
<td>INSERT INTO parent_table (id, s) VALUES (1000, 'hello'); INSERT INTO child_table (id, s) VALUES (1000, 'world'); COMMIT;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T13</td>
<td>If Q5 finishes now, result is 0.</td>
<td>If Q6 finishes now, result is 0 or 1.</td>
<td></td>
</tr>
</tbody>
</table>
doesn't find a matching row in both tables, it returns a count of zero. If the query does find both the new rows in `PARENT_TABLE` and `CHILD_TABLE`, the query returns a count of one. In a long-running query, the lookups from the joined tables might happen at widely separated times.

**Note**
These differences in behavior depend on the timing of when transactions are committed and when the queries process the underlying table rows. Thus, you're most likely to see such differences in report queries that take minutes or hours and that run on Aurora clusters processing OLTP transactions at the same time. These are the kinds of mixed workloads that benefit the most from the `READ COMMITTED` isolation level on Aurora Replicas.

**Aurora MySQL hints**

You can use SQL hints with Aurora MySQL queries to fine-tune performance. You can also use hints to prevent execution plans for important queries to change based on unpredictable conditions.

**Tip**
To verify the effect that a hint has on a query, examine the query plan produced by the `EXPLAIN` statement. Compare the query plans with and without the hint.

The following hints apply to queries that use the hash join feature. These hints are available in Aurora MySQL 2.08 and higher.

**HASH_JOIN, NO_HASH_JOIN**

Turns on or off the ability of the optimizer to choose whether to use the hash join optimization method for a query. `HASH_JOIN` enables the optimizer to use hash join if that mechanism is more efficient. `NO_HASH_JOIN` prevents the optimizer from using hash join for the query. This hint is available in Aurora MySQL 2.08 and higher.

The following examples show how to use this hint.

```sql
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**

In a hash join query, specifies whether or not to use the specified table for the probe side of the join. The query tests whether column values from the build table exist in the probe table, instead of reading the entire contents of the probe table. You can use `HASH_JOIN_PROBING` and `HASH_JOIN_BUILDING` to specify how hash join queries are processed without reordering the tables within the query text. This hint is available in Aurora MySQL 2.08 and higher.

The following examples show how to use this hint. Specifying the `HASH_JOIN_PROBING` hint for the table `T2` has the same effect as specifying `NO_HASH_JOIN_PROBING` for the table `T1`.

```sql
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**

In a hash join query, specifies whether or not to use the specified table for the build side of the join. The query processes all the rows from this table to build the list of column values to cross-reference with the other table. You can use `HASH_JOIN_PROBING` and `HASH_JOIN_BUILDING` to specify
how hash join queries are processed without reordering the tables within the query text. This hint is available in Aurora MySQL 2.08 and higher.

The following examples show how to use this hint. Specifying the HASH JOIN_BUILDING hint for the table T2 has the same effect as specifying NO_HASH_JOIN_BUILDING for the table T1.

```sql
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**

Specifies that tables in the query are joined based on the order they are listed in the query. It is especially useful with queries involving three or more tables. It is intended as a replacement for the MySQL STRAIGHT_JOIN hint. Equivalent to the MySQL JOIN_FIXED_ORDER hint. This hint is available in Aurora MySQL 2.08 and higher.

The following examples show how to use this hint.

```sql
EXPLAIN SELECT /*+ JOIN_FIXED_ORDER */ f1, f2
   FROM t1 JOIN t2 USING (id) JOIN t3 USING (id) JOIN t4 USING (id);
```

**JOIN_ORDER**

Specifies the join order for the tables in the query. It is especially useful with queries involving three or more tables. Equivalent to the MySQL JOIN_ORDER hint. This hint is available in Aurora MySQL 2.08 and higher.

The following examples show how to use this hint.

```sql
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**

Specifies the tables to put first in the join order. It is especially useful with queries involving three or more tables. Equivalent to the MySQL JOIN_PREFIX hint. This hint is available in Aurora MySQL 2.08 and higher.

The following examples show how to use this hint.

```sql
EXPLAIN SELECT /*+ JOIN_ORDER (t4, t2) */ f1, f2
   FROM t1 JOIN t2 USING (id) JOIN t3 USING (id) JOIN t4 USING (id);
```

**JOIN_SUFFIX**

Specifies the tables to put last in the join order. It is especially useful with queries involving three or more tables. Equivalent to the MySQL JOIN_SUFFIX hint. This hint is available in Aurora MySQL 2.08 and higher.

The following examples show how to use this hint.

```sql
EXPLAIN SELECT /*+ JOIN_ORDER (t1, t3) */ f1, f2
   FROM t1 JOIN t2 USING (id) JOIN t3 USING (id) JOIN t4 USING (id);
```

For information about using hash join queries, see Working with hash joins in Aurora MySQL (p. 845).
Aurora MySQL stored procedures

You can call the following stored procedures while connected to the primary instance in an Aurora MySQL cluster. These procedures control how transactions are replicated from an external database into Aurora MySQL, or from Aurora MySQL to an external database. To learn how to use replication based on global transaction identifiers (GTIDs) with Aurora MySQL, see Using GTID-based replication for Aurora MySQL (p. 762).

Topics
- `mysql.rds_set_master_auto_position` (p. 871)
- `mysql.rds_set_external_master_with_auto_position` (p. 871)
- `mysql.rds_skip_transaction_with_gtid` (p. 873)

`mysql.rds_set_master_auto_position`

Sets the replication mode to be based on either binary log file positions or on global transaction identifiers (GTIDs).

Syntax

```sql
CALL mysql.rds_set_master_auto_position (auto_position_mode);
```

Parameters

`auto_position_mode`

A value that indicates whether to use log file position replication or GTID-based replication:
- 0 – Use the replication method based on binary log file position. The default is 0.
- 1 – Use the GTID-based replication method.

Usage notes

For an Aurora MySQL DB cluster, you call this stored procedure while connected to the primary instance. The master user must run the `mysql.rds_set_master_auto_position` procedure.

For Aurora, this procedure is supported for Aurora MySQL version 2.04 and later MySQL 5.7-compatible versions. GTID-based replication isn't supported for Aurora MySQL 1.1 or 1.0.

`mysql.rds_set_external_master_with_auto_position`

Configures an Aurora MySQL primary instance to accept incoming replication from an external MySQL instance. This procedure also configures replication based on global transaction identifiers (GTIDs).

This procedure is available for both Amazon RDS MySQL and Aurora MySQL. It works differently depending on the context. When used with Aurora MySQL, this procedure doesn't configure delayed replication. This limitation is because Amazon RDS MySQL supports delayed replication but Aurora MySQL doesn't.

Syntax
CALL mysql.rds_set_external_master_with_auto_position (  
    host_name,  
    host_port,  
    replication_user_name,  
    replication_user_password,  
    ssl_encryption  
);

Parameters

host_name

The host name or IP address of the MySQL instance running external to Aurora to become the replication master.

host_port

The port used by the MySQL instance running external to Aurora to be configured as the replication master. If your network configuration includes Secure Shell (SSH) port replication that converts the port number, specify the port number that is exposed by SSH.

replication_user_name

The ID of a user with REPLICATION CLIENT and REPLICATION SLAVE permissions on the MySQL instance running external to Aurora. We recommend that you provide an account that is used solely for replication with the external instance.

replication_user_password

The password of the user ID specified in replication_user_name.

ssl_encryption

This option is not currently implemented. The default is 0.

Usage notes

For an Aurora MySQL DB cluster, you call this stored procedure while connected to the primary instance.

The master user must run the mysql.rds_set_external_master_with_auto_position procedure. The master user runs this procedure on the primary instance of an Aurora MySQL DB cluster that acts as a replication target. This can be the replication target of an external MySQL DB instance or an Aurora MySQL DB cluster.

For Aurora, this procedure is supported for Aurora MySQL version 2.04 and later MySQL 5.7-compatible versions. GTID-based replication isn't supported for Aurora MySQL 1.1 or 1.0.

Before you run mysql.rds_set_external_master_with_auto_position, configure the external MySQL DB instance to be a replication master. To connect to the external MySQL instance, specify values for replication_user_name and replication_user_password. These values must indicate a replication user that has REPLICATION CLIENT and REPLICATION SLAVE permissions on the external MySQL instance.

To configure an external MySQL instance as a replication master

1. Using the MySQL client of your choice, connect to the external MySQL instance and create a user account to be used for replication. The following is an example.

   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
2. On the external MySQL instance, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. The following example grants REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the ‘repl_user’ user for your domain.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
IDENTIFIED BY 'SomePassW0rd'
```

When you call `mysql.rds_set_external_master_with_auto_position`, Amazon RDS records certain information. This information is the time, the user, and an action of “set master” in the `mysql.rds_history` and `mysql.rds_replication_status` tables.

To skip a specific GTID-based transaction that is known to cause a problem, you can use the `mysql.rds_skip_transaction_with_gtid` stored procedure. For more information about working with GTID-based replication, see Using GTID-based replication for Aurora MySQL (p. 762).

**Examples**

When run on an Aurora primary instance, the following example configures the Aurora cluster to act as a read replica of an instance of MySQL running external to Aurora.

```
call mysql.rds_set_external_master_with_auto_position(
    'Externaldb.some.com',
    3306,
    'repl_user'@'mydomain.com',
    'SomePassW0rd');
```

### `mysql.rds_skip_transaction_with_gtid`

Skips replication of a transaction with the specified global transaction identifier (GTID) on an Aurora primary instance.

You can use this procedure for disaster recovery when a specific GTID transaction is known to cause a problem. Use this stored procedure to skip the problematic transaction. Examples of problematic transactions include transactions that disable replication, delete important data, or cause the DB instance to become unavailable.

**Syntax**

```
CALL mysql.rds_skip_transaction_with_gtid (gtid_to_skip);
```

**Parameters**

- `gtid_to_skip`

  The GTID of the replication transaction to skip.

**Usage notes**

For an Aurora MySQL DB cluster, you call this stored procedure while connected to the primary instance. The master user must run the `mysql.rds_skip_transaction_with_gtid` procedure.
For Aurora, this procedure is supported for Aurora MySQL version 2.04 and later MySQL 5.7-compatible versions. GTID-based replication isn't supported for Aurora MySQL 1.1 or 1.0.

Database engine updates for Amazon Aurora MySQL

Amazon Aurora releases updates regularly. Updates are applied to Aurora DB clusters during system maintenance windows. The timing when updates are applied depends on the region and maintenance window setting for the DB cluster, as well as the type of update.

Updates are applied to all instances in a DB cluster at the same time. An update requires a database restart on all instances in a DB cluster, so you experience 20 to 30 seconds of downtime, after which you can resume using your DB cluster or clusters. You can view or change your maintenance window settings from the AWS Management Console.

Following, you can learn how to choose the right Aurora MySQL version for your cluster, how to specify the version when you create or upgrade a cluster, and the procedures to upgrade a cluster from one version to another with minimal interruption.

Topics
- Aurora MySQL version numbers and special versions (p. 874)
- Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877)
- Database engine updates for Amazon Aurora MySQL 2.0 (p. 881)
- Database engine updates for Amazon Aurora MySQL 1.1 (p. 930)
- Database engine updates for Aurora MySQL Serverless clusters (p. 977)
- MySQL bugs fixed by Aurora MySQL database engine updates (p. 979)
- Security vulnerabilities fixed in Amazon Aurora MySQL (p. 994)

Aurora MySQL version numbers and special versions

Although Aurora with MySQL compatibility is compatible with the MySQL database engines, Aurora MySQL includes features and bug fixes that are specific to particular Aurora MySQL versions. Application developers can check the Aurora MySQL version in their applications by using SQL. Database administrators can check and specify Aurora MySQL versions when creating or upgrading Aurora MySQL DB clusters and DB instances.

Topics
- Checking or specifying Aurora MySQL engine versions through AWS (p. 874)
- Checking Aurora MySQL versions using SQL (p. 876)
- Aurora MySQL long-term support (LTS) releases (p. 876)
- Upgrade paths between 5.6-compatible and 5.7-compatible clusters (p. 877)

Checking or specifying Aurora MySQL engine versions through AWS

When you perform administrative tasks using the AWS Management Console, AWS CLI, or RDS API, you specify the Aurora MySQL version in a descriptive alphanumeric format.

Starting with Aurora MySQL 2.03.2 and 1.19.0, Aurora engine versions have the following syntax.
The `mysql-major-version` portion is 5.6 or 5.7. This value represents the version of the client protocol and general level of MySQL feature support for the corresponding Aurora MySQL version.

The `aurora-mysql-version` is a dotted value with three parts: the Aurora MySQL major version, the Aurora MySQL minor version, and the patch level. The major version is 1 or 2, representing Aurora MySQL compatible with MySQL 5.6 or 5.7 respectively. The minor version represents the feature release within the 1.x or 2.x series. The patch level begins at 0 for each minor version, and represents the set of subsequent bug fixes that apply to the minor version. Occasionally, a new feature is incorporated into a minor version but not made visible immediately. In these cases, the feature undergoes fine-tuning and is made public in a later patch level.

All 1.x Aurora MySQL engine versions are wire-compatible with Community MySQL 5.6.10a. All 2.x Aurora MySQL engine versions are wire-compatible with Community MySQL 5.7.12.

For example, the engine versions for Aurora MySQL 2.03.2 and 1.19.0 are the following.

```
5.7.mysql_aurora.2.03.2
5.6.mysql_aurora.1.19.0
```

**Note**

There isn’t a one-to-one correspondence between community MySQL 5.6 or 5.7 versions and the Aurora MySQL 1.x and 2.x versions. To check which bug fixes and new features are in a particular Aurora MySQL release, see Database engine updates for Amazon Aurora MySQL 2.0 (p. 881) and Database engine updates for Amazon Aurora MySQL 1.1 (p. 930). For a chronological list of new features and releases, see Document history (p. 1316). To check the minimum version required for a security-related fix, see Security vulnerabilities fixed in Amazon Aurora MySQL (p. 994).

For Aurora MySQL 2.x, all versions 2.03.1 and lower are represented by the engine version 5.7.12. In the same way, all versions before 1.19.0 are represented by the engine version 5.6.10a. These older version designations don’t include the 5.7.mysql_aurora prefix. When you specified 5.7.12 or 5.6.10a while creating or modifying a cluster, you got the highest version before the 2.03.2 and 1.19.0 versions where the version numbering changed. To determine the exact version number for those older versions, you used the SQL technique explained in Checking Aurora MySQL versions using SQL (p. 876).

You specify the Aurora MySQL engine version in some AWS CLI commands and RDS API operations. For example, you specify the `--engine-version` option when you run the AWS CLI commands `create-db-cluster` and `modify-db-cluster`. You specify the `EngineVersion` parameter when you run the RDS API operations `CreateDBCluster` and `ModifyDBCluster`.

In Aurora MySQL 1.19.0 and higher or 2.03.2 and higher, the engine version in the AWS Management Console also includes the Aurora version. Upgrading the cluster changes the displayed value. This change helps you to specify and check the precise Aurora MySQL versions, without the need to connect to the cluster or run any SQL commands.

**Tip**

For Aurora clusters managed through AWS CloudFormation, this change in the `EngineVersion` setting can trigger actions by AWS CloudFormation. For information about how AWS CloudFormation treats changes to the `EngineVersion` setting, see the AWS CloudFormation documentation.

Before Aurora MySQL 1.19.0 and 2.03.2, the process to update the engine version is to use the **Apply a Pending Maintenance Action** option for the cluster. This process doesn’t change the Aurora MySQL engine version that the console displays. For example, suppose that you see an Aurora MySQL cluster with a reported engine version of 5.6.10a or 5.7.12. To find out the specific version, connect to the cluster and query the `AURORA_VERSION` system variable as described previously.
Checking Aurora MySQL versions using SQL

The Aurora version numbers that you can retrieve in your application using SQL queries use the format `<major version>.<minor version>.<patch version>`. You can get this version number for any DB instance in your Aurora MySQL cluster by querying the `AURORA_VERSION` system variable. To get this version number, use one of the following queries.

```sql
select aurora_version();
select @@aurora_version;
```

Those queries produce output similar to the following.

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

The version numbers that the console, CLI, and RDS API return by using the techniques described in Checking or specifying Aurora MySQL engine versions through AWS (p. 874) are typically more descriptive. However, for versions before 2.03.2 and 1.19, AWS always returns the version numbers 5.7.12 or 5.6.10a. For those older versions, use the SQL technique to check the precise version number.

Aurora MySQL long-term support (LTS) releases

Each new Aurora MySQL version remains available for a certain amount of time for you to use when you create or upgrade a DB cluster. After this period, you must upgrade any clusters that use that version. You can manually upgrade your cluster before the support period ends, or Aurora can automatically upgrade it for you when its Aurora MySQL version is no longer supported.

Aurora designates certain Aurora MySQL versions as long-term support (LTS) releases. DB clusters that use LTS releases can stay on the same version longer and undergo fewer upgrade cycles than clusters that use non-LTS releases. Aurora supports each LTS release for at least one year after that release becomes available. When a DB cluster that's on an LTS release is required to upgrade, Aurora upgrades it to the next LTS release. That way, the cluster doesn't need to be upgraded again for a long time.

During the lifetime of an Aurora MySQL LTS release, new patch levels introduce fixes to important issues. The patch levels don't include any new features. You can choose whether to apply such patches to DB clusters running the LTS release. For certain critical fixes, Amazon might perform a managed upgrade to a patch level within the same LTS release. Such managed upgrades are performed automatically within the cluster maintenance window.

We recommend that you upgrade to the latest release, instead of using the LTS release, for most of your Aurora MySQL clusters. Doing so takes advantage of Aurora as a managed service and gives you access to the latest features and bug fixes. The LTS releases are intended for clusters with the following characteristics:

- You can't afford downtime on your Aurora MySQL application for upgrades outside of rare occurrences for critical patches.
- The testing cycle for the cluster and associated applications takes a long time for each update to the Aurora MySQL database engine.
- The database version for your Aurora MySQL cluster has all the DB engine features and bug fixes that your application needs.
The current LTS releases for Aurora MySQL are the following:

- Aurora MySQL version 2.04.9. For more details about this version, see [Aurora MySQL database engine updates 2020-08-14 (version 2.04.9) (p. 902)](https://docs.aws.amazon.com/aurora/latest/userguide/aurora_msql_updates.html#version2049).

### Upgrade paths between 5.6-compatible and 5.7-compatible clusters

For most Aurora MySQL 1.x and 2.x versions, you can upgrade a MySQL 5.6-compatible cluster to any version of a MySQL 5.7-compatible cluster.

However, if your cluster is running Aurora MySQL 1.23 or higher, any upgrade to Aurora MySQL version 2.x must be to Aurora MySQL 2.09 or higher. This restriction applies even when you upgrade by restoring a snapshot to create a new Aurora cluster. Aurora MySQL 1.23 includes improvements in Aurora storage. For example, the maximum size of the cluster volume is larger in Aurora MySQL 1.23 and later. Aurora MySQL 2.09 is the first 2.x version that has the same storage enhancements.

### Upgrading and patching Amazon Aurora MySQL DB clusters

You can use the following methods to upgrade the minor version of a DB cluster or to patch a DB cluster:

- Upgrading Aurora MySQL by modifying the engine version (p. 877) (for Aurora MySQL 1.19.0 and higher, or 2.03.2 and higher)
- Enabling automatic upgrades between minor Aurora MySQL versions (p. 878)
- Upgrading Aurora MySQL by applying pending maintenance to an Aurora MySQL DB cluster (p. 879) (before Aurora MySQL 1.19.0 or 2.03.2)

For information about how zero-downtime patching can reduce interruptions during the upgrade process, see [Using zero-downtime patching (p. 880)](https://docs.aws.amazon.com/aurora/latest/userguide/aurora_msql_updates.html#zdp).

### Upgrading Aurora MySQL by modifying the engine version

Upgrading the minor version of an Aurora MySQL cluster applies additional fixes and new features to an existing cluster. You can do this type of upgrade for clusters that are running Amazon Aurora MySQL version 1.19.0 and higher, or 2.03.2 and higher.

This kind of upgrade applies to Aurora MySQL clusters where the original version and the upgraded version are both in the Aurora MySQL 1.x series, or both in the Aurora MySQL 2.x series. The process is fast and straightforward because it doesn't involve any conversion for the Aurora MySQL metadata or reorganization of your table data.

You perform this kind of upgrade by modifying the engine version of the DB cluster using the AWS Management Console, AWS CLI, or the RDS API. If your cluster is running Aurora MySQL 1.x, choose a higher 1.x version. If your cluster is running Aurora MySQL 2.x, choose a higher 2.x version.

### To modify the engine version of a DB cluster

- By using the console – Modify the properties of your cluster. In the Modify DB cluster window, change the Aurora MySQL engine version in the DB engine version box. If you aren't familiar with the general procedure for modifying a cluster, follow the instructions at Modifying the DB cluster by using the console, CLI, and API (p. 327).
• **By using the AWS CLI** – Call the `modify-db-cluster` AWS CLI command, and specify the name of your DB cluster for the `--db-cluster-identifier` option and the engine version for the `--engine-version` option.

  For example, to upgrade to Aurora MySQL version 2.03.2, set the `--engine-version` option to `5.7.mysql_aurora.2.03.2`. Specify the `--apply-immediately` option to immediately update the engine version for your DB cluster.

• **By using the RDS API** – Call the `ModifyDBCluster` API operation, and specify the name of your DB cluster for the `DBClusterIdentifier` parameter and the engine version for the `EngineVersion` parameter. Set the `ApplyImmediately` parameter to `true` to immediately update the engine version for your DB cluster.

### Enabling automatic upgrades between minor Aurora MySQL versions

For an Amazon Aurora MySQL DB cluster, you can specify that Aurora upgrades the DB cluster automatically to new minor versions as those versions are released. You do so by enabling the automatic minor version upgrade property of the DB cluster using the AWS Management Console, AWS CLI, or the RDS API.

The automatic upgrades occur during the maintenance window for the database.

**Important**

Until August 2020, you could specify this setting for a DB instance that was part of an Aurora MySQL DB cluster, but the setting had no effect. Now, the setting does apply to Aurora MySQL. If you have clusters created before August 2020, check whether the DB instances in the cluster already had the **Enable auto minor version upgrade** setting enabled. If so, confirm that this setting is still appropriate and change it if not. Aurora only performs the automatic upgrade if all DB instances in your cluster have this setting enabled.

Automatic minor version upgrade doesn't apply to clusters running the LTS version for Aurora MySQL 1.x or 2.x. Aurora won't automatically upgrade clusters running 2.04.9, 1.19.6, or other patch levels of those minor versions.

Automatic minor version upgrade doesn't apply to the following kinds of Aurora MySQL clusters:

- Multi-master clusters.
- Clusters that are part of an Aurora global database.
- Clusters that have cross-Region replicas.

If any of the DB instances in a cluster don't have the auto minor version upgrade setting turned on, Aurora doesn't automatically upgrade any of the instances in that cluster. Make sure to keep that setting consistent for all the DB instances in the cluster.

The outage duration varies depending on workload, cluster size, the amount of binary log data, and if Aurora can use the zero-downtime patching (ZDP) feature. Aurora restarts the database cluster, so you might experience a short period of unavailability before resuming use of your cluster. In particular, the amount of binary log data affects recovery time. The DB instance processes the binary log data during recovery. Thus, a high volume of binary log data increases recovery time.

**To enable automatic minor version upgrades for an Aurora MySQL DB cluster**

1. Follow the general procedure to modify the DB instances in your cluster, as described in [Modify a DB instance in a DB cluster](p. 328). Repeat this procedure for each DB instance in your cluster.
2. Do the following to enable automatic minor version upgrades for your cluster:
• **By using the console** – Complete the following steps:
  1. Sign in to the Amazon RDS console. Choose **Databases**, and find the DB cluster where you want to turn automatic minor version upgrade on or off.
  2. Choose each DB instance in the DB cluster that you want to modify. Apply the following change for each DB instance in sequence:
     a. Choose **Modify**.
     b. Choose the **Enable auto minor version upgrade** setting. This setting is part of the **Maintenance** section.
     c. Choose **Continue** and check the summary of modifications.
     d. (Optional) Choose **Apply immediately** to apply the changes immediately.
     e. On the confirmation page, choose **Modify DB instance**.
• **By using the AWS CLI** – Call the `modify-db-instance` AWS CLI command. Specify the name of your DB instance for the `--db-instance-identifier` option and `true` for the `--auto-minor-version-upgrade` option. Optionally, specify the `--apply-immediately` option to immediately enable this setting for your DB instance. Run a separate `modify-db-instance` command for each DB instance in the cluster.
• **By using the RDS API** – Call the `ModifyDBInstance` API operation and specify the name of your DB cluster for the `DBInstanceIdentifier` parameter and `true` for the `AutoMinorVersionUpgrade` parameter. Optionally, set the `ApplyImmediately` parameter to `true` to immediately enable this setting for your DB instance. Call a separate `ModifyDBInstance` operation for each DB instance in the cluster.

You can use a CLI command such as the following to check the status of the **Enable auto minor version upgrade** for all of the DB instances in your Aurora MySQL clusters.

```bash
aws rds describe-db-instances
   --query '*[].
   {DBClusterIdentifier:DBClusterIdentifier,DBInstanceIdentifier:DBInstanceIdentifier,AutoMinorVersionUpgrade:AutoMinorVersionUpgrade}'
```

That command produces output similar to the following.

```json
[
  {
    "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
  },
  ...
]
```

**Upgrading Aurora MySQL by applying pending maintenance to an Aurora MySQL DB cluster**

When upgrading to Aurora MySQL version 1.x versions, new database engine minor versions and patches show as an **available** maintenance upgrade for your DB cluster. You can upgrade or patch the database
version of your DB cluster by applying the available maintenance action. We recommend applying the update on a nonproduction DB cluster first, so that you can see how changes in the new version affect your instances and applications.

To apply pending maintenance actions

- **By using the console** – Complete the following steps:
  1. Sign in to the Amazon RDS console, choose Databases, and choose the DB cluster that shows the available maintenance upgrade.
  2. For Actions, choose Upgrade now to immediately update the database version for your DB cluster, or Upgrade at next window to update the database version for your DB cluster during the next DB cluster maintenance window.

- **By using the AWS CLI** – Call the `apply-pending-maintenance-action` AWS CLI command, and specify the Amazon Resource Name (ARN) for your DB cluster for the `--resource-id` option and `system-update` for the `--apply-action` option. Set the `--opt-in-type` option to immediate to immediately update the database version for your DB cluster, or `next-maintenance` to update the database version for your instance during the next cluster maintenance window.

- **By using the RDS API** – Call the `ApplyPendingMaintenanceAction` API operation, and specify the ARN for your DB cluster for the `ResourceId` parameter and `system-update` for the `ApplyAction` parameter. Set the `OptInType` parameter to `immediate` to immediately update the database version for your DB cluster, or `next-maintenance` to update the database version for your instance during the next cluster maintenance window.

For more information on how Amazon RDS manages database and operating system updates, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**

If your current Aurora MySQL version is 1.14.x but lower than 1.14.4, you can upgrade only to 1.14.4 (which supports db.r4 instance classes). Also, to upgrade from 1.14.x to a higher minor Aurora MySQL version, such as 1.17, the 1.14.x version must be 1.14.4.

### Using zero-downtime patching

The zero-downtime patching (ZDP) feature attempts, on a best-effort basis, to preserve client connections through an engine patch. If ZDP completes successfully, application sessions are preserved and the database engine restarts while patching. The database engine restart can cause a drop in throughput lasting approximately 5 seconds.

ZDP is available in Aurora MySQL 1.13 and later, compatible with MySQL 5.6. It's also available in Aurora MySQL 2.07 and later, compatible with MySQL 5.7.

ZDP might not complete successfully under the following conditions:

- Long-running queries or transactions are in progress. If Aurora can perform ZDP in this case, any open transactions are canceled.
- Binary logging is enabled or binary log replication is in-progress.
- Open Secure Socket Layer (SSL) connections exist.
- Temporary tables or table locks are in use, for example while data definition language (DDL) statements run. If Aurora can perform ZDP in this case, any open transactions are canceled.
- Pending parameter changes exist.

Starting in Aurora MySQL 1.19 and 2.07, the ZDP mechanism is improved. These improvements make ZDP more likely to succeed when there are long-running transactions, binary logging, table locks, or temporary tables.
If no suitable time window for performing ZDP becomes available because of one or more of these conditions, patching reverts to the standard behavior.

**Note**
ZDP applies only to the primary instance of a DB cluster. ZDP isn't applicable to Aurora Replicas. Prepared statements don't prevent ZDP, but they aren't preserved after ZDP completes.

### Database engine updates for Amazon Aurora MySQL 2.0

The following are Amazon Aurora 2.0 database engine updates:

- Aurora MySQL database engine updates 2020-12-11 (version 2.09.1) (p. 882)
- Aurora MySQL database engine updates 2020-09-17 (version 2.09.0) (p. 883)
- Aurora MySQL database engine updates 2020-11-12 (version 2.08.3) (p. 887)
- Aurora MySQL database engine updates 2020-08-28 (version 2.08.2) (p. 888)
- Aurora MySQL database engine updates 2020-06-18 (version 2.08.1) (p. 889)
- Aurora MySQL database engine updates 2020-06-02 (version 2.08.0) (p. 889)
- Aurora MySQL database engine updates 2020-11-10 (version 2.07.3) (p. 892)
- Aurora MySQL database engine updates 2020-04-17 (version 2.07.2) (p. 894)
- Aurora MySQL database engine updates 2019-12-23 (version 2.07.1) (p. 895)
- Aurora MySQL database engine updates 2019-11-25 (version 2.07.0) (p. 895)
- Aurora MySQL database engine updates 2019-11-22 (version 2.06.0) (p. 898)
- Aurora MySQL database engine updates 2019-11-11 (version 2.05.0) (p. 900)
- Aurora MySQL database engine updates 2020-08-14 (version 2.04.9) (p. 902)
- Aurora MySQL database engine updates 2019-11-20 (version 2.04.8) (p. 905)
- Aurora MySQL database engine updates 2019-11-14 (version 2.04.7) (p. 907)
- Aurora MySQL database engine updates 2019-09-19 (version 2.04.6) (p. 909)
- Aurora MySQL database engine updates 2019-07-08 (version 2.04.5) (p. 910)
- Aurora MySQL database engine updates 2019-05-29 (version 2.04.4) (p. 912)
- Aurora MySQL database engine updates 2019-05-09 (version 2.04.3) (p. 913)
- Aurora MySQL database engine updates 2019-05-02 (version 2.04.2) (p. 914)
- Aurora MySQL database engine updates 2019-03-25 (version 2.04.1) (p. 916)
- Aurora MySQL database engine updates 2019-03-25 (version 2.04) (p. 916)
- Aurora MySQL database engine updates 2019-02-07 (p. 917) (Version 2.03.4)
- Aurora MySQL database engine updates 2019-01-18 (p. 918) (Version 2.03.3)
- Aurora MySQL database engine updates 2019-01-09 (p. 919) (Version 2.03.2)
- Aurora MySQL database engine updates 2018-10-24 (p. 919) (Version 2.03.1)
- Aurora MySQL database engine updates 2018-10-11 (p. 920) (Version 2.03)
- Aurora MySQL database engine updates 2018-10-08 (p. 920) (Version 2.02.5)
- Aurora MySQL database engine updates 2018-09-21 (p. 921) (Version 2.02.4)
- Aurora MySQL database engine updates 2018-08-23 (p. 922) (Version 2.02.3)
- Aurora MySQL database engine updates 2018-06-04 (p. 924) (Version 2.02.2)
- Aurora MySQL database engine updates 2018-05-03 (p. 926) (Version 2.02)
- Aurora MySQL database engine updates 2018-03-13 (p. 927) (Version 2.01.1)
Aurora MySQL database engine updates 2020-12-11 (version 2.09.1)

Version: 2.09.1

Aurora MySQL 2.09.1 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 1.23.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, 2.07.*, 2.08.*, and 2.09.*.

You can restore a snapshot from Aurora MySQL 1.23.* into Aurora MySQL 2.09.1. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.09.1. You can't upgrade an existing Aurora MySQL 1.23.* cluster directly to 2.09.1; however, you can restore its snapshot to Aurora MySQL 2.09.1.

To create a cluster with an older version of Aurora MySQL, specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

Security fixes:

Fixes and other enhancements to fine-tune handling in a managed environment. Additional CVE fixes below:

- CVE-2020-14567
- CVE-2020-14559
- CVE-2020-14553
- CVE-2020-14547
- CVE-2020-14540
- CVE-2020-2812
- CVE-2020-2806
- CVE-2020-2780
- CVE-2020-2765
- CVE-2020-2763
- CVE-2020-2760
- CVE-2020-2579

Availability improvements:

- Fixed an issue that might cause a client session to hang when the database engine encounters an error while reading from or writing to the network.
• Fixed a memory leak in dynamic resizing feature, introduced in 2.09.0.

Global databases:
• Fixed multiple issues where a global database secondary Region's replicas might restart when upgraded to release 2.09.0 while the primary Region writer was on an older release version.

Integration of MySQL community edition bug fixes
• Replication: Interleaved transactions could sometimes deadlock the slave applier when the transaction isolation level was set to REPEATABLE READ. (Bug #25040331)
• For a table having a TIMESTAMP or DATETIME column having a default of CURRENT_TIMESTAMP, the column could be initialized to 0000-00-00 00:00:00 if the table had a BEFORE INSERT trigger. (Bug #25209512, Bug #84077)
• For an INSERT statement for which the VALUES list produced values for the second or later row using a subquery containing a join, the server could exit after failing to resolve the required privileges. (Bug #23762382)

Aurora MySQL database engine updates 2020-09-17 (version 2.09.0)

Version: 2.09.0
Aurora MySQL 2.09.0 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 1.23.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, 2.07.*, 2.08.*, and 2.09.*.

You can restore a snapshot from Aurora MySQL 1.23.* into Aurora MySQL 2.09.0. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.09.0. You can't upgrade an existing Aurora MySQL 1.23.* cluster directly to 2.09.0; however, you can restore its snapshot to Aurora MySQL 2.09.0.

Important
The improvements to Aurora storage in this version limit the available upgrade paths from Aurora MySQL 1.* to Aurora MySQL 2.09. When you upgrade an Aurora MySQL 1.* cluster to 2.09, you must upgrade from Aurora MySQL 1.23.

To create a cluster with an older version of Aurora MySQL, specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

New features:
• With this release, you can create Amazon Aurora MySQL database instances with up to 128 tebibytes (TiB) of storage. The new storage limit is an increase from the prior 64 TiB. The 128 TiB storage size
supports larger databases. This capability is not supported on small instances sizes (db.t2 or db.t3). A single tablespace cannot grow beyond 64 TiB due to InnoDB limitations with 16 KB page size.

Aurora alerts you when the cluster volume size is near 128 TiB, so that you can take action prior to hitting the size limit. The alerts appear in the mysql log and RDS Events in the AWS Management Console.

- You can now turn parallel query on or off for an existing cluster by changing the value of the DB cluster parameter `aurora_parallel_query`. You don't need to use the `parallelquery` setting for the `--engine-mode` parameter when creating the cluster.

Parallel query is now expanded to be available in all regions where Aurora MySQL is available.

There are a number of other functionality enhancements and changes to the procedures for upgrading and enabling parallel query in an Aurora cluster. For more information, see Working with parallel query for Amazon Aurora MySQL (p. 697).

- Aurora dynamically resizes your cluster storage space. With dynamic resizing, the storage space for your Aurora DB cluster automatically decreases when you remove data from the DB cluster. For more information, see Storage scaling (p. 349).

Note
The dynamic resizing feature is being deployed in phases to the AWS Regions where Aurora is available. Depending on the Region where your cluster is, this feature might not be available yet. For more information, see the What's New announcement.

High priority fixes:

- Backport of Community Bug #27659490: SELECT USING DYNAMIC RANGE AND INDEX MERGE USE TOO MUCH MEMORY (OOM)
- Bug #26881508: MYSQL #1: DISABLE_ABORT_ON_ERROR IN AUTH_COMMON.H
- Backport of Community Bug #24437124: POSSIBLE BUFFER OVERFLOW ON CREATE TABLE
- Backport of Bug #27158030: INNODB ONLINE ALTER CRASHES WITH CONCURRENT DML
- Bug #29770705: SERVER CRASHED WHILE EXECUTING SELECT WITH SPECIFIC WHERE CLAUSE
- Backport of BUG #26502135: MYSQLD SEGFAULTS IN MDL_CONTEXT::TRY_ACQUIRE_LOCK_IMPL
- Backport of Bug #26935001: ALTER TABLE AUTO_INCREMENT TRIES TO READ INDEX FROM DISCARDED TABLESPACE
- Bug #28491099: [FATAL] MEMORY BLOCK IS INVALID | INNODB: ASSERTION FAILURE: UTOUT.CC:670
- Bug #30499288: GCC 9.2.1 REPORTS A NEW WARNING FOR OS_FILE_GET_PARENT_DIR
- Bug #29952565: where MYSQLD GOT SIGNAL 11 WHILE EXECUTING A QUERY(UNION + ORDER BY + SUB-QUERY)
- Bug #3028268: OUT OF MEMORY CRASH
- Bug #30441969: BUG #29723340: MYSQL SERVER CRASH AFTER SQL QUERY WITH DATA ?AST
- Bug #30569003: 5.7 REPLICATION BREAKAGE WITH SYNTAX ERROR WITH GRANT MANAGEMENT
- Bug #29915479: RUNNING COM_REGISTER_SLAVE WITHOUT COM_BINLOG_DUMP CAN RESULTS IN SERVER EXIT
- Bug #30569003: 5.7 REPLICATION BREAKAGE WITH SYNTAX ERROR WITH GRANT MANAGEMENT
- Bug #29915479: RUNNING COM_REGISTER_SLAVE WITHOUT COM_BINLOG_DUMP CAN RESULTS IN SERVER EXIT
- Bug #20712046: SHOW PROCESSLIST AND PERFORMANCE_SCHEMA TABLES DO NOT MASK PASSWORD FROM QUERY
- Backport bug #18898433: EXTREMELY SLOW PERFORMANCE WITH OUTER JOINS AND JOIN BUFFER (fixed in 5.7.21). Queries with many left joins were slow if join buffering was used (for example, using the block nested loop algorithm). (Bug #18898433, Bug #72854)*
- Backport bug #26402045: MYSQLD CRASHES ON QUERY (fixed in MySQL 5.7.23). Certain cases of subquery materialization could cause a server exit. These queries now produce an error suggesting that materialization be disabled. (Bug #26402045)
- [Backport from MySQL] users other than rdsadmin is disallowed to update pfs table in the reader replica.
- Fix the issue where the customer can not update the perfschema in the reader replica
- Bug #26666274: INFINITE LOOP IN PERFORMANCE SCHEMA BUFFER CONTAINER
- Bug #26997096: relay_log_space value is not updated in a synchronized manner so that its value sometimes much higher than the actual disk space used by relay logs.
- BUG #25082593: FOREIGN KEY VALIDATION DOESN'T NEED TO ACQUIRE GAP LOCK IN READ COMMITTED
- CVE-2019-2731
- CVE-2018-2645
- CVE-2019-2581
- CVE-2018-2787
- CVE-2019-2482
- CVE-2018-2640
- CVE-2018-2784
- CVE-2019-2628
- CVE-2019-2911
- CVE-2019-2628
- CVE-2018-3284
- CVE-2018-3065
- CVE-2019-2537
- CVE-2019-2948
- CVE-2019-2434
- CVE-2019-2420

**Availability improvements:**

- Enable lock manager ABA fix by default.
- Fixed an issue in the lock manager where a race condition can cause a lock to be shared by two transactions, causing the database to restart.
- Fixed an issue when creating a temporary table with compressed row format might result in a restart.
- Fix default value of table_open_cache on 16XL and 24XL instances which could cause repeated failovers and high CPU utilization on large instances classes (R4/R5-16XL, R5-12XL, R5-24XL). This impacted 2.07.x.
- Fixed an issue where restoring a cluster from Amazon S3 to Aurora MySQL version 2.08.0 takes longer than expected when the S3 backup didn't include the mysql.host table.
- Fixed an issue which might cause repeated failovers due to updates of virtual columns with secondary indexes.
- Fixed an issue related to transaction lock memory management with long-running write transactions resulting in a database restart.
- Fixed multiple issues where the the engine might crash during zero-downtime patching while checking for safe point for patching.
- Fixed an issue to skip redo logging for temporary tables, which was previously causing a crash.
• Fixed a race condition in the lock manager between killing connection/query and the session killed.
• Fixed an issue where the database could crash if it is a binlog replica and receives a DDL event over the MySQL `time_zone` table.

Global databases:
• `MySQL INFORMATION_SCHEMA.REPLICA_HOST_STATUS` view in a secondary Region now shows the entries for the replicas belonging to that Region.
• Fixed unexpected query failures that could occur in a Global DB secondary Region after temporary network connectivity issues between the primary and secondary Regions.

Parallel query:
• Fixed the `EXPLAIN` plan for a Parallel Query query, which is incorrect for a simple single-table query.
• Fixed self-deadlatch that may occur when Parallel Query is enabled.

General improvements:
• Export to S3 now supports the `ENCRYPTION` keyword.
• The `aurora_binlog_replication_max_yield_seconds` parameter now has a max value of 36,000. The previous maximum accepted value was 45. This parameter works only when the parameter `aurora_binlog_use_large_read_buffer` is set to 1.
• Changed the behavior to map `MIXED` binlog_format to `ROW` instead of `STATEMENT` when executing `LOAD DATA FROM INFILE | S3`.
• Fixed an issue where a binlog replica connected to an Aurora MySQL binlog primary might show incomplete data when the primary executed `LOAD DATA FROM S3` and `binlog_format` is set to `STATEMENT`.
• Increased maximum allowable length for audit system variables `server_audit_incl_users` and `server_audit_excl_users` from 1024 bytes to 2000 bytes.
• Fixed an issue where users may lose access to the database when lowering the `max_connections` parameter in the parameter group when the current connections is greater than the value being set.
• Fixed an issue in Data Activity Streams where a single quote and backslash were not escaped properly.

Integration of MySQL community edition bug fixes
• Bug #27659490: SELECT USING DYNAMIC RANGE AND INDEX MERGE USE TOO MUCH MEMORY(OOM)
• Bug #26881508: MYSQL #1: DISABLE_ABORT_ON_ERROR IN AUTH_COMMON.H
• Bug #24437124: POSSIBLE BUFFER OVERFLOW ON CREATE TABLE
• Bug #27158030: INNODB ONLINE ALTER CRASHES WITH CONCURRENT DML
• Bug #29770705: SERVER CRASHED WHILE EXECUTING SELECT WITH SPECIFIC WHERE CLAUSE
• Bug #26502135: MYSQLD SEGFAULTS IN MDL_CONTEXT::TRY_ACQUIRE_LOCK_IMPL
• Bug #26935001: ALTER TABLE AUTO_INCREMENT TRIES TO READ INDEX FROM DISCARDED TABLESPACE
• Bug #28491099: [FATAL] MEMORY BLOCK IS INVALID | INNODB: ASSERTION FAILURE: UTOUT.CC:670
• Bug #30499288: GCC 9.2.1 REPORTS A NEW WARNING FOR OS_FILE_GET_PARENT_DIR
• Bug #29952565: where MYSQLD GOT SIGNAL 11 WHILE EXECUTING A QUERY(UNION + ORDER BY + SUB-QUERY)
• Bug #30628268: OUT OF MEMORY CRASH
• Bug #30441969: BUG #29723340: MYSQL SERVER CRASH AFTER SQL QUERY WITH DATA ?AST
• Bug #30569003: 5.7 REPLICATION BREAKAGE WITH SYNTAX ERROR WITH GRANT MANAGEMENT
• Bug #29915479: RUNNING COM_REGISTER_SLAVE WITHOUT COM_BINLOG_DUMP CAN RESULTS IN SERVER EXIT
• Bug #30569003: 5.7 REPLICATION BREAKAGE WITH SYNTAX ERROR WITH GRANT MANAGEMENT
• Bug #29915479: RUNNING COM_REGISTER_SLAVE WITHOUT COM_BINLOG_DUMP CAN RESULTS IN SERVER EXIT
• Bug #20712046: SHOW PROCESSLIST AND PERFORMANCE_SCHEMA TABLES DO NOT MASK PASSWORD FROM QUERY
• Bug #18898433: EXTREMELY SLOW PERFORMANCE WITH OUTER JOINS AND JOIN BUFFER (fixed in 5.7.21)
• Bug #26402045: MYSQLD CRASHES ON QUERY (fixed in MySQL 5.7.23)
• Bug #23103937: PS_TRUNCATE_ALL_TABLES() DOES NOT WORK IN SUPER_READ_ONLY MODE
• Bug #26666274: INFINITE LOOP IN PERFORMANCE SCHEMA BUFFER CONTAINER
• Bug #26997096: relay_log_space value is not updated in a synchronized manner so that its value sometimes much higher than the actual disk space used by relay logs. (https://github.com/mysql/mysql-server/commit/78f25d2809ad457e81f90342239c9bc32a36cda)
• Bug #25082593: FOREIGN KEY VALIDATION DOESN'T NEED TO ACQUIRE GAP LOCK IN READ COMMITTED
• Bug #24764800: REPLICATION FAILING ON SLAVE WITH XAER_RMFAIL ERROR.
• Bug #81441: WARNING ABOUT LOCALHOST WHEN USING SKIP-NAME-RESOLVE.

Aurora MySQL database engine updates 2020-11-12 (version 2.08.3)

Version: 2.08.3

Aurora MySQL 2.08.3 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases for upgrade to 2.08.3 are: 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, 2.07.*, and 2.08.*.

You can upgrade existing Aurora MySQL 2.* database clusters directly to Aurora MySQL 2.08.3. You can upgrade an existing Aurora MySQL 1.* cluster directly to 2.07.3 or higher and then directly upgrade to 2.08.3.

To create a cluster with an older version of Aurora MySQL, specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

Security fixes:
Fixes and other enhancements to fine-tune handling in a managed environment. Additional CVE fixes below:

- CVE-2020-14567
- CVE-2020-14559
- CVE-2020-14553
- CVE-2020-14547
- CVE-2020-14540
- CVE-2020-2812
- CVE-2020-2806
- CVE-2020-2780
- CVE-2020-2765
- CVE-2020-2763
- CVE-2020-2760
- CVE-2020-2579

Integration of MySQL community edition bug fixes

- Bug #23762382 - INSERT VALUES QUERY WITH JOIN IN A SELECT CAUSES INCORRECT BEHAVIOR.
- Bug #25209512 - CURRENT_TIMESTAMP PRODUCES ZEROS IN TRIGGER.

**Aurora MySQL database engine updates 2020-08-28 (version 2.08.2)**

**Version:** 2.08.2

Aurora MySQL 2.08.2 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, 2.07.*, and 2.08.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.08.2. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.08.2. You can't upgrade an existing Aurora MySQL 1.* cluster directly to 2.08.2; however, you can restore its snapshot to Aurora MySQL 2.08.2. See Restoring from a DB cluster snapshot (p. 420) for more information about restoring snapshots.

To create a cluster with an older version of Aurora MySQL, specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

**Improvements**

**Critical fixes:**
• Fixed an issue that might cause an unplanned outage and affect database availability.

**Availability fixes:**

• Fixed an issue where the Aurora MySQL database could restart if it is a binlog replica and replicates a DDL event over the `mysql.time_zone` table.

### Aurora MySQL database engine updates 2020-06-18 (version 2.08.1)

**Version:** 2.08.1

Aurora MySQL 2.08.1 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, 2.07.*, and 2.08.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.08.1. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.08.1. You can’t upgrade an existing Aurora MySQL 1.* cluster directly to 2.08.1; however, you can restore its snapshot to Aurora MySQL 2.08.1.

To create a cluster with an older version of Aurora MySQL, specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**

For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

### Improvements

**New features:**

• Global database write forwarding. In an Aurora global database, now you can perform certain write operations, such as DML statements, while connected to a secondary cluster. The write operations are forwarded to the primary cluster, and any changes are replicated back to the secondary clusters. For more information, see Using write forwarding in an Amazon Aurora global database (p. 233).

**General stability fixes:**

• Fixed an issue where restoring a cluster from Amazon S3 to Aurora MySQL version 2.08.0 took longer than expected if the S3 backup didn’t include the `mysql.host` table.

### Aurora MySQL database engine updates 2020-06-02 (version 2.08.0)

**Version:** 2.08.0

Aurora MySQL 2.08.0 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.
Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, 2.07.*, and 2.08.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.08.0. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.08.0. You can't upgrade an existing Aurora MySQL 1.* cluster directly to 2.08.0; however, you can restore its snapshot to Aurora MySQL 2.08.0.

To create a cluster with an older version of Aurora MySQL, specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

New features:

- Improved binary log (binlog) processing to reduce crash recovery time and commit time latency when very large transactions are involved.
- Launching Database Activity Streams (DAS) feature for Aurora MySQL. This feature provides a near real-time data stream of the database activity in your relational database to help you monitor activity. For more information, see Using Database Activity Streams with Amazon Aurora (p. 565).
- Updated timezone files to support the latest Brazil timezone change.
- Introduced new keywords in SQL to exercise the hash join functionality for a specific table and/or inner table: HASH_JOIN, HASH_JOIN_PROBING, and HASH_JOIN_BUILDING. For additional details, see Aurora MySQL hints (p. 869).
- Introduced join order hint support in Aurora MySQL 5.7 by backporting a MySQL 8.0 feature. The new hints are JOIN_FIXED_ORDER, JOIN_ORDER, JOIN_PREFIX, and JOIN_SUFFIX. For detailed documentation of join order hint support, see WL#9158: Join order hints.
- Aurora Machine Learning now supports user-defined functions with MEDIUMINT as the return type.
- The lambda_async() stored procedure now supports all MySQL utf8 characters.

High priority fixes:

- Fixed an issue that could cause a reader DB instance to return incomplete results for an FTS query after the INFORMATION_SCHEMA.INNODB_SYS_TABLES table is queried on the writer DB instance.
  - CVE-2019-5443
  - CVE-2019-3822

Availability improvements:

- Fixed an issue that resulted in a database restart after a multi-query statement that accesses multiple tables or databases is executed with the query cache enabled.
- Fixed a race condition in the lock manager that resulted in a database restart or failover during transaction rollback.
- Fixed an issue that triggered database restart or failover when multiple connections are trying to update the same table with a Full-Text Search index.
- Fixed an issue that could trigger a database restart or failover during a kill session command.
• Fixed an issue that caused reader DB instance to restart during a multi-statement transaction with multiple SELECT statements and a heavy write workload on the writer DB instance with AUTOCOMMIT enabled.

• Fixed an issue that caused reader DB instance to restart after executing long-running queries while the writer DB instance is under a heavy OLTP write workload.

General improvements:

• Improved database recovery time and commit latency for long running transactions when binlog is enabled.

• Improved the algorithm to generate better statistics for estimating distinct value counts on indexed columns, including columns with skewed data distributions.

• Reduced the response time and CPU utilization of join queries that access MyISAM temporary tables and the results spill to local storage.

• Fixed an issue that prevented Aurora MySQL 5.6 snapshots with database or table names containing spaces from being restored to a new Aurora MySQL 5.7 cluster.

• Included victim transaction info when deadlock is resolved in show engine innodb status.

• Fixed an issue that caused connections to get stuck when clients of multiple different versions are connected to the same database and are accessing the query cache.

• Fixed a memory leak resulting from multiple invocations of the Zero-Downtime Patch (ZDP) or Zero-Downtime Restart (ZDR) workflow throughout the lifetime of a database instance.

• Fixed an error message in Zero-Downtime Patch (ZDP) or Zero-Downtime Restart (ZDR) operations wrongly stating that the last transaction was aborted if the auto-commit flag is turned off.

• Fixed an issue in Zero-Downtime Patch (ZDP) operations that could lead to a server failure error message when restoring user session variables in the new database process.

• Fixed an issue in Zero Downtime Patch (ZDP) operations that might cause intermittent database failures when there are long running queries during patching.

• Fixed an issue where queries including an Aurora Machine Learning function returned empty error messages due to an incorrectly handled error response from Machine Learning services such as Amazon Sagemaker and Amazon Comprehend.

• Fixed an issue in the out-of-memory monitoring functionality that did not honor a custom value of the table_definition_cache parameter.

• The error message “Query execution was interrupted” is returned if an Aurora Machine Learning query is interrupted. Previously, the generic message “Internal error in processing ML request” was returned instead.

• Fixed an issue that could cause a binlog worker to experience a connection timeout when the slave_net_timeout parameter is less than the aurora_binlog_replication_max_yield_seconds parameter and there is low workload on the binlog master cluster.

• Improved monitoring of the binlog recovery progress by outputting informational messages in the error log at a frequency of one message per minute.

• Fixed an issue that could cause active transactions not to be reported by the SHOW ENGINE INNODB STATUS query.

Integration of MySQL community edition bug fixes

• Bug #25289359: A full-text cache lock taken when data is synchronized was not released if the full-text cache size exceeded the full-text cache size limit.

• Bug #29138644: Manually changing the system time while the MySQL server was running caused page cleaner thread delays.
• Bug #25222337: A NULL virtual column field name in a virtual index caused a server exit during a field name comparison that occurs while populating virtual columns affected by a foreign key constraint.

• Bug #25053286: Executing a stored procedure containing a query that accessed a view could allocate memory that was not freed until the session ended.

• Bug #25586773: Executing a stored procedure containing a statement that created a table from the contents of certain SELECT statements could result in a memory leak.

• Bug #28834208: During log application, after an OPTIMIZE TABLE operation, InnoDB did not populate virtual columns before checking for virtual column index updates.

• Bug #26666274: Infinite loop in performance schema buffer container due to 32-bit unsigned integer overflow.

Aurora MySQL database engine updates 2020-11-10 (version 2.07.3)

Version: 2.07.3

Aurora MySQL 2.07.3 is generally available. Aurora MySQL 2.* versions are compatible with MySQL 5.7 and Aurora MySQL 1.* versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 1.23.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, 2.07.*, 2.08.*, and 2.09.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.07.3. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.07.3. You can’t upgrade an existing Aurora MySQL 1.* cluster directly to 2.07.3; however, you can restore its snapshot to Aurora MySQL 2.07.3.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

Security fixes:

Fixes and other enhancements to fine-tune handling in a managed environment. Additional CVE fixes below:

• CVE-2020-14567
• CVE-2020-14559
• CVE-2020-14553
• CVE-2020-14547
• CVE-2020-14540
• CVE-2020-2812
• CVE-2020-2806
• CVE-2020-2780
• CVE-2020-2765
• CVE-2020-2763
• CVE-2020-2760
• CVE-2020-2579
- **CVE-2019-2740**

**Availability improvements:**

- Fixed a race condition in the lock manager between the killing of a connection/query and the termination of the session resulting in a database restart.
- Fixed an issue that results in a database restart after a multi-query statement that accesses multiple tables or databases is executed with the query cache enabled.
- Fixed an issue that might cause repeated restarts due to updates of virtual columns with secondary indexes.

**Integration of MySQL community edition bug fixes**

- **InnoDB:** Concurrent XA transactions that ran successfully to the XA prepare stage on the master conflicted when replayed on the slave, resulting in a lock wait timeout in the applier thread. The conflict was due to the GAP lock range which differed when the transactions were replayed serially on the slave. To prevent this type of conflict, GAP locks taken by XA transactions in **READ COMMITTED** isolation level are now released (and no longer inherited) when XA transactions reach the prepare stage. (Bug #27189701, Bug #25866046)
- **InnoDB:** A gap lock was taken unnecessarily during foreign key validation while using the **READ COMMITTED** isolation level. (Bug #25082593)
- **Replication:** When using XA transactions, if a lock wait timeout or deadlock occurred for the applier (SQL) thread on a replication slave, the automatic retry did not work. The cause was that while the SQL thread would do a rollback, it would not roll the XA transaction back. This meant that when the transaction was retried, the first event was XA START which was invalid as the XA transaction was already in progress, leading to an XAER_RMFAIL error. (Bug #24764800)
- **Replication:** Interleaved transactions could sometimes deadlock the slave applier when the transaction isolation level was set to **REPEATABLE READ**. (Bug #25040331)
- **Replication:** The value returned by a **SHOW SLAVE STATUS** statement for the total combined size of all existing relay log files (Relay_Log_Space) could become much larger than the actual disk space used by the relay log files. The I/O thread did not lock the variable while it updated the value, so the SQL thread could automatically delete a relay log file and write a reduced value before the I/O thread finished updating the value. The I/O thread then wrote its original size calculation, ignoring the SQL thread's update and so adding back the space for the deleted file. The Relay_Log_Space value is now locked during updates to prevent concurrent updates and ensure an accurate calculation. (Bug #26997096, Bug #87832)
- For an **INSERT** statement for which the VALUES list produced values for the second or later row using a subquery containing a join, the server could exit after failing to resolve the required privileges. (Bug #23762382)
- For a table having a **TIMESTAMP** or **DATETIME** column having a default of **CURRENT_TIMESTAMP**, the column could be initialized to **0000-00-00 00:00:00** if the table had a **BEFORE INSERT** trigger. (Bug #25209512, Bug #84077)
- A server exit could result from simultaneous attempts by multiple threads to register and deregister metadata Performance Schema objects. (Bug #26502135)
- Executing a stored procedure containing a statement that created a table from the contents of certain **SELECT** statements could result in a memory leak. (Bug #25586773)
- Executing a stored procedure containing a query that accessed a view could allocate memory that was not freed until the session ended. (Bug #25053286)
- Certain cases of subquery materialization could cause a server exit. These queries now produce an error suggesting that materialization be disabled. (Bug #26402045)
- Queries with many left joins were slow if join buffering was used (for example, using the block nested loop algorithm). (Bug #18898433, Bug #72854)
The optimizer skipped the second column in a composite index when executing an inner join with a LIKE clause against the second column. (Bug #28086754)

Aurora MySQL database engine updates 2020-04-17 (version 2.07.2)

Version: 2.07.2

Aurora MySQL 2.07.2 is generally available. Aurora MySQL 2.* versions are compatible with MySQL 5.7 and Aurora MySQL 1.* versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, and 2.07.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.07.2. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.07.2. You can't upgrade an existing Aurora MySQL 1.* cluster directly to 2.07.2; however, you can restore its snapshot to Aurora MySQL 2.07.2.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

Note
This version is currently not available in the following AWS Region: [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

High priority fixes:

- Fixed an issue that caused cloning to take longer on some database clusters with high write loads.
- Fixed an issue that could cause queries on a reader DB instance with execution plans using secondary indexes to return uncommitted data. The issue is limited to data affected by data manipulation language (DML) operations that modify primary or secondary index key columns.

General improvements:

- Fixed an issue that resulted in a slow restore of an Aurora 1.x DB cluster containing FTS (Full Text Search) indexes to an Aurora 2.x DB cluster.
- Fixed an issue that caused slower restores of an Aurora 1.x database snapshot containing partitioned tables with special characters in table names to an Aurora 2.x DB cluster.
- Fixed an issue that caused errors when querying slow query logs and general logs in reader DB instances.

Integration of MySQL community edition bug fixes

- Bug #23104498: Fixed an issue in Performance Schema in reporting total memory used. ([https://github.com/mysql/mysql-server/commit/20b6840df5452f47313c6f9a6ca075bfbcc00a96b](https://github.com/mysql/mysql-server/commit/20b6840df5452f47313c6f9a6ca075bfbcc00a96b))
- Bug #22551677: Fixed an issue in Performance Schema that could lead to the database engine crashing when attempting to take it offline. ([https://github.com/mysql/mysql-server/commit/05e2386ecc32b6b444b900c9f8a87a1d8d531e9](https://github.com/mysql/mysql-server/commit/05e2386ecc32b6b444b900c9f8a87a1d8d531e9))
• Bug #23550835, Bug #23298025, Bug #81464: Fixed an issue in Performance Schema that causes a
database engine crash due to exceeding the capacity of an internal buffer. (https://github.com/mysql/
mysql-server/commit/b4287f93857bf2f99b18fd06f555bbe5b12debfc)

Aurora MySQL database engine updates 2019-12-23 (version 2.07.1)

Version: 2.07.1

Aurora MySQL 2.07.1 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7
and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*,
1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, and 2.07.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.07.1.
You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL
2.07.1. You cannot upgrade an existing Aurora MySQL 1.* cluster directly to 2.07.1; however, you can
restore its snapshot to Aurora MySQL 2.07.1.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the
AWS Management Console, the AWS CLI, or the RDS API.

Note
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East)
[us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1],
Asia Pacific (Hong Kong) [ap-east-1], and Middle East (Bahrain) [me-south-1]. There will be a
separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through
AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and
patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

High priority fixes:

• Fixed a slow memory leak in Aurora specific database tracing and logging sub-system that lowers the
freeable memory.

General Stability fixes:

• Fixed a crash during execution of a complex query involving multi-table joins and aggregation that use
intermediate tables internally.

Aurora MySQL database engine updates 2019-11-25 (version 2.07.0)

Version: 2.07.0

Aurora MySQL 2.07.0 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7
and Aurora MySQL 1.x versions are compatible with MySQL 5.6.
Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, and 2.07.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.07.0. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.07.0. You cannot upgrade an existing Aurora MySQL 1.* cluster directly to 2.07.0; however, you can restore its snapshot to Aurora MySQL 2.07.0.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

**Note**
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], Asia Pacific (Hong Kong) [ap-east-1], Middle East (Bahrain) [me-south-1], and South America (São Paulo) [sa-east-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see [Maintaining an Amazon Aurora DB cluster](p. 388).

**Note**
For information on how to upgrade your Aurora MySQL database cluster, see [Upgrading and patching Amazon Aurora MySQL DB clusters](p. 877).

**Improvements**

**New features:**

- Global Databases now allow adding secondary read-only replica regions for database clusters deployed in these AWS Regions: US East (N. Virginia) [us-east-1], US East (Ohio) [us-east-2], US West (N. California) [us-west-1], US West (Oregon) [us-west-2], Europe (Ireland) [eu-west-1], Europe (London) [eu-west-2], Europe (Paris) [eu-west-3], Asia Pacific (Tokyo) [ap-northeast-1], Asia Pacific (Seoul) [ap-northeast-2], Asia Pacific (Singapore) [ap-southeast-1], Asia Pacific (Sydney) [ap-southeast-2], Canada (Central) [ca-central-1], Europe (Frankfurt) [eu-central-1], and Asia Pacific (Mumbai) [ap-south-1].
- Amazon Aurora machine learning is a highly optimized integration between the Aurora MySQL database and AWS machine learning (ML) services. Aurora machine learning allows developers to add a variety of ML-based predictions to their database applications by invoking ML models using the familiar SQL programming language they already use for database development, without having to build custom integrations or learn separate tools. For more information, see [Using machine learning (ML) capabilities with Amazon Aurora](p. 877).
- Added support for the ANSI `READ COMMITTED` isolation level on the read replicas. This isolation level enables long-running queries on the read replica to execute without impacting the high throughput of writes on the writer node. For more information, see [Aurora MySQL isolation levels](p. 877).

**Critical fixes:**

- CVE-2019-2922
- CVE-2019-2923
- CVE-2019-2924
- CVE-2019-2910

**High-priority fixes:**

- Fixed an issue in the DDL recovery that resulted in prolonged database downtime. Clusters that become unavailable after executing multi-table drop statement, for example `DROP TABLE t1, t2, t3`, should be updated to this version.
• Fixed an issue in the DDL recovery that resulted in prolonged database downtime. Clusters that become unavailable after executing `INPLACE ALTER TABLE` DDL statements should be updated to this version.

**General stability fixes:**

• Fixed an issue that generated inconsistent data in the `information_schema.replica_host_status` table.

**Integration of MySQL community edition bug fixes**

• Bug #26251621: INCORRECT BEHAVIOR WITH TRIGGER AND GCOL
• Bug #22574695: ASSERTION `!TABLE || (TABLE->READ_SET || BITMAP_IS_SET(TABLE->READ_SET, FIEL
• Bug #25966845: INSERT ON DUPLICATE KEY GENERATE A DEADLOCK
• Bug #23070734: CONCURRENT TRUNCATE TABLES CAUSE STALL
• Bug #26191879: FOREIGN KEY CASCADES USE EXCESSIVE MEMORY
• Bug #20989615: INNODB AUTO_INCREMENT PRODUCES SAME VALUE TWICE

**Comparison with Aurora MySQL version 1**

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

• Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
• Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

**MySQL 5.7 compatibility**

Aurora MySQL 2.0.7.0 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.0.7.0 does not currently support the following MySQL 5.7 features:

• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The `CREATE TABLESPACE` SQL statement
Aurora MySQL database engine updates 2019-11-22 (version 2.06.0)

Version: 2.06.0

Aurora MySQL 2.06.0 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, and 2.06.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.06.0. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.06.0. You cannot upgrade an existing Aurora MySQL 1.* cluster directly to 2.06.0; however, you can restore its snapshot to Aurora MySQL 2.06.0.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

Note
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], Asia Pacific (Hong Kong) [ap-east-1], and Middle East (Bahrain) [me-south-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

New features:

- Aurora MySQL clusters now support the instance types db.r5.8xlarge, db.r5.16xlarge, and db.r5.24xlarge. For more information about instance types for Aurora MySQL clusters, see DB instance classes (p. 46).
- The hash join feature is now generally available and does not require the Aurora lab mode setting to be ON. This feature can improve query performance when you need to join a large amount of data by using an equi-join. For more information about using this feature, see Working with hash joins in Aurora MySQL (p. 845).
- The hot row contention feature is now generally available and does not require the Aurora lab mode setting to be ON. This feature substantially improves throughput for workloads with many transactions contending for rows on the same page.
- Aurora MySQL 2.06 and higher support “rewinding” a DB cluster to a specific time, without restoring data from a backup. This feature, known as Backtrack, provides a quick way to recover from user errors, such as dropping the wrong table or deleting the wrong row. Backtrack completes within seconds, even for large databases. Read the AWS blog for an overview, and refer to Backtracking an Aurora DB cluster (p. 677) for more details.
- Aurora 2.06 and higher support synchronous AWS Lambda invocations through the native function lambda_sync(). Also available is native function lambda_async(), which can be used as an alternative to the existing stored procedure for asynchronous Lambda invocation. For information about calling Lambda functions, see Invoking a Lambda function from an Amazon Aurora MySQL DB cluster (p. 818).
Critical fixes:

None.

High-priority fixes:

CVE fixes

- CVE-2019-2805
- CVE-2019-2730
- CVE-2019-2739
- CVE-2019-2778
- CVE-2019-2758
- CVE-2018-3064
- CVE-2018-3058
- CVE-2018-2786
- CVE-2017-3653
- CVE-2017-3455
- CVE-2017-3465
- CVE-2017-3244
- CVE-2016-5612

Connection handling

- Database availability has been improved to better service a surge in client connections while executing one or more DDLs. It is handled by temporarily creating additional threads when needed. You are advised to upgrade if the database becomes unresponsive following a surge in connections while processing DDL.

Engine restart

- Fixed an issue of prolonged unavailability while restarting the engine. This addresses an issue in the buffer pool initialization. This issue occurs rarely but can potentially impact any supported release.
- Fixed an issue that causes a database configured as a binlog master to restart while a heavy write workload is running.

General stability fixes:

- Made improvements where queries accessing uncached data could be slower than usual. Customers experiencing unexplained elevated read latency while accessing uncached data are encouraged to upgrade as they may be experiencing this issue.
- Fixed an issue that failed to restore partitioned tables from a database snapshot. Customers who encounter errors when accessing partitioned tables in a database that has been restored from the snapshot of an Aurora MySQL 1.* database are advised to use this version.
- Improved stability of the Aurora Replicas by fixing lock contention between threads serving read queries and the one applying schema changes while a DDL query is in progress on the writer DB instance.
- Fixed a stability issue related to mysql.innodb_table_stats table update triggered by DDL operations.
- Fixed an issue that incorrectly reported ERROR 1836 when a nested query is executed against a temporary table on the Aurora Replica.
Performance enhancements:

- Improved performance of binlog replication by preventing unnecessary API calls to the cache if the query cache has been disabled on the binlog worker.

Comparison with Aurora MySQL version 1

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
- Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

MySQL 5.7 compatibility

Aurora MySQL 2.06.0 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.06.0 does not currently support the following MySQL 5.7 features:

- Group replication plugin
- Increased page size
- InnoDB buffer pool loading at startup
- InnoDB full-text parser plugin
- Multisource replication
- Online buffer pool resizing
- Password validation plugin
- Query rewrite plugins
- Replication filtering
- The CREATE TABLESPACE SQL statement

Aurora MySQL database engine updates 2019-11-11 (version 2.05.0)

Version: 2.05.0

Aurora MySQL 2.05.0 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.* and 2.04.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.05.0. You also have the option to upgrade existing Aurora MySQL 2.* database clusters, up to 2.04.6, to Aurora
MySQL 2.05.0. You cannot upgrade an existing Aurora MySQL 1.* cluster directly to 2.05.0; however, you can restore its snapshot to Aurora MySQL 2.05.0.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

**Note**
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], Asia Pacific (Hong Kong) [ap-east-1], Europe (Stockholm) [eu-north-1], and Middle East (Bahrain) [me-south-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

**Improvements**

**Critical fixes:**
- CVE-2018-0734
- CVE-2019-2534
- CVE-2018-3155
- CVE-2018-2612
- CVE-2017-3599
- CVE-2018-3056
- CVE-2018-2562
- CVE-2017-3329
- CVE-2018-2696
- Fixed an issue where the events in current binlog file on the master were not replicated on the worker if the value of the parameter `sync_binlog` was not set to 1.

**High-priority fixes:**
- Customers with database size close to 64 tebibytes (TiB) are strongly advised to upgrade to this version to avoid downtime due to stability bugs affecting volumes close to the Aurora storage limit.
- The default value of the parameter `aurora_binlog_replication_max_yield_seconds` has been changed to zero to prevent an increase in replication lag in favor of foreground query performance on the binlog master.

**Integration of MySQL bug fixes**
- Bug#23054591: PURGE BINARY LOGS TO is reading the whole binlog file and causing MySQL to Stall

**Comparison with Aurora MySQL version 1**

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).
- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
• Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
• Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
• Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

MySQL 5.7 compatibility

Aurora MySQL 2.05.0 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.05.0 does not currently support the following MySQL 5.7 features:

• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The CREATE TABLESPACE SQL statement

Aurora MySQL database engine updates 2020-08-14 (version 2.04.9)

Version: 2.04.9

Aurora MySQL 2.04.9 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, and 2.05.*. You can restore a snapshot of any 2.* Aurora MySQL release into Aurora MySQL 2.04.9. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.04.9.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], Asia Pacific (Hong Kong) [ap-east-1], and Middle East (Bahrain) [me-south-1]. There will be a separate announcement once it is made available.
Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

High-priority fixes:

CVE fixes

- CVE-2019-2805
- CVE-2019-2730
- CVE-2019-2739
- CVE-2019-2778
- CVE-2019-2758
- CVE-2018-3064
- CVE-2018-3058
- CVE-2018-2786
- CVE-2017-3653
- CVE-2017-3455
- CVE-2017-3464
- CVE-2017-3465
- CVE-2017-3244
- CVE-2016-5612
- CVE-2019-2628
- CVE-2019-2740
- CVE-2019-2922
- CVE-2019-2923
- CVE-2019-2924
- CVE-2019-2910
- CVE-2019-5443
- CVE-2019-3822
- CVE-2020-2760
- CVE-2019-2911
- CVE-2018-2813

Availability improvements:

- Fixed an issue that could cause a database restart or failover due to execution of a kill session command.
- Fixed an issue that causes a database restart during execution of a complex query involving multi-table joins and aggregation that use intermediate tables internally.
- Fixed an issue that causes database restarts due to an interrupted DROP TABLE on multiple tables.
- Fixed an issue that causes a database failover during database recovery.
- Fixed a database restart caused by incorrect reporting of threads_running when audit and slow query logs are enabled.
- Fixed an issue where a kill query command might get stuck during execution.
- Fixed a race condition in the lock manager that resulted in a database restart or failover during transaction rollback.
• Fixed an issue that triggered database restart or failover when multiple connections are trying to update the same table with a Full-Text Search index.
• Fixed an issue that can cause a deadlock when purging an index resulting in a failover or restart.

General improvements:

• Fixed issues that could cause queries on read replicas to use data from an uncommitted transaction. This issue is limited to the transactions that are started immediately after a database restart.
• Fixed an issue encountered during INPLACE ALTER TABLE for a table with triggers defined and when the DDL did not contain a RENAME clause.
• Fixed an issue that caused cloning to take longer on some database clusters with high writeload.
• Fixed an issue encountered during an upgrade when a partitioned table has embedded spaces in the name.
• Fixed an issue where the read replica might transiently see partial results of a recently committed transaction on the writer.
• Fixed an issue where queries on a read replica against an FTS table may produce stale results. This will only occur when the FTS query on the read replica closely follows a query on INFORMATION_SCHEMA.INNODB_SYS_TABLES for the same FTS table on the writer.
• Fixed an issue that resulted in a slow restore of Aurora 1.x database cluster containing FTS (Full-Text Search) indexes to an Aurora 2.x database cluster.
• Extended maximum allowable length to 2000 for server_audit_incl_users and server_audit_excl_users global parameters.
• Fixed an issue where Aurora 1.x to Aurora 2.x restore might take an extended time to complete.
• Fixed an issue where a lambda_async invocation through stored procedure doesn't work with Unicode.
• Fixed an issue encountered when a spatial index does not properly handle an off-record geometry column.
• Fixed an issue that might cause a query to fail on a reader DB instance with InternalFailureException error with message "Operation terminated (internal error)".

Integration of MySQL bug fixes

• Bug #23070734, Bug #80060: Concurrent TRUNCATE TABLEs cause stalls
• Bug #23103937: PS_TRUNCATE_ALL_TABLES() DOES NOT WORK IN SUPER_READ_ONLY MODE
• Bug#22551677: When taking the server offline, a race condition within the Performance Schema could lead to a server exit.
• Bug #27082268: Invalid FTS sync synchronization.
• BUG #12589870: Fixed an issues which causes a restart with multi-query statement when query cache is enabled.
• Bug #26402045: Certain cases of subquery materialization could cause a server exit. These queries now produce an error suggesting that materialization be disabled.
• Bug #18898433: Queries with many left joins were slow if join buffering was used (for example, using the block nested loop algorithm).
• Bug #25222337: A NULL virtual column field name in a virtual index caused a server exit during a field name comparison that occurs while populating virtual columns affected by a foreign key constraint. (https://github.com/mysql/mysql-server/commit/273d5c9d7072c63b6c47dbef6963d7dc491d5131)
• Bug #25053286: Executing a stored procedure containing a query that accessed a view could allocate memory that was not freed until the session ended. (https://github.com/mysql/mysql-server/commit/d7b37d4d141a95f577916448650c429f0d6e193d)
• Bug #25586773: Executing a stored procedure containing a statement that created a table from the contents of certain SELECT statements could result in a memory leak. (https://dev.mysql.com/doc/refman/5.7/en/select.html)
• Bug #26666274: INFINITE LOOP IN PERFORMANCE SCHEMA BUFFER CONTAINER.
• Bug #23550835, Bug #23298025, Bug #81464: A SELECT Performance Schema tables when an internal buffer was full could cause a server exit.

Comparison with Aurora MySQL version 1

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

• Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
• Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
• Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
• Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

MySQL 5.7 compatibility

Aurora MySQL 2.04.9 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.04.9 does not currently support the following MySQL 5.7 features:

• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The CREATE TABLESPACE SQL statement

Aurora MySQL database engine updates 2019-11-20 (version 2.04.8)

Version: 2.04.8

Aurora MySQL 2.04.8 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.
Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, and 2.05.*. You can restore a snapshot of any 2.* Aurora MySQL release into Aurora MySQL 2.04.8. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.04.8.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**

This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], Asia Pacific (Hong Kong) [ap-east-1], and Middle East (Bahrain) [me-south-1]. There will be a separate announcement once it is made available.

**Note**

For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

**Improvements**

**New features:**

- **Read replica improvements:**
  - Reduced network traffic from the writer instance by efficiently transmitting data to reader instances within the Aurora DB cluster. This improvement is enabled by default, because it helps prevent replicas from falling behind and restarting. The parameter for this feature is `aurora_enable_repl_bin_log_filtering`.
  - Reduced network traffic from the writer to reader instances within the Aurora DB cluster using compression. This improvement is enabled by default for 8xlarge and 16xlarge instance classes only, because these instances can tolerate additional CPU overhead for compression. The parameter for this feature is `aurora_enable_replica_log_compression`.

- **High-priority fixes:**
  - Improved memory management in the Aurora writer instance that prevents restart of writer due to out of memory conditions during heavy workload in presence of reader instances within the Aurora DB cluster.
  - Fix for a non-deterministic condition in the scheduler that results in engine restart while accessing the performance schema object concurrently.

**Comparison with Aurora MySQL version 1**

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

MySQL 5.7 compatibility

Aurora MySQL 2.04.8 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.04.8 does not currently support the following MySQL 5.7 features:

• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The CREATE TABLESPACE SQL statement

Aurora MySQL database engine updates 2019-11-14 (version 2.04.7)

Version: 2.04.7

Aurora MySQL 2.04.7 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.* and 2.04.*.

You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL 2.04.7. You also have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.04.7. You can’t upgrade an existing Aurora MySQL 1.* cluster directly to 2.04.7; however, you can restore its snapshot to Aurora MySQL 2.04.7.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], Asia Pacific (Hong Kong) [ap-east-1], and Middle East (Bahrain) [me-south-1]. There will be a separate announcement once it is made available.

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

907
Improvements

High-priority fixes:

Connection Handling

• Database availability has been improved to better service a surge in client connections while executing one or more DDLs. It is handled by temporarily creating additional threads when needed. You are advised to upgrade if the database becomes unresponsive following a surge in connections while processing DDL.
• Fixed an issue that resulted in an incorrect value for the Threads_running global status variable.

Engine Restart

• Fixed an issue of prolonged unavailability while restarting the engine. This addresses an issue in the buffer pool initialization. This issue occurs rarely but can potentially impact any supported release.

General stability fixes:

• Made improvements where queries accessing uncached data could be slower than usual. Customers experiencing unexplained elevated read latencies while accessing uncached data are encouraged to upgrade as they may be experiencing this issue.

Comparison with Aurora MySQL version 1

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

• Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
• Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
• Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
• Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

MySQL 5.7 compatibility

Aurora MySQL 2.04.7 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.04.7 does not currently support the following MySQL 5.7 features:

• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
Online buffer pool resizing
Password validation plugin
Query rewrite plugins
Replication filtering
The `CREATE TABLESPACE` SQL statement

**Aurora MySQL database engine updates 2019-09-19 (version 2.04.6)**

**Version:** 2.04.6

Aurora MySQL 2.04.6 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

You have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.04.6. We do not allow in-place upgrade of Aurora MySQL 1.* clusters. This restriction will be lifted in a later Aurora MySQL 2.* release. You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.* and 2.04.* into Aurora MySQL 2.04.6.

To use an older version of Aurora MySQL, you can create new database clusters by specifying the engine version through the AWS Management Console, the AWS CLI, or the Amazon RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**
This version is currently not available in the following AWS Regions: Europe (London) [eu-west-2], AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], and Asia Pacific (Hong Kong) [ap-east-1]. There will be a separate announcement once it is made available.

**Note**
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

**Improvements**

- Fixed an issue where the events in current binlog file on the master were not replicated on the worker if the value of the parameter `sync_binlog` was not set to 1.
- The default value of the parameter `aurora_binlog_replication_max_yield_seconds` has been changed to zero to prevent an increase in replication lag in favor of foreground query performance on the binlog master.

**Integration of MySQL bug fixes**

- Bug#23054591: PURGE BINARY LOGS TO is reading the whole binlog file and causing MySQL to Stall

**Comparison with Aurora MySQL version 1**

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
• Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
• Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
• Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

MySQL 5.7 compatibility

Aurora MySQL 2.04.6 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.04.6 does not currently support the following MySQL 5.7 features:
• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The CREATE TABLESPACE SQL statement

Aurora MySQL database engine updates 2019-07-08 (version 2.04.5)

Version: 2.04.5

Aurora MySQL 2.04.5 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

You have the option to upgrade existing Aurora MySQL 2.* database clusters to Aurora MySQL 2.04.5. We do not allow in-place upgrade of Aurora MySQL 1.* clusters. This restriction will be lifted in a later Aurora MySQL 2.* release. You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.* and 2.04.* into Aurora MySQL 2.04.5.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements
• Fixed a race condition during storage volume growth that caused the database to restart.
• Fixed an internal communication failure during volume open that caused the database to restart.
• Added DDL recovery support for `ALTER TABLE ALGORITHM=INPLACE` on partitioned tables.
• Fixed an issue with DDL recovery of `ALTER TABLE ALGORITHM=COPY` that caused the database to restart.
• Improved Aurora Replica stability under heavy delete workload on the writer.
• Fixed a database restart caused by a deadlatch between the thread performing full-text search index sync and the thread performing eviction of full-text search table from dictionary cache.
• Fixed a stability issue on the binlog worker during DDL replication while the connection to the binlog master is unstable.
• Fixed an out-of-memory issue in the full-text search code that caused the database to restart.
• Fixed an issue on the Aurora Writer that caused it to restart when the entire 64 tebibyte (TiB) volume is used.
• Fixed a race condition in the Performance Schema feature that caused the database to restart.
• Fixed an issue that caused aborted connections when handling an error in network protocol management.

Comparison with Aurora MySQL version 1

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

• Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
• Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
• Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
• Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

MySQL 5.7 compatibility

Aurora MySQL 2.04.5 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.04.5 does not currently support the following MySQL 5.7 features:

• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The CREATE TABLESPACE SQL statement

Aurora MySQL database engine updates 2019-05-29 (version 2.04.4)

Version: 2.04.4

Aurora MySQL 2.04.4 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster (including restoring a snapshot), you have the option of choosing compatibility with either MySQL 5.7 or MySQL 5.6. We do not allow in-place upgrade of Aurora MySQL 1.* clusters or restore of Aurora MySQL 1.* clusters from an Amazon S3 backup into Aurora MySQL 2.04.4. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.*, and 2.04.* into Aurora MySQL 2.04.4.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1], Europe (Stockholm) [eu-north-1], China (Ningxia) [cn-northwest-1], and Asia Pacific (Hong Kong) [ap-east-1] AWS Regions. There will be a separate announcement once it is made available.

Note
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

• Fixed an issue that could cause failures when loading data into Aurora from S3.
• Fixed an issue that could cause failures when upload data from Aurora to S3.
• Fixed an issue that caused aborted connections when handling an error in network protocol management.
• Fixed an issue that could cause a crash when dealing with partitioned tables.
• Fixed an issue with the Performance Insights feature being unavailable in some regions.

Comparison with Aurora MySQL version 1

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

• Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
• Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
• Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
• Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).
MySQL 5.7 compatibility

Aurora MySQL 2.04.4 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.04.4 does not currently support the following MySQL 5.7 features:

- Group replication plugin
- Increased page size
- InnoDB buffer pool loading at startup
- InnoDB full-text parser plugin
- Multisource replication
- Online buffer pool resizing
- Password validation plugin
- Query rewrite plugins
- Replication filtering
- The create tablespace SQL statement

Aurora MySQL database engine updates 2019-05-09 (version 2.04.3)

Version: 2.04.3

Aurora MySQL 2.04.3 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster (including restoring a snapshot), you have the option of choosing compatibility with either MySQL 5.7 or MySQL 5.6. We do not allow in-place upgrade of Aurora MySQL 1.* clusters or restore of Aurora MySQL 1.* clusters from an Amazon S3 backup into Aurora MySQL 2.04.3. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.*, and 2.04.* into Aurora MySQL 2.04.3.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note

This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Ningxia) [cn-northwest-1] AWS Regions. There will be a separate announcement once it is made available.

Note

For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

- Fixed a bug in binlog replication that can cause an issue on Aurora instances configured as binlog worker.
- Fixed an out-of-memory condition when handling large stored routines.
- Fixed an error in handling certain kinds of ALTER TABLE commands.
- Fixed an issue with aborted connections because of an error in network protocol management.
Comparison with Aurora MySQL version 1

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
- Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

MySQL 5.7 compatibility

Aurora MySQL 2.04.3 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.04.3 does not currently support the following MySQL 5.7 features:

- Group replication plugin
- Increased page size
- InnoDB buffer pool loading at startup
- InnoDB full-text parser plugin
- Multisource replication
- Online buffer pool resizing
- Password validation plugin
- Query rewrite plugins
- Replication filtering
- The CREATE TABLESPACE SQL statement

Aurora MySQL database engine updates 2019-05-02 (version 2.04.2)

Version: 2.04.2

Aurora MySQL 2.04.2 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster (including restoring a snapshot), you have the option of choosing compatibility with either MySQL 5.7 or MySQL 5.6. We do not allow in-place upgrade of Aurora MySQL 1.* clusters or restore of Aurora MySQL 1.* clusters from an Amazon S3 backup into Aurora MySQL 2.04.2. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.*, 2.04.0, and 2.04.1 into Aurora MySQL 2.04.2.
If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Ningxia) [cn-northwest-1] AWS Regions. There will be a separate announcement once it is made available.

**Note**
For information on how to upgrade your Aurora MySQL database cluster, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

**Improvements**

- Added support for SSL binlog replication using custom certificates. For information on using SSL binlog replication in Aurora MySQL, see mysql_rds_import_binlog_ssl_material.
- Fixed a dead latch on the Aurora primary instance that occurs when a table with a Full Text Search index is being optimized.
- Fixed an issue on the Aurora Replicas where performance of certain queries using SELECT(*) could be impacted on tables that have secondary indexes.
- Fixed a condition that resulted in Error 1032 being posted.
- Improved the stability of Aurora Replicas by fixing multiple deadlatches.

**Integration of MySQL bug fixes**

- Bug #24829050 - INDEX_MERGE_INTERSECTION OPTIMIZATION CAUSES WRONG QUERY RESULTS

**Comparison with Aurora MySQL version 1**

The following Amazon Aurora MySQL features are supported in Aurora MySQL Version 1 (compatible with MySQL 5.6), but these features are currently not supported in Aurora MySQL Version 2 (compatible with MySQL 5.7).

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
- Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

**MySQL 5.7 compatibility**

Aurora MySQL 2.04.2 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.04.2 does not currently support the following MySQL 5.7 features:

- Group replication plugin
- Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The `CREATE TABLESPACE` SQL statement

Aurora MySQL database engine updates 2019-03-25 (version 2.04.1)

Version: 2.04.1

Aurora MySQL 2.04.1 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster (including restoring a snapshot), you have the option of choosing compatibility with either MySQL 5.7 or MySQL 5.6. We do not allow in-place upgrade of Aurora MySQL 1.* clusters or restore of Aurora MySQL 1.* clusters from an Amazon S3 backup into Aurora MySQL 2.04.1. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 2.01.*, 2.02.*, 2.03.*, 2.04.0 into Aurora MySQL 2.04.1.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] region. There will be a separate announcement once it is made available.

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

• Fixed an issue where an Aurora MySQL 5.6 snapshot for versions lower than 1.16 could not be restored to the latest Aurora MySQL 5.7 cluster.

Aurora MySQL database engine updates 2019-03-25 (version 2.04)

Version: 2.04

Aurora MySQL 2.04 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster (including restoring a snapshot), you have the option of choosing compatibility with either MySQL 5.7 or MySQL 5.6. We do not allow in-place upgrade of Aurora MySQL 1.* clusters or restore of Aurora MySQL 1.* clusters from an Amazon S3 backup into Aurora MySQL 2.04.0. We plan to remove these restrictions in a later Aurora MySQL 2.* release.
You can restore snapshots of Aurora MySQL 1.19.*, 2.01.*, 2.02.*, and 2.03.* into Aurora MySQL 2.04.0. You cannot restore snapshots of Aurora MySQL 1.14.* or lower, 1.15.*, 1.16.*, 1.17.*, 1.18.* into Aurora MySQL 2.04.0. This restriction is removed in Aurora MySQL 2.04.1.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] region. There will be a separate announcement once it is made available.

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

• Supports GTID-based replication. For information about using GTID-based replication with Aurora MySQL, see Using GTID-based replication for Aurora MySQL (p. 762).

• Fixed an issue where an Aurora Replica incorrectly throws a Running in read-only mode error when a statement deleting or updating rows in a temporary table contains an InnoDB subquery.

Integration of MySQL bug fixes

• Bug #26225783: MYSQL CRASH ON CREATE TABLE (REPRODUCEABLE) -> INNODB: ALONG SEMAPHORE WAIT.

Aurora MySQL database engine updates 2019-02-07

Version: 2.03.4

Aurora MySQL 2.03.4 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster (including restoring a snapshot), you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

We don't allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.03.4 or restore to Aurora MySQL 2.03.4 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

• Support for UTF8MB4 Unicode 9.0 accent-sensitive and case-insensitive collation, utf8mb4_0900_as_ci.
Aurora MySQL database engine updates 2019-01-18

Version: 2.03.3

Aurora MySQL 2.03.3 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster (including restoring a snapshot), you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

We don't allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.03.3 or restore to Aurora MySQL 2.03.3 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

- Fixed an issue where an Aurora Replica might become dead-latched when running a backward scan on an index.
- Fixed an issue where an Aurora Replica might restart when the Aurora primary instance runs in-place DDL operations on partitioned tables.
- Fixed an issue where an Aurora Replica might restart during query cache invalidation after a DDL operation on the Aurora primary instance.
- Fixed an issue where an Aurora Replica might restart during a SELECT query on a table while the Aurora primary instance runs truncation on that table.
- Fixed a wrong result issue with MyISAM temporary tables where only indexed columns are accessed.
- Fixed an issue in slow logs that generated incorrect large values for `query_time` and `lock_time` periodically after approximately 40,000 queries.
- Fixed an issue where a schema named "tmp" could cause migration from RDS MySQL to Aurora MySQL to become stuck.
- Fixed an issue where the audit log might have missing events during log rotation.
- Fixed an issue where the Aurora primary instance restored from an Aurora 5.6 snapshot might restart when the Fast DDL feature in the lab mode is enabled.
- Fixed an issue where the CPU usage is 100% caused by the dictionary stats thread.
- Fixed an issue where an Aurora Replica might restart when running a `CHECK TABLE` statement.

Integration of MySQL bug fixes

- Bug #25361251: INCORRECT BEHAVIOR WITH INSERT ON DUPLICATE KEY IN SP
- Bug #26734162: INCORRECT BEHAVIOR WITH INSERT OF BLOB + ON DUPLICATE KEY UPDATE
- Bug #27460607: INCORRECT BEHAVIOR OF IODKU WHEN INSERT SELECT's SOURCE TABLE IS EMPTY
- SELECT DISTINCT NOT RETURNING DISTINCT ROWS IN 5.7 (Bug #22343910)
- Delete from joined tables with where using derived table fails with error 1093 (Bug #23074801).
• GCOLS: INCORRECT BEHAVIOR WITH CHARSET CHANGES (Bug #25287633).

Aurora MySQL database engine updates 2019-01-09

Version: 2.03.2

Aurora MySQL 2.03.2 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster (including restoring a snapshot), you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

We don't allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.03.2 or restore to Aurora MySQL 2.03.2 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

• Aurora Version Selector – Starting with Aurora MySQL 2.03.2, you can choose from among multiple versions of MySQL 5.7-compatible Aurora on the AWS Management Console. For more information, see Checking or specifying Aurora MySQL engine versions through AWS (p. 874).

Aurora MySQL database engine updates 2018-10-24

Version: 2.03.1

Aurora MySQL 2.03.1 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, you can choose compatibility with either MySQL 5.7 or MySQL 5.6. When restoring a MySQL 5.6-compatible snapshot, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 2.01.*, 2.02.*, and 2.03 into Aurora MySQL 2.03.1.

We don't allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.03.1 or restore to Aurora MySQL 2.03.1 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.
Improvements

• Fix an issue where the Aurora Writer might restart when running transaction deadlock detection.

Aurora MySQL database engine updates 2018-10-11

Version: 2.03

Aurora MySQL 2.03 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, you can choose compatibility with either MySQL 5.7 or MySQL 5.6. When restoring a MySQL 5.6-compatible snapshot, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 2.01.*, and 2.02.* into Aurora MySQL 2.03.

We don't allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.03 or restore to Aurora MySQL 2.03 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

• Performance schema is available.
• Fixed an issue where zombie sessions with killed state might consume more CPU.
• Fixed a dead latch issue when a read-only transaction is acquiring a lock on a record on the Aurora Writer.
• Fixed an issue where the Aurora Replica without customer workload might have high CPU utilization.
• Multiple fixes on issues that might cause the Aurora Replica or the Aurora writer to restart.
• Added capability to skip diagnostic logging when the disk throughput limit is reached.
• Fixed a memory leak issue when binlog is enabled on the Aurora Writer.

Integration of MySQL community edition bug fixes

• REVERSE SCAN ON A PARTITIONED TABLE DOES ICP - ORDER BY DESC (Bug #24929748).
• JSON_OBJECT CREATES INVALID JSON CODE (Bug#26867509).
• INSERTING LARGE JSON DATA TAKES AN INORDINATE AMOUNT OF TIME (Bug #22843444).
• PARTITIONED TABLES USE MORE MEMORY IN 5.7 THAN 5.6 (Bug #25080442).

Aurora MySQL database engine updates 2018-10-08

Version: 2.02.5
Aurora MySQL 2.02.5 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, you can choose compatibility with either MySQL 5.7 or MySQL 5.6. When restoring a MySQL 5.6-compatible snapshot, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 2.01.*, and 2.02.* into Aurora MySQL 2.02.5. You can also perform an in-place upgrade from Aurora MySQL 2.01.* or 2.02.* to Aurora MySQL 2.02.5.

We don’t allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.02.5 or restore to Aurora MySQL 2.02.5 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

The performance schema is disabled for this release of Aurora MySQL 5.7. Upgrade to Aurora 2.03 for performance schema support.

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

• Fix an issue where an Aurora Replica might restart when it is doing a reverse scan on a table.

Aurora MySQL database engine updates 2018-09-21

Version: 2.02.4

Aurora MySQL 2.02.4 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, you can choose compatibility with either MySQL 5.7 or MySQL 5.6. When restoring a MySQL 5.6-compatible snapshot, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 2.01.*, and 2.02.* into Aurora MySQL 2.02.4. You can also perform an in-place upgrade from Aurora MySQL 2.01.* or 2.02.* to Aurora MySQL 2.02.4.

We don’t allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.02.4 or restore to Aurora MySQL 2.02.4 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

The performance schema is disabled for this release of Aurora MySQL 5.7. Upgrade to Aurora 2.03 for performance schema support.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

• Fixed a stability issue related to Full Text Search indexes on tables restored from an Aurora MySQL 5.6 snapshot.
Integration of MySQL community edition bug fixes

- BUG#13651665 INNODB MAY BE UNABLE TO LOAD TABLE DEFINITION AFTER RENAME
- BUG#21371070 INNODB: CANNOT_ALLOCATE 0_BYTES.
- BUG#21378944 FTS ASSERT ENC.SRC_ILIST_PTR != NULL, FTS_OPTIMIZE_WORD(), OPTIMIZE TABLE
- BUG#21508537 ASSERTION FAILURE UT_A(!VICTIM_TRX->READ_ONLY)
- BUG#21983865 UNEXPECTED DEADLOCK WITH INNODB_AUTOINC_LOCK_MODE=0
- BUG#22679185 INVALID INNODB FTS DOC ID DURING INSERT
- BUG#22899305 GCOLS: ASSERTION: !(COL->PRTYPE & 256).
- BUG#22956469 MEMORY LEAK INTRODUCED IN 5.7.8 IN MEMORY/INNODB/OS0FILE
- BUG#22996488 CRASH IN FTS_SYNC_INDEX WHEN DOING DDL IN A LOOP
- BUG#23014521 GCOL:INNODB: ASSERTION: !IS_V
- BUG#23021168 REPLICATION STOPS AFTER TRX IS ROLLED BACK ASYNC
- BUG#23052231 ASSERTION: ADD_AUTOINC < DICT_TABLE_GET_N_USER_COLS
- BUG#23149683 ROTATE INNODB MASTER KEY WITH KEYRING_OKV_CONF_DIR MISSING: SIGSEGV; SIGNAL 11
- BUG#23762382 INSERT VALUES QUERY WITH JOIN IN A SELECT CAUSES INCORRECT BEHAVIOR
- BUG#25209512 CURRENT_TIMESTAMP PRODUCES ZEROS IN TRIGGER
- BUG#26626277 BUG IN "INSERT... ON DUPLICATE KEY UPDATE" QUERY
- BUG#26734162 INCORRECT BEHAVIOR WITH INSERT OF BLOB + ON DUPLICATE KEY UPDATE
- BUG#27460607 INCORRECT WHEN INSERT SELECT's SOURCE TABLE IS EMPTY

Aurora MySQL database engine updates 2018-08-23

Version: 2.02.3

Aurora MySQL 2.02.3 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, you can choose compatibility with either MySQL 5.7 or MySQL 5.6. When restoring a MySQL 5.6-compatible snapshot, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 2.01.*, and 2.02.* into Aurora MySQL 2.02.3. You can also perform an in-place upgrade from Aurora MySQL 2.01.* or 2.02.* to Aurora MySQL 2.02.3.

We don’t allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.02.3 or restore to Aurora MySQL 2.02.3 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

The performance schema is disabled for this release of Aurora MySQL 5.7. Upgrade to Aurora 2.03 for performance schema support.

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).
Comparison with Aurora MySQL 5.6

The following Amazon Aurora MySQL features are supported in Aurora MySQL 5.6, but these features are currently not supported in Aurora MySQL 5.7.

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. These functions are available for MySQL 5.7-compatible clusters in Aurora MySQL 2.06 and higher. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
- Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

Currently, Aurora MySQL 2.01 does not support features added in Aurora MySQL version 1.16 and later. For information about Aurora MySQL version 1.16, see Aurora MySQL database engine updates 2017-12-11 (p. 955).

MySQL 5.7 compatibility

Aurora MySQL 2.02.3 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.02.3 does not currently support the following MySQL 5.7 features:

- Global transaction identifiers (GTIDs). Aurora MySQL supports GTIDs in version 2.04 and higher.
- Group replication plugin
- Increased page size
- InnoDB buffer pool loading at startup
- InnoDB full-text parser plugin
- Multisource replication
- Online buffer pool resizing
- Password validation plugin
- Query rewrite plugins
- Replication filtering
- The CREATE TABLESPACE SQL statement
- X Protocol

CLI differences between Aurora MySQL 2.x and Aurora MySQL 1.x

- The engine name for Aurora MySQL 2.x is aurora-mysql; the engine name for Aurora MySQL 1.x continues to be aurora.
- The engine version for Aurora MySQL 2.x is 5.7.12; the engine version for Aurora MySQL 1.x continues to be 5.6.10ann.
- The default parameter group for Aurora MySQL 2.x is default.aurora-mysql5.7; the default parameter group for Aurora MySQL 1.x continues to be default.aurora5.6.
- The DB cluster parameter group family name for Aurora MySQL 2.x is aurora-mysql5.7; the DB cluster parameter group family name for Aurora MySQL 1.x continues to be aurora5.6.
Refer to the Aurora documentation for the full set of CLI commands and differences between Aurora MySQL 2.x and Aurora MySQL 1.x.

**Improvements**

- Fixed an issue where an Aurora Replica can restart when using optimistic cursor restores while reading records.
- Updated the default value of the parameter `innodb_stats_persistent_sample_pages` to 128 to improve index statistics.
- Fixed an issue where an Aurora Replica might restart when it accesses a small table that is being concurrently modified on the Aurora primary instance.
- Fixed `ANALYZE TABLE` to stop flushing the table definition cache.
- Fixed an issue where the Aurora primary instance or an Aurora Replica might restart when converting a point query for geospatial to a search range.

**Aurora MySQL database engine updates 2018-06-04**

**Version:** 2.02.2

Aurora MySQL 2.02.2 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, you can choose compatibility with either MySQL 5.7 or MySQL 5.6. When restoring a MySQL 5.6-compatible snapshot, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14*, 1.15*, 1.16*, 1.17*, 2.01*, and 2.02 into Aurora MySQL 2.02.2. You can also perform an in-place upgrade from Aurora MySQL 2.01* or 2.02 to Aurora MySQL 2.02.2.

We don’t allow in-place upgrade of Aurora MySQL 1.* clusters into Aurora MySQL 2.02.2 or restore to Aurora MySQL 2.02.2 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.* release.

The performance schema is disabled for this release of Aurora MySQL 5.7. Upgrade to Aurora 2.03 for performance schema support.

**Note**

This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Comparison with Aurora MySQL 5.6**

The following Amazon Aurora MySQL features are supported in Aurora MySQL 5.6, but these features are currently not supported in Aurora MySQL 5.7.

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

Currently, Aurora MySQL 2.01 does not support features added in Aurora MySQL version 1.16 and later. For information about Aurora MySQL version 1.16, see Aurora MySQL database engine updates 2017-12-11 (p. 955).

MySQL 5.7 compatibility

Aurora MySQL 2.02.2 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.02.2 does not currently support the following MySQL 5.7 features:

• Global transaction identifiers (GTIDs). Aurora MySQL supports GTIDs in version 2.04 and higher.
• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The CREATE TABLESPACE SQL statement
• X Protocol

CLI differences between Aurora MySQL 2.x and Aurora MySQL 1.x

• The engine name for Aurora MySQL 2.x is aurora-mysql; the engine name for Aurora MySQL 1.x continues to be aurora.
• The engine version for Aurora MySQL 2.x is 5.7.12; the engine version for Aurora MySQL 1.x continues to be 5.6.10aann.
• The default parameter group for Aurora MySQL 2.x is default.aurora-mysql5.7; the default parameter group for Aurora MySQL 1.x continues to be default.aurora5.6.
• The DB cluster parameter group family name for Aurora MySQL 2.x is aurora-mysql5.7; the DB cluster parameter group family name for Aurora MySQL 1.x continues to be aurora5.6.

Refer to the Aurora documentation for the full set of CLI commands and differences between Aurora MySQL 2.x and Aurora MySQL 1.x.

Improvements

• Fixed an issue where an Aurora Writer can occasionally restart when tracking Aurora Replica progress.
• Fixed an issue where an Aurora Replica restarts or throws an error when a partitioned table is accessed after running index create or drop statements on the table on the Aurora Writer.
• Fixed an issue where a table on an Aurora Replica is inaccessible while it is applying the changes caused by running ALTER table ADD/DROP column statements on the Aurora Writer.
Aurora MySQL database engine updates 2018-05-03

Version: 2.02

Aurora MySQL 2.02 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, you can choose compatibility with either MySQL 5.7 or MySQL 5.6. When restoring a MySQL 5.6-compatible snapshot, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14*, 1.15*, 1.16*, 1.17* and 2.01* into Aurora MySQL 2.02. You can also perform an in-place upgrade from Aurora MySQL 2.01* to Aurora MySQL 2.02.

We don't allow in-place upgrade of Aurora MySQL 1.x clusters into Aurora MySQL 2.02 or restore to Aurora MySQL 2.02 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.x release.

The performance schema is disabled for this release of Aurora MySQL 5.7. Upgrade to Aurora 2.03 for performance schema support.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Comparison with Aurora MySQL 5.6

The following Amazon Aurora MySQL features are supported in Aurora MySQL 5.6, but these features are currently not supported in Aurora MySQL 5.7.

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
- Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

Currently, Aurora MySQL 2.01 does not support features added in Aurora MySQL version 1.16 and later. For information about Aurora MySQL version 1.16, see Aurora MySQL database engine updates 2017-12-11 (p. 955).

MySQL 5.7 compatibility

Aurora MySQL 2.02 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.02 does not currently support the following MySQL 5.7 features:

- Global transaction identifiers (GTIDs). Aurora MySQL supports GTIDs in version 2.04 and higher.
- Group replication plugin
- Increased page size
- InnoDB buffer pool loading at startup
Amazon Aurora User Guide for Aurora
Database engine updates for Amazon Aurora MySQL 2.0

- InnoDB full-text parser plugin
- Multisource replication
- Online buffer pool resizing
- Password validation plugin
- Query rewrite plugins
- Replication filtering
- The `CREATE TABLESPACE` SQL statement
- X Protocol

**CLI differences between Aurora MySQL 2.x and Aurora MySQL 1.x**

- The engine name for Aurora MySQL 2.x is `aurora-mysql`; the engine name for Aurora MySQL 1.x continues to be `aurora`.
- The engine version for Aurora MySQL 2.x is 5.7.12; the engine version for Aurora MySQL 1.x continues to be 5.6.10a.nn.
- The default parameter group for Aurora MySQL 2.x is `default.aurora-mysql5.7`; the default parameter group for Aurora MySQL 1.x continues to be `default.aurora5.6`.
- The DB cluster parameter group family name for Aurora MySQL 2.x is `aurora-mysql5.7`; the DB cluster parameter group family name for Aurora MySQL 1.x continues to be `aurora5.6`.

Refer to the Aurora documentation for the full set of CLI commands and differences between Aurora MySQL 2.x and Aurora MySQL 1.x.

**Improvements**

- Fixed an issue where an Aurora Writer restarts when running INSERT statements and exploiting the Fast Insert optimization.
- Fixed an issue where an Aurora Replica restarts when running ALTER DATABASE statements on the Aurora Replica.
- Fixed an issue where an Aurora Replica restarts when running queries on tables that have just been dropped on the Aurora Writer.
- Fixed an issue where an Aurora Replica restarts when setting `innodb_adaptive_hash_index` to `OFF` on the Aurora Replica.
- Fixed an issue where an Aurora Replica restarts when running TRUNCATE TABLE queries on the Aurora Writer.
- Fixed an issue where the Aurora Writer freezes in certain circumstances when running INSERT statements. On a multi-node cluster, this can result in a failover.
- Fixed a memory leak associated with setting session variables.
- Fixed an issue where the Aurora Writer freezes in certain circumstances associated with purging undo for tables with generated columns.
- Fixed an issue where the Aurora Writer can sometimes restart when binary logging is enabled.

**Integration of MySQL bug fixes**

- Left join returns incorrect results on the outer side (Bug #22833364).

**Aurora MySQL database engine updates 2018-03-13**

*Version:* 2.01.1
Aurora MySQL 2.01.1 is generally available. Aurora MySQL 2.x versions are compatible with MySQL 5.7 and Aurora MySQL 1.x versions are compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, you can choose compatibility with either MySQL 5.7 or MySQL 5.6. When restoring a MySQL 5.6-compatible snapshot, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14*, 1.15*, 1.16*, and 1.17* into Aurora MySQL 2.01.1.

We don't allow in-place upgrade of Aurora MySQL 1.x clusters into Aurora MySQL 2.01.1 or restore to Aurora MySQL 2.01.1 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.x release.

The performance schema is disabled for this release of Aurora MySQL 5.7. Upgrade to Aurora 2.03 for performance schema support.

**Comparison with Aurora MySQL 5.6**

The following Amazon Aurora MySQL features are supported in Aurora MySQL 5.6, but these features are currently not supported in Aurora MySQL 5.7.

- Asynchronous key prefetch (AKP). For more information, see Working with asynchronous key prefetch in Amazon Aurora (p. 842).
- Hash joins. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. For more information, see Invoking a Lambda function with an Aurora MySQL native function (p. 819).
- Scan batching. For more information, see Aurora MySQL database engine updates 2017-12-11 (p. 955).
- Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

Currently, Aurora MySQL 2.01.1 does not support features added in Aurora MySQL version 1.16 and later. For information about Aurora MySQL version 1.16, see Aurora MySQL database engine updates 2017-12-11 (p. 955).

**MySQL 5.7 compatibility**

Aurora MySQL 2.01.1 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.01.1 does not currently support the following MySQL 5.7 features:

- Global transaction identifiers (GTIDs). Aurora MySQL supports GTIDs in version 2.04 and higher.
- Group replication plugin
- Increased page size
- InnoDB buffer pool loading at startup
- InnoDB full-text parser plugin
- Multisource replication
- Online buffer pool resizing
- Password validation plugin
- Query rewrite plugins
- Replication filtering
There are no visible images or diagrams in the text.

- The `CREATE TABLESPACE` SQL statement
- X Protocol

**CLI differences between Aurora MySQL 2.x and Aurora MySQL 1.x**

- The engine name for Aurora MySQL 2.x is `aurora-mysql`; the engine name for Aurora MySQL 1.x continues to be `aurora`.
- The engine version for Aurora MySQL 2.x is `5.7.12`; the engine version for Aurora MySQL 1.x continues to be `5.6.10ann`.
- The default parameter group for Aurora MySQL 2.x is `default.aurora-mysql5.7`; the default parameter group for Aurora MySQL 1.x continues to be `default.aurora5.6`.
- The DB cluster parameter group family name for Aurora MySQL 2.x is `aurora-mysql5.7`; the DB cluster parameter group family name for Aurora MySQL 1.x continues to be `aurora5.6`.

Refer to the Aurora documentation for the full set of CLI commands and differences between Aurora MySQL 2.x and Aurora MySQL 1.x.

**Improvements**

- Fixed an issue with snapshot restore where Aurora-specific database privileges were created incorrectly when a MySQL 5.6-compatible snapshot was restored with MySQL 5.7 compatibility.
- Added support for 1.17 snapshot restores.

**Aurora MySQL database engine updates 2018-02-06**

**Version:** 2.01

Aurora MySQL 2.01 is generally available. Going forward, Aurora MySQL 2.x versions will be compatible with MySQL 5.7 and Aurora MySQL 1.x versions will be compatible with MySQL 5.6.

When creating a new Aurora MySQL DB cluster, including those restored from snapshots, you can choose compatibility with either MySQL 5.7 or MySQL 5.6.

You can restore snapshots of Aurora MySQL 1.14*, 1.15*, and 1.16* into Aurora MySQL 2.01.

We don’t allow in-place upgrade of Aurora MySQL 1.x clusters into Aurora MySQL 2.01 or restore to Aurora MySQL 2.01 from an Amazon S3 backup. We plan to remove these restrictions in a later Aurora MySQL 2.x release.

The performance schema is disabled for this release of Aurora MySQL 5.7. Upgrade to Aurora 2.03 for performance schema support.

**Comparison with Aurora MySQL 5.6**

The following Amazon Aurora MySQL features are supported in Aurora MySQL 5.6, but these features are currently not supported in Aurora MySQL 5.7.

- Asynchronous key prefetch (AKP). For more information, see "Working with asynchronous key prefetch in Amazon Aurora" (p. 842).
- Hash joins. For more information, see "Working with hash joins in Aurora MySQL" (p. 845).
- Native functions for synchronously invoking AWS Lambda functions. For more information, see "Invoking a Lambda function with an Aurora MySQL native function" (p. 819).
- Scan batching. For more information, see "Aurora MySQL database engine updates 2017-12-11" (p. 955).
• Migrating data from MySQL using an Amazon S3 bucket. For more information, see Migrating data from MySQL by using an Amazon S3 bucket (p. 646).

Currently, Aurora MySQL 2.01 does not support features added in Aurora MySQL version 1.16 and later. For information about Aurora MySQL version 1.16, see Aurora MySQL database engine updates 2017-12-11 (p. 955).

MySQL 5.7 compatibility

Aurora MySQL 2.01 is wire-compatible with MySQL 5.7 and includes features such as JSON support, spatial indexes, and generated columns. Aurora MySQL uses a native implementation of spatial indexing using z-order curves to deliver >20x better write performance and >10x better read performance than MySQL 5.7 for spatial datasets.

Aurora MySQL 2.01 does not currently support the following MySQL 5.7 features:
• Global transaction identifiers (GTIDs). Aurora MySQL supports GTIDs in version 2.04 and higher.
• Group replication plugin
• Increased page size
• InnoDB buffer pool loading at startup
• InnoDB full-text parser plugin
• Multisource replication
• Online buffer pool resizing
• Password validation plugin
• Query rewrite plugins
• Replication filtering
• The CREATE TABLESPACE SQL statement
• X Protocol

CLI differences between Aurora MySQL 2.x and Aurora MySQL 1.x

• The engine name for Aurora MySQL 2.x is aurora-mysql; the engine name for Aurora MySQL 1.x continues to be aurora.
• The engine version for Aurora MySQL 2.x is 5.7.12; the engine version for Aurora MySQL 1.x continues to be 5.6.10a.nn.
• The default parameter group for Aurora MySQL 2.x is default.aurora-mysql5.7; the default parameter group for Aurora MySQL 1.x continues to be default.aurora5.6.
• The DB cluster parameter group family name for Aurora MySQL 2.x is aurora-mysql5.7; the DB cluster parameter group family name for Aurora MySQL 1.x continues to be aurora5.6.

Refer to the Aurora documentation for the full set of CLI commands and differences between Aurora MySQL 2.x and Aurora MySQL 1.x.

Database engine updates for Amazon Aurora MySQL 1.1

The following are Amazon Aurora 1.1 database engine updates:
• Aurora MySQL database engine updates 2020-11-24 (version 1.23.1) (p. 932)
• Aurora MySQL database engine updates 2020-09-02 (version 1.23.0) (p. 932)
• Aurora MySQL database engine updates 2020-11-09 (version 1.22.3) (p. 935)
• Aurora MySQL database engine updates 2020-03-05 (version 1.22.2) (p. 937)
• Aurora MySQL database engine updates 2019-12-23 (version 1.22.1) (p. 937)
• Aurora MySQL database engine updates 2019-11-25 (version 1.22.0) (p. 938)
• Aurora MySQL database engine updates 2019-11-25 (version 1.21.0) (p. 941)
• Aurora MySQL database engine updates 2020-03-05 (version 1.20.1) (p. 942)
• Aurora MySQL database engine updates 2019-11-11 (version 1.20.0) (p. 943)
• Aurora MySQL database engine updates 2020-03-05 (version 1.19.6) (p. 944)
• Aurora MySQL database engine updates 2019-09-19 (version 1.19.5) (p. 945)
• Aurora MySQL database engine updates 2019-06-05 (version 1.19.2) (p. 946)
• Aurora MySQL database engine updates 2019-05-09 (version 1.19.1) (p. 946)
• Aurora MySQL database engine updates 2019-02-07 (version 1.19.0) (p. 947)
• Aurora MySQL database engine updates 2018-09-20 (p. 948) (Version 1.18.0)
• Aurora MySQL database engine updates 2020-03-05 (p. 949) (Version 1.17.9)
• Aurora MySQL database engine updates 2019-01-17 (p. 949) (Version 1.17.8)
• Aurora MySQL database engine updates 2018-10-08 (p. 950) (Version 1.17.7)
• Aurora MySQL database engine updates 2018-09-06 (p. 951) (Version 1.17.6)
• Aurora MySQL database engine updates 2018-08-14 (p. 952) (Version 1.17.5)
• Aurora MySQL database engine updates 2018-08-07 (p. 952) (Version 1.17.4)
• Aurora MySQL database engine updates 2018-06-05 (p. 953) (Version 1.17.3)
• Aurora MySQL database engine updates 2018-04-27 (p. 953) (Version 1.17.2)
• Aurora MySQL database engine updates 2018-03-23 (p. 954) (Version 1.17.1)
• Aurora MySQL database engine updates 2018-03-13 (p. 954) (Version 1.17)
• Aurora MySQL database engine updates 2017-12-11 (p. 955) (Version 1.16)
• Aurora MySQL database engine updates 2017-11-20 (p. 956) (Version 1.15.1)
• Aurora MySQL database engine updates 2017-10-24 (p. 957) (Version 1.15)
• Aurora MySQL database engine updates: 2018-03-13 (p. 959) (Version 1.14.4)
• Aurora MySQL database engine updates: 2017-09-22 (p. 959) (Version 1.14.1)
• Aurora MySQL database engine updates: 2017-08-07 (p. 960) (Version 1.14)
• Aurora MySQL database engine updates: 2017-05-15 (p. 961) (Version 1.13)
• Aurora MySQL database engine updates: 2017-04-05 (p. 962) (Version 1.12)
• Aurora MySQL database engine updates: 2017-02-23 (p. 964) (Version 1.11)
• Aurora MySQL database engine updates: 2017-01-12 (p. 966) (Version 1.10.1)
• Aurora MySQL database engine updates: 2016-12-14 (p. 966) (Version 1.10)
• Aurora MySQL database engine updates: 2016-11-10 (p. 967) (Versions 1.9.0, 1.9.1)
• Aurora MySQL database engine updates: 2016-10-26 (p. 968) (Version 1.8.1)
• Aurora MySQL database engine updates: 2016-10-18 (p. 968) (Version 1.8)
• Aurora MySQL database engine updates: 2016-09-20 (p. 970) (Version 1.7.1)
• Aurora MySQL database engine updates: 2016-08-30 (p. 970) (Version 1.7)
• Aurora MySQL database engine updates: 2016-06-01 (p. 971) (Version 1.6.5)
• Aurora MySQL database engine updates: 2016-04-06 (p. 971) (Version 1.6)
• Aurora MySQL database engine updates: 2016-01-11 (p. 973) (Version 1.5)
• Aurora MySQL database engine updates: 2015-12-03 (p. 973) (Version 1.4)
Aurora MySQL database engine updates 2020-11-24 (version 1.23.1)

Version: 1.23.1

Aurora MySQL 1.23.1 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases for upgrade to 1.23.1 are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, and 1.23.*.

To create a cluster with an older version of Aurora MySQL, specify the engine version through the RDS Console, the AWS CLI, or the Amazon RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

Security fixes:

Fixes and other enhancements to fine-tune handling in a managed environment. Additional CVE fixes below:

- CVE-2020-14559
- CVE-2020-14539

Availability improvements:

- Fixed an issue that causes an Aurora reader instance in a global database secondary cluster running 1.23.0 to restart repeatedly.
- Fixed an issue where a global database secondary Region's replicas might restart when upgraded to release 1.23.0 while the primary Region writer was on an older release version.
- Fixed a memory leak in dynamic resizing feature, introduced in Aurora MySQL 1.23.0.
- Fixed an issue that might cause server restart during execution of a query using the parallel query feature.
- Fixed an issue that might cause a client session to hang when the database engine encounters an error while reading from or writing to the network.

Aurora MySQL database engine updates 2020-09-02 (version 1.23.0)

Version: 1.23.0

Aurora MySQL 1.23.0 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 1.23.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, 2.07.*, 2.08.*, and 2.09.*. You can restore the snapshot of an Aurora MySQL 1.* database into Aurora MySQL 1.23.0.
Important
The improvements to Aurora storage in this version limit the available upgrade paths from Aurora MySQL 1.23 to Aurora MySQL 2.*. When you upgrade an Aurora MySQL 1.23 cluster to 2.*, you must upgrade to Aurora MySQL 2.09.0 or later.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the RDS Console, the AWS CLI, or the Amazon RDS API.

Note
This version is currently not available in the following regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

New features:
- You can now turn parallel query on or off for an existing cluster by changing the value of the DB cluster parameter `aurora_parallel_query`. You don't need to use the `parallelquery` setting for the `--engine-mode` parameter when creating the cluster.

Parallel query is now expanded to be available in all regions where Aurora MySQL is available.

There are a number of other functionality enhancements and changes to the procedures for upgrading and enabling parallel query in an Aurora cluster. For more information, see Working with parallel query for Amazon Aurora MySQL (p. 697).

- With this release, you can create Amazon Aurora MySQL database instances with up to 128 tebibytes (TiB) of storage. The new storage limit is an increase from the prior 64 TiB. The 128 TiB storage size supports larger databases. This capability is not supported on small instances sizes (db.t2 or db.t3). A single tablespace cannot grow beyond 64 TiB due to InnoDB limitations with 16 KB page size.

Aurora alerts you when the cluster volume size is near 128 TiB, so that you can take action prior to hitting the size limit. The alerts appear in the mysql log and RDS Events in the AWS Management Console.

- Improved binary log (binlog) processing to reduce crash recovery time and commit time latency when very large transactions are involved.

- Aurora dynamically resizes your cluster storage space. With dynamic resizing, the storage space for your Aurora DB cluster automatically decreases when you remove data from the DB cluster. For more information, see Storage scaling (p. 349).

Note
The dynamic resizing feature is being deployed in phases to the AWS Regions where Aurora is available. Depending on the Region where your cluster is, this feature might not be available yet. For more information, see the What's New announcement.

High priority fixes:
- CVE-2019-2911
- CVE-2019-2537
- CVE-2018-2787
- CVE-2018-2784
- CVE-2018-2645
- CVE-2018-2640
Availability improvements:

- Fixed an issue in the lock manager where a race condition can cause a lock to be shared by two transactions, causing the database to restart.
- Fixed an issue related to transaction lock memory management with long-running write transactions resulting in a database restart.
- Fixed a race condition in the lock manager that resulted in a database restart or failover during transaction rollback.
- Fixed an issue during upgrade from 5.6 to 5.7 when the innodb_file_format changed on a table that had Fast DDL enabled.
- Fixed multiple issues where the engine might restart during zero-downtime patching while checking for a quiesced point in database activity for patching.
- Fixed an issue related to DDL recovery that impacts restart of the DB instance while recovering an interrupted DROP TRIGGER operation.
- Fixed a bug that might cause unavailability of the database if a crash occurs during the execution of certain partitioning operations. Specifically, an interrupted ALTER TABLE operation that modifies the type of partitioning or the number of partitions in a table.
- Fix default value of table_open_cache on 16XL and 24XL instances which could cause repeated failovers and high CPU utilization on large instances classes (R4/R5-16XL, R5-12XL, R5-24XL). This impacted 1.21.x and 1.22.x.

Global databases:

- Populate missing data in the MySQL INFORMATION_SCHEMA.REPLICA_HOST_STATUS view on primary and secondary AWS Regions in an Aurora global database.
- Fixed unexpected query failures that could occur in a Global DB secondary Region due to garbage collection of UNDO records in the primary Region, after temporary network connectivity issues between the primary and secondary Regions.

Parallel query:

- Fixed an issue where parallel query might cause a long-running query to return an empty result.
- Fixed an issue where a query on a small table on the Aurora read replica might take more than one second.
- Fixed an issue that might cause a restart when a parallel query and a DML statement are executing concurrently under a heavy workload.

General improvements:

- Fixed an issue where queries using spatial index might return partial results if spatial index was created on tables with already existing large spatial values.
- Increased maximum allowable length for audit system variables server_audit_incl_users and server_audit_excl_users from 1024 bytes to 2000 bytes.
- Fixed an issue where a binlog replica connected to an Aurora MySQL binlog primary might show incomplete data when the Aurora MySQL binlog primary loads data from S3 under statement binlog_format.
- Comply with community behavior to map mixed binlog_format to row instead of statement for loading data.
- Fixed an issue causing binlog replication to stop working when the user closes the connection and the session is using temporary tables.
- Improved response time of a query involving MyISAM temporary tables.
• Fix permission issue when binlog worker runs a native lambda function.
• Fixed an issue on Aurora read replicas when trying to query or rotate the slow log or general log.
• Fixed an issue that broke logical replication when the binlog_checksum parameter is set to different values on the master and the replica.
• Fixed an issue where the read replica might transiently see partial results of a recently committed transaction on the writer.
• Include transaction info of the rolled-back transaction in show engine innodb status when a deadlock is resolved.

Integration of MySQL community edition bug fixes

• Binlog events with ALTER TABLE ADD COLUMN ALGORITHM=QUICK will be rewritten as ALGORITHM=DEFAULT to be compatible with the community edition.
• Bug #22350047: IF CLIENT KILLED AFTER ROLLBACK TO SAVEPOINT PREVIOUS STMTS COMMITTED
• Bug #29915479: RUNNING COM_REGISTER_SLAVE WITHOUT COM_BINLOG_DUMP CAN RESULTS IN SERVER EXIT
• Bug #30441969: BUG #29723340: MYSQL SERVER CRASH AFTER SQL QUERY WITH DATA ?AST
• Bug #30628268: OUT OF MEMORY CRASH
• Bug #27081349: UNEXPECTED BEHAVIOUR WHEN DELETE WITH SPATIAL FUNCTION
• Bug #2730859: UNEXPECTED BEHAVIOUR WHILE HANDLING INVALID POLYGON"
• Bug #27081349: UNEXPECTED BEHAVIOUR WHEN DELETE WITH SPATIAL"
• Bug #26935001: ALTER TABLE AUTO_INCREMENT TRIES TO READ INDEX FROM DISCARDED TABLESPACE
• Bug #29770705: SERVER CRASHED WHILE EXECUTING SELECT WITH SPECIFIC WHERE CLAUSE
• Bug #27659490: SELECT USING DYNAMIC RANGE AND INDEX MERGE USE TOO MUCH MEMORY(OOM)
• Bug #24786290: REPLICA TION BREAKS AFTER Bug #74145 HAPPENS IN MASTER
• Bug #27703912: EXCESSIVE MEMORY USAGE WITH MANY PREPARE
• Bug #20527363: TRUNCATE TEMPORARY TABLE CRASH: IDICT_TF2_FLAG_IS_SET(TABLE, DICT_TF2_TEMPORARY)
• Bug#23103937 PS_TRUNCATE_ALL_TABLES() DOES NOT WORK IN SUPER_READ_ONLY MODE
• Bug #25053286: USE VIEW WITH CONDITION IN PROCEDURE CAUSES INCORRECT BEHAVIOR (fixed in 5.6.36)
• Bug #25586773: INCORRECT BEHAVIOR FOR CREATE TABLE SELECT IN A LOOP IN SP (fixed in 5.6.39)
• Bug #27407480: AUTOMATIC_SP_PRIVILEGES ReQUIRES NEED THE INSERT PRIVILEGES FOR MYSQL.USER TABLE
• Bug #26997096: relay_log_space value is not updated in a synchronized manner so that its value is sometimes much higher than the actual disk space used by relay logs.
• Bug#15831300 SLAVE_TYPE_CONVERSIONS=ALL_NON_LOSSY NOT WORKING AS EXPECTED
• SSL Bug backport Bug #17087862, Bug #20551271
• Bug #16894092: PERFORMANCE REGRESSION IN 5.6.6+ FOR INSERT INTO ... SELECT ... FROM (fixed in 5.6.15).
• Port a bug fix related to SLAVE_TYPE_CONVERSIONS.

Aurora MySQL database engine updates 2020-11-09 (version 1.22.3)

Version: 1.22.3
Aurora MySQL 1.22.3 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases for upgrade to 1.22.3 are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, and 1.22.*.

To create a cluster with an older version of Aurora MySQL, specify the engine version through the RDS Console, the AWS CLI, or the Amazon RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

Security fixes:

Fixes and other enhancements to fine-tune handling in a managed environment. Additional CVE fixes below:

- CVE-2020-14559
- CVE-2020-14539
- CVE-2020-2579
- CVE-2020-2812
- CVE-2020-2780
- CVE-2020-2763

Availability improvements:

- Fixed issues that might cause server restarts during recovery of a DDL statement that was not committed.
- Fixed race conditions in the lock manager that can cause a server restart.
- Fixed an issue that might cause the monitoring agent to restart the server during recovery of a large transaction

General improvements:

- Changed the behavior to map `MIXED binlog_format to ROW` instead of `STATEMENT` when executing `LOAD DATA FROM INFILE | S3`.
- Fixed an issue where a binlog replica connected to an Aurora MySQL binlog primary might show incomplete data when the primary executed `LOAD DATA FROM S3` and `binlog_format` is set to `STATEMENT`.

Integration of MySQL community edition bug fixes

- Bug #26654685: A corrupt index ID encountered during a foreign key check raised an assertion
- Bug #15831300: By default, when promoting integers from a smaller type on the master to a larger type on the slave (for example, from a SMALLINT column on the master to a BIGINT column on the slave), the promoted values are treated as though they are signed. Now in such cases it is possible to modify or override this behavior using one or both of `ALL_SIGNED`, `ALL UNSIGNED` in the set of values specified for the `slave_type_conversions` server system variable. For more information, see Row-based replication: attribute promotion and demotion, as well as the description of the variable.
- Bug #17449901: With `foreign_key_checks=0`, InnoDB permitted an index required by a foreign key constraint to be dropped, placing the table into an inconsistent and causing the foreign key check
that occurs at table load to fail. InnoDB now prevents dropping an index required by a foreign key constraint, even with foreign_key_checks=0. The foreign key constraint must be removed before dropping the foreign key index.

- **BUG #20768847:** An ALTER TABLE ... DROP INDEX operation on a table with foreign key dependencies raised an assertion.

## Aurora MySQL database engine updates 2020-03-05 (version 1.22.2)

**Version:** 1.22.2

Aurora MySQL 1.22.2 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.* and 2.07.*. You can restore the snapshot of an Aurora MySQL 1.* database into Aurora MySQL 1.22.2.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the RDS Console, the AWS CLI, or the Amazon RDS API.

**Note**

This version is currently not available in the following regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

### Improvements

**High priority fixes:**

- Fixed an issue of intermittent connection failures after certificate rotation.
- Fixed an issue that caused cloning to take longer on some database clusters with high write loads.
- Fixed an issue that broke logical replication when the `binlog_checksum` parameter is set to different values on the master and the replica.
- Fixed an issue where slow log and general log may not properly rotate on read replicas.
- Fixed an issue with ANSI Read Committed Isolation Level behavior.

## Aurora MySQL database engine updates 2019-12-23 (version 1.22.1)

**Version:** 1.22.1

Aurora MySQL 1.22.1 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, and 2.07.*. To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI or the RDS API. You have the option to upgrade existing Aurora MySQL 1.* database clusters to Aurora MySQL 1.22.1.
Note
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], Asia Pacific (Hong Kong) [ap-east-1], and Middle East (Bahrain) [me-south-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

Critical fixes:

- Fixed issues that prevented engine recovery involving table locks and temporary tables.
- Improved the stability of binary log when temporary tables are used.

High priority fixes:

- Fixed a slow memory leak in Aurora specific database tracing and logging sub-system that lowers the freeable memory.

Aurora MySQL database engine updates 2019-11-25 (version 1.22.0)

Version: 1.22.0

Aurora MySQL 1.22.0 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.*, and 2.07.*. To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI or the RDS API. You have the option to upgrade existing Aurora MySQL 1.* database clusters to Aurora MySQL 1.22.0.

Note
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], Asia Pacific (Hong Kong) [ap-east-1], Middle East (Bahrain) [me-south-1], and South America (São Paulo) [sa-east-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

New features:

- Aurora MySQL clusters now support the instance types r5.8xlarge, r5.16xlarge and r5.24xlarge.
• Binlog has new enhancements for improved commit time latency when very large transactions are involved.

• Aurora MySQL now has a mechanism to minimize the time window during which events of a large transaction are written to binlog on commit. This effectively prevents lengthy offline recovery incurred when database crashes occur during that time window. This feature also fixes the issue where a large transaction blocks small transactions on binlog commit. This feature is off by default and can be enabled by the service team if needed for your workload. When enabled, it will be triggered when a transaction size is > 500MB.

• Added support for the ANSI READ COMMITTED isolation level on the read replicas. This isolation level enables long-running queries on the read replica to execute without impacting the high throughput of writes on the writer node. For more information, see Aurora MySQL isolation levels.

• Global Databases now allow adding secondary read-only replica regions for database clusters deployed in these AWS Regions: regions: US East (N. Virginia) [us-east-1], US East (Ohio) [us-east-2], US West (N. California) [us-west-1], US West (Oregon) [us-west-2], Europe (Ireland) [eu-west-1], Europe (London) [eu-west-2], Europe (Paris) [eu-west-3], Asia Pacific (Tokyo) [ap-northeast-1], Asia Pacific (Seoul) [ap-northeast-2], Asia Pacific (Singapore) [ap-southeast-1], Asia Pacific (Sydney) [ap-southeast-2], Canada (Central) [ca-central-1], Europe (Frankfurt) [eu-central-1], and Asia Pacific (Mumbai) [ap-south-1].

• The hot row contention feature is now generally available and does not require the Aurora lab mode setting to be ON. This feature substantially improves throughput for workloads with many transactions contending for rows on the same page.

• This version has updated timezone files to support the latest Brazil timezone update for new clusters.

Critical fixes:
• CVE-2019-2922
• CVE-2019-2923
• CVE-2019-2924
• CVE-2019-2910

High priority fixes:
• CVE-2019-2805
• CVE-2019-2730
• CVE-2019-2740
• CVE-2018-3064
• CVE-2018-3058
• CVE-2017-3653
• CVE-2017-3464
• CVE-2017-3244
• CVE-2016-5612
• CVE-2016-5439
• CVE-2016-0606
• CVE-2015-4904
• CVE-2015-4879
• CVE-2015-4864
• CVE-2015-4830
• CVE-2015-4826
• CVE-2015-2620
• CVE-2015-0382
• CVE-2015-0381
• CVE-2014-6555
• CVE-2014-4258
• CVE-2014-4260
• CVE-2014-2444
• CVE-2014-2436
• CVE-2013-5881
• CVE-2014-0393
• CVE-2013-5908
• CVE-2013-5807
• CVE-2013-3806
• CVE-2013-3811
• CVE-2013-3804
• CVE-2013-3807
• CVE-2013-2378
• CVE-2013-2375
• CVE-2013-1523
• CVE-2013-2381
• CVE-2012-5615
• CVE-2014-6489

• Fixed an issue in the DDL recovery component that resulted in prolonged database downtime. Clusters that become unavailable after executing `TRUNCATE TABLE` query on a table with an `AUTO_INCREMENT` column should be updated.

• Fixed an issue in the DDL recovery component that resulted in prolonged database downtime. Clusters that become unavailable after executing `DROP TABLE` query on multiple tables in parallel should be updated.

**General stability fixes:**

• Fixed an issue that caused read replicas to restart during a long-running transaction. Customers who encounter replica restarts that coincide with an accelerated drop in freeable memory should consider upgrading to this version.

• Fixed an issue that incorrectly reported `ERROR 1836` when a nested query is executed against a temporary table on the read replica.

• Fixed a parallel query abort error on an Aurora reader instance while a heavy write workload is running on the Aurora writer instance.

• Fixed an issue that causes a database configured as a Binlog Master to restart while a heavy write workload is running.

• Fixed an issue of prolonged unavailability while restarting the engine. This addresses an issue in the buffer pool initialization. This issue occurs rarely but can potentially impact any supported release.

• Fixed an issue that generated inconsistent data in the `information_schema.replica_host_status` table.

• Fixed a race condition between the parallel query and the standard execution paths that caused the Reader nodes to restart intermittently.

• Improved stability of the database when the number of number of client connections exceeds the `max_connections` parameter value.

• Improved stability of the reader instances by blocking unsupported DDL and `LOAD FROM S3` queries.
Integration of MySQL community edition bug fixes

- Bug#16346241 - SERVER CRASH IN ITEM_PARAM::QUERY_VAL_STR
- Bug#17735850 - NAME_CONST() CRASH IN ITEM_NAME_CONST::ITEM_NAME_CONST()
- Bug #20989615 - INNODB AUTO_INCREMENT PRODUCES SAME VALUE TWICE
- Bug #20181776 - ACCESS CONTROL DOESN'T MATCH MOST SPECIFIC HOST WHEN IT CONTAINS WILDCARD
- Bug #27326796 - MYSQL CRASH WITH INNODB ASSERTION FAILURE IN FILE PARS0PARS.CC
- Bug #20590013 - IF YOU HAVE A FULLTEXT INDEX AND DROP IT YOU CAN NO LONGER PERFORM ONLINE DDL

Aurora MySQL database engine updates 2019-11-25 (version 1.21.0)

Version: 1.21.0

Aurora MySQL 1.21.0 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 2.01.*, 2.02.*, 2.03.* and 2.04.*. To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI or the RDS API. You have the option to upgrade existing Aurora MySQL 1.* database clusters to Aurora MySQL 1.21.0.

Note
This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], Asia Pacific (Hong Kong) [ap-east-1], Europe (Stockholm) [eu-north-1], and Middle East (Bahrain) [me-south-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

Critical fixes:
- CVE-2018-0734
- CVE-2019-2534
- CVE-2018-2612
- CVE-2017-3599
- CVE-2018-2562
- CVE-2017-3329
- CVE-2018-2696
- CVE-2015-4737

High priority fixes:
- Customers with database size close to 64 tebibytes (TiB) are strongly advised to upgrade to this version to avoid downtime due to stability bugs affecting volumes close to the Aurora storage limit.
General stability fixes:

- Fixed a parallel query abort error on Aurora reader instances while a heavy write workload is running on the Aurora writer instance.
- Fixed an issue on Aurora reader instances that reduced free memory during long-running transactions while there is a heavy transaction commit traffic on the writer instance.
- The value of the parameter `aurora_disable_hash_join` is now persisted after database restart or host replacement.
- Fixed an issue related to the Full Text Search cache that caused the Aurora instance to run out of memory. Customers using Full Text Search should upgrade.
- Improved stability of the database when the hash join feature is enabled and the instance is low on memory. Customers using hash join should upgrade.
- Fixed an issue in the query cache where the "Too many connections" error could cause a reboot.
- Fixed the free memory calculation on T2 instances to include swap memory space to prevent unnecessary reboots.

Integration of MySQL community edition bug fixes

- Bug #19929406: HANDLE_FATAL_SIGNAL (SIG=11) IN __MEMMOVE_SSSE3_BACK FROM STRING::COPY
- Bug #17059925: For UNION statements, the rows-examined value was calculated incorrectly. This was manifested as too-large values for the `ROWS_EXAMINED` column of Performance Schema statement tables (such as `events_statements_current`).
- Bug #11827369: Some queries with `SELECT ... FROM DUAL` nested subqueries raised an assertion.
- Bug #16311231: Incorrect results were returned if a query contained a subquery in an `IN` clause that contained an `XOR` operation in the `WHERE` clause.

Aurora MySQL database engine updates 2020-03-05 (version 1.20.1)

Version: 1.20.1

Aurora MySQL 1.20.1 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.* and 2.07.*. You can restore the snapshot of an Aurora MySQL 1.* database into Aurora MySQL 1.20.1.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the RDS Console, the AWS CLI, or the Amazon RDS API.

Note

This version is currently not available in the following regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

High priority fixes:

- Fixed an issue of intermittent connection failures after certificate rotation.
• Fixed an issue related to connection close concurrency that would result in a failover under heavy workload.

**General stability fixes:**

• Fixed a crash during execution of a complex query involving multi-table joins and aggregation that uses intermediate tables internally.

### Aurora MySQL database engine updates 2019-11-11 (version 1.20.0)

**Version:** 1.20.0

Aurora MySQL 1.20.0 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 2.01.*, 2.02.*, 2.03.* and 2.04.*. To create a cluster with an older version of Aurora MySQL, please specify the engine version through the AWS Management Console, the AWS CLI or the RDS API. You have the option to upgrade existing Aurora MySQL 1.* database clusters, up to 1.19.5, to Aurora MySQL 1.20.0.

**Note**

This version is currently not available in the following AWS Regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], Asia Pacific (Hong Kong) [ap-east-1], Europe (Stockholm) [eu-north-1], and Middle East (Bahrain) [me-south-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**

The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

### Improvements

**Critical fixes:**

• CVE-2018-0734
• CVE-2019-2534
• CVE-2018-2612
• CVE-2017-3599
• CVE-2018-2562
• CVE-2017-3329
• CVE-2018-2696
• CVE-2015-4737

**High priority fixes:**

• Customers with database size close to 64 tebibytes (TiB) are strongly advised to upgrade to this version to avoid downtime due to stability bugs affecting volumes close to the Aurora storage limit.

**General stability fixes:**
• Fixed a parallel query abort error on Aurora reader instances while a heavy write workload is running on the Aurora writer instance.
• Fixed an issue on Aurora reader instances that reduced free memory during long-running transactions while there is a heavy transaction commit traffic on the writer instance.
• The value of the parameter aurora_disable_hash_join is now persisted after database restart or host replacement.
• Fixed an issue related to the Full Text Search cache that caused the Aurora instance to run out of memory. Customers using Full Text Search should upgrade.
• Improved stability of the database when the hash join feature is enabled and the instance is low on memory. Customers using hash join should upgrade.
• Fixed an issue in the query cache where the "Too many connections" error could cause a reboot.
• Fixed the free memory calculation on T2 instances to include swap memory space to prevent unnecessary reboots.

Integration of MySQL community edition bug fixes
• Bug #19929406: HANDLE_FATAL_SIGNAL (SIG=11) IN __MEMMOVE_SSSE3_BACK FROM STRING::COPY
• Bug #17059925: For UNION statements, the rows-examined value was calculated incorrectly. This was manifested as too-large values for the ROWS EXAMINED column of Performance Schema statement tables (such as events_statements_current).
• Bug #11827369: Some queries with SELECT ... FROM DUAL nested subqueries raised an assertion.
• Bug #16311231: Incorrect results were returned if a query contained a subquery in an IN clause that contained an XOR operation in the WHERE clause.

Aurora MySQL database engine updates 2020-03-05 (version 1.19.6)

Version: 1.19.6

Aurora MySQL 1.19.6 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.* and 2.07.*. You can restore the snapshot of an Aurora MySQL 1.* database into Aurora MySQL 1.19.6.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the RDS Console, the AWS CLI, or the Amazon RDS API.

**Note**
This version is currently not available in the following regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Improvements**

**High priority fixes:**
• Fixed an issue of intermittent connection failures after certificate rotation.
Aurora MySQL database engine updates 2019-09-19 (version 1.19.5)

Version: 1.19.5

Aurora MySQL 1.19.5 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

You have the option to upgrade existing database clusters to Aurora MySQL 1.19.5. You can restore snapshots of Aurora MySQL 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.1, and 1.19.2 into Aurora MySQL 1.19.5.

To use an older version of Aurora MySQL, you can create new database clusters by specifying the engine version through the AWS Management Console, the AWS CLI, or the RDS API.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the following AWS Regions: Europe (London) [eu-west-2], AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1], China (Ningxia) [cn-northwest-1], and Asia Pacific (Hong Kong) [ap-east-1]. There will be a separate announcement once it is made available.

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

- Fixed an issue on Aurora reader instances that reduced free memory during long-running transactions while there is a heavy transaction commit traffic on the writer instance.
- Fixed a parallel query abort error on Aurora reader instances while a heavy write workload is running on the Aurora writer instance.
- The value of the parameter aurora_disable_hash_join is now persisted after database restart or host replacement.
- Fixed an issue related to the Full Text Search cache that caused the Aurora instance to run out of memory.
- Improved stability of the database when the volume size is close to the 64 tebibyte (TiB) volume limit by reserving 160 GB of space for the recovery workflow to complete without a failover.
- Improved stability of the database when the hash join feature is enabled and the instance is low on memory.
- Fixed the free memory calculation to include swap memory space on T2 instances that caused them to reboot prematurely.
- Fixed an issue in the query cache where the "Too many connections" error could cause a reboot.

Integration of MySQL community edition bug fixes

- CVE-2018-2696
- CVE-2015-4737
- Bug #19929406: HANDLE_FATAL_SIGNAL (SIG=11) IN __MEMMOVE_SSSE3_BACK FROM STRING::COPY
- Bug #17059925: For UNION statements, the rows-examined value was calculated incorrectly. This was manifested as too-large values for the ROWS_EXAMINED column of Performance Schema statement tables (such as events_statements_current).
- Bug #11827369: Some queries with SELECT ... FROM DUAL nested subqueries raised an assertion.
• Bug #16311231: Incorrect results were returned if a query contained a subquery in an IN clause that contained an XOR operation in the WHERE clause.

Aurora MySQL database engine updates 2019-06-05 (version 1.19.2)

Version: 1.19.2

Aurora MySQL 1.19.2 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, can be created with 1.17.8, 1.19.0, 1.19.1, or 1.19.2. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.19.2. To use an older version, you can create new database clusters in Aurora MySQL 1.14.4, Aurora MySQL 1.15.1, Aurora MySQL 1.16, Aurora MySQL 1.17.8, or Aurora MySQL 1.18. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1], Europe (Stockholm) [eu-north-1], China (Ningxia) [cn-northwest-1], and Asia Pacific (Hong Kong) [ap-east-1] AWS Regions. There will be a separate announcement once it is made available.

Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

• Fixed an issue that could cause failures when loading data into Aurora from Amazon S3.
• Fixed an issue that could cause failures when uploading data from Aurora to Amazon S3.
• Fixed an issue that created zombie sessions left in a killed state.
• Fixed an issue that caused aborted connections when handling an error in network protocol management.
• Fixed an issue that could cause a crash when dealing with partitioned tables.
• Fixed an issue related to binlog replication of trigger creation.

Aurora MySQL database engine updates 2019-05-09 (version 1.19.1)

Version: 1.19.1

Aurora MySQL 1.19.1 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, can be created with 1.17.8, 1.19.0, or 1.19.1. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.19.1. To use an older version, you can create new database clusters in Aurora MySQL 1.14.4, Aurora MySQL 1.15.1, Aurora MySQL 1.16, Aurora MySQL 1.17.8, or Aurora MySQL 1.18. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.
Note
The procedure to upgrade your DB cluster has changed. For more information, see Upgrading and patching Amazon Aurora MySQL DB clusters (p. 877).

Improvements

- Fixed a bug in binlog replication that can cause an issue on Aurora instances configured as binlog worker.
- Fixed an error in handling certain kinds of `ALTER TABLE` commands.
- Fixed an issue with aborted connections because of an error in network protocol management.

Aurora MySQL database engine updates 2019-02-07 (version 1.19.0)

Version: 1.19.0

Aurora MySQL 1.19.0 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, can be created with 1.17.8 or 1.19.0. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.19.0. To use an older version, you can create new database clusters in Aurora MySQL 1.14.4, Aurora MySQL 1.15.1, Aurora MySQL 1.16, Aurora MySQL 1.17.8, or Aurora MySQL 1.18.0. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

Features

- **Aurora Version Selector** - Starting with Aurora MySQL 1.19.0, you can choose from among multiple versions of MySQL 5.6 compatible Aurora on the Amazon RDS console. For more information, see Checking or specifying Aurora MySQL engine versions through AWS (p. 874).

Improvements

- Fixed a stability issue related to the `CHECK TABLE` query on an Aurora Replica.
- Introduced a new global user variable `aurora_disable_hash_join` to disable Hash Join.
- Fixed a stability issue when generating the output row during multiple table hash join.
- Fixed an issue that returned a wrong result because of a plan change during Hash Join applicability check.
- Zero Downtime Patching is supported with long running transactions. This enhancement will come into effect when upgrading from version 1.19 to a higher one.
- Zero Downtime Patching is now supported when binlog is enabled. This enhancement will come into effect when upgrading from version 1.19 to a higher one.
- Fixed an issue that caused a spike in CPU utilization on the Aurora Replica unrelated to the workload.
- Fixed a race condition in the lock manager that resulted in a database restart.
• Fixed a race condition in the lock manager component to improve stability of Aurora instances.
• Improved stability of the deadlock detector inside the lock manager component.
• INSERT operation on a table is prohibited if InnoDB detects that the index is corrupted.
• Fixed a stability issue in Fast DDL.
• Improved Aurora stability by reducing the memory consumption in scan batching for single-row subquery.
• Fixed a stability issue that occurred after a foreign key was dropped while the system variable foreign_key_checks is set to 0.
• Fixed an issue in the Out Of Memory Avoidance feature that erroneously overrode changes to the table_definition_cache value made by the user.
• Fixed stability issues in the Out Of Memory Avoidance feature.
• Fixed an issue that set query_time and lock_time in slow_query_log to garbage values.
• Fixed a parallel query stability issue triggered by improper handling of string collation internally.
• Fixed a parallel query stability issue triggered by a secondary index search.
• Fixed a parallel query stability issue triggered by a multi-table update.

Integration of MySQL community edition bug fixes
• BUG #32917: DETECT ORPHAN TEMP-POOL FILES, AND HANDLE GRACEFULLY
• BUG #63144 CREATE TABLE IF NOT EXISTS METADATA LOCK IS TOO RESTRICTIVE

Aurora MySQL database engine updates 2018-09-20

Version: 1.18.0

Aurora MySQL 1.18.0 is generally available. All new Aurora MySQL parallel query clusters with MySQL 5.6 compatibility, including those restored from snapshots, will be created in Aurora MySQL 1.18.0. You have the option, but are not required, to upgrade existing parallel query clusters to Aurora MySQL 1.18.0. You can create new DB clusters in Aurora MySQL 1.14.4, Aurora MySQL 1.15.1, Aurora MySQL 1.16, or Aurora MySQL 1.17.6. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.18.0 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

Important
Aurora MySQL 1.18.0 only applies to Aurora parallel query clusters. If you upgrade a provisioned 5.6.10a cluster, the resulting version is 1.17.8. If you upgrade a parallel query 5.6.10a cluster, the resulting version is 1.18.0.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Features

• Parallel Query is available with this release, for new clusters and restored snapshots. Aurora MySQL parallel query is an optimization that parallelizes some of the I/O and computation involved in processing data-intensive queries. The work that is parallelized includes retrieving rows from storage, extracting column values, and determining which rows match the conditions in the WHERE clause and join clauses. This data-intensive work is delegated (in database optimization terms, pushed down) to multiple nodes in the Aurora distributed storage layer. Without parallel query, each query brings all the scanned data to a single node within the Aurora MySQL cluster (the head node) and performs all the query processing there.
• When the parallel query feature is enabled, the Aurora MySQL engine automatically determines when queries can benefit, without requiring SQL changes such as hints or table attributes.

For more information, see Working with parallel query for Amazon Aurora MySQL (p. 697).

• **OOM Avoidance:** This feature monitors the system memory and tracks memory consumed by various components of the database. Once the system runs low on memory, it performs a list of actions to release memory from various tracked components in an attempt to save the database from running into Out of Memory (OOM) and thereby avoiding a database restart. This best-effort feature is enabled by default for t2 instances and can be enabled on other instance classes via a new instance parameter named `aurora_oom_response`. The instance parameter takes a string of comma separated actions that an instance should take when its memory is low. Valid actions include "print", "tune", "decline", "kill_query" or any combination of these. Any empty string means there should be no actions taken and effectively renders the feature to be disabled. Note that the default actions for the feature is "print, tune". Usage examples:
  - "print" – Only prints the queries taking high amount of memory.
  - "tune" – Tunes the internal table caches to release some memory back to the system.
  - "decline" – Declines new queries once the instance is low on memory.
  - "kill_query" – Kills the queries in descending order of memory consumption until the instance memory surfaces above the low threshold. Data definition language (DDL) statements are not killed.
  - "print, tune" – Performs actions described for both "print" and "tune".
  - "tune, decline, kill_query" – Performs the actions described for "tune", "decline", and "kill_query".

For information about handling out-of-memory conditions and other troubleshooting advice, see Amazon Aurora MySQL out of memory issues (p. 1309).

### Aurora MySQL database engine updates 2020-03-05

**Version:** 1.17.9

Aurora MySQL 1.17.9 is generally available. Aurora MySQL 1.* versions are compatible with MySQL 5.6 and Aurora MySQL 2.* versions are compatible with MySQL 5.7.

Currently supported Aurora MySQL releases are 1.14.*, 1.15.*, 1.16.*, 1.17.*, 1.18.*, 1.19.*, 1.20.*, 1.21.*, 1.22.*, 2.01.*, 2.02.*, 2.03.*, 2.04.*, 2.05.*, 2.06.* and 2.07.*. You can restore the snapshot of an Aurora MySQL 1.* database into Aurora MySQL 1.17.9.

To create a cluster with an older version of Aurora MySQL, please specify the engine version through the RDS Console, the AWS CLI, or the Amazon RDS API.

**Note**

This version is currently not available in the following regions: AWS GovCloud (US-East) [us-gov-east-1], AWS GovCloud (US-West) [us-gov-west-1]. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Improvements**

**High priority fixes:**

• Fixed an issue of intermittent connection failures after certificate rotation.
Aurora MySQL 1.17.8 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, will be created in Aurora MySQL 1.17.8. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.17.8. To use an older version, you can create new database clusters in Aurora MySQL 1.14.4, 1.15.1, 1.16, or 1.17.7. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.17.8 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

**Note**
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through **AWS Premium Support**. For more information, see **Maintaining an Amazon Aurora DB cluster** (p. 388).

**Improvements**
- Fixed a performance issue that increased the CPU utilization on an Aurora Replica after a restart.
- Fixed a stability issue for **SELECT** queries that used hash join.

**Integration of MySQL community edition bug fixes**
- BUG #13418638: CREATE TABLE IF NOT EXISTS METADATA LOCK IS TOO RESTRICTIVE

**Aurora MySQL database engine updates 2018-10-08**

**Version:** 1.17.7

Aurora MySQL 1.17.7 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, will be created in Aurora MySQL 1.17.7. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.17.7. To use an older version, you can create new database clusters in Aurora MySQL 1.14.4, 1.15.1, 1.16, or 1.17.7. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.17.7 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

**Note**
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through **AWS Premium Support**. For more information, see **Maintaining an Amazon Aurora DB cluster** (p. 388).

**Improvements**
- The InnoDB status variable **innodb_buffer_pool_size** has been made publicly visible for the customers to modify.
- Fixed a stability issue on the Aurora cluster that occurred during failovers.
- Improved cluster availability by fixing a DDL recovery issue that occurred after an unsuccessful **TRUNCATE** operation.
- Fixed a stability issue related to the **mysql.innodb_table_stats** table update, triggered by DDL operations.
• Fixed Aurora Replica stability issues triggered during query cache invalidation after a DDL operation.
• Fixed a stability issue triggered by invalid memory access during periodic dictionary cache eviction in the background.

Integration of MySQL community edition bug fixes

• Bug #16208542: Drop index on a foreign key column leads to missing table.
• Bug #76349: memory leak in add_derived_key().
• Bug #16862316: For partitioned tables, queries could return different results depending on whether Index Merge was used.
• Bug #17588348: Queries using the index_merge optimization (see Index merge optimization) could return invalid results when run against tables that were partitioned by HASH.

Aurora MySQL database engine updates 2018-09-06

Version: 1.17.6

Aurora MySQL 1.17.6 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, will be created in Aurora MySQL 1.17.6. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.17.6. To use an older version, you can create new database clusters in Aurora MySQL 1.14.4, 1.15.1, 1.16, or 1.17.5. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.17.6 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

• Fixed a stability issue on the Aurora Reader for SELECT queries while the Aurora Writer is performing DDL operations on the same table.
• Fixed a stability issue caused by the creation and deletion of DDL logs for temporary tables that use Heap/Memory engine.
• Fixed a stability issue on the binlog worker when DDL statements are being replicated while the connection to the Binlog Master is unstable.
• Fixed a stability issue encountered while writing to the slow query log.
• Fixed an issue with the replica status table that exposed incorrect Aurora Reader lag information.

Integration of MySQL community edition bug fixes

• For an ALTER TABLE statement that renamed or changed the default value of a BINARY column, the alteration was done using a table copy and not in place. (Bug #67141, Bug #14735373, Bug #69580, Bug #17024290)
• An outer join between a regular table and a derived table that is implicitly groups could cause a server exit. (Bug #16177639)
Aurora MySQL database engine updates 2018-08-14

Version: 1.17.5

Aurora MySQL 1.17.5 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, will be created in Aurora MySQL 1.17.5. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.17.5. To use an older version, you can create new database clusters in Aurora MySQL 1.14.4, 1.15.1, 1.16, or 1.17.4. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.17.5 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

- Fixed an issue where an Aurora Writer might experience a restart after an Aurora cluster is patched using the Zero-Downtime Patching feature.

Aurora MySQL database engine updates 2018-08-07

Version: 1.17.4

Aurora MySQL 1.17.4 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, will be created in Aurora MySQL 1.17.4. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.17.4. To use an older version, you can create new database clusters in Aurora MySQL 1.14.4, 1.15.1, 1.16, or 1.17.3. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.17.4 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

Note
This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

- Replication improvements:
  - Reduced network traffic by not transmitting binlog records to cluster replicas. This improvement is enabled by default.
  - Reduced network traffic by compressing replication messages. This improvement is enabled by default for 8xlarge and 16xlarge instance classes. Such large instances can sustain a heavy volume of write traffic that results in substantial network traffic for replication messages.
  - Fixes to the replica query cache.
  - Fixed an issue where ORDER BY LOWER(col_name) could produce incorrect ordering while using the utf8_bin collation.
- Fixed an issue where DDL statements (especially `TRUNCATE TABLE`) could cause problems on Aurora replicas, including instability or missing tables.
- Fixed an issue where sockets are left in a half-open state when storage nodes are restarted.
- The following new DB cluster parameters are available:
  - `aurora_enable_zdr` – Allow connections opened on an Aurora Replica to stay active on replica restart.
  - `aurora_enable_replica_log_compression` – Enable compression of replication payloads to improve network bandwidth utilization between the master and Aurora Replicas.
  - `aurora_enable_repl_bin_log_filtering` – Enable filtering of replication records that are unusable by Aurora Replicas on the master.

**Aurora MySQL database engine updates 2018-06-05**

**Version:** 1.17.3

Aurora MySQL 1.17.3 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, will be created in Aurora MySQL 1.17.3. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.17.3. You can create new database clusters in Aurora MySQL 1.14.4, Aurora MySQL 1.15.1, or Aurora MySQL 1.16. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.17.3 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

**Note**

This version is currently not available in the AWS GovCloud (US-West) [us-gov-west-1] and China (Beijing) [cn-north-1] regions. There will be a separate announcement once it is made available.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Improvements**

- Fixed an issue where an Aurora Replica can restart when using optimistic cursor restores while reading records.
- Fixed an issue where an Aurora Writer restarts when trying to kill a MySQL session (kill "<session id>") with performance schema enabled.
- Fixed an issue where an Aurora Writer restarts when computing a threshold for garbage collection.
- Fixed an issue where an Aurora Writer can occasionally restart when tracking Aurora Replica progress in log application.
- Fixed an issue with the Query Cache when auto-commit is off and that could potentially cause stale reads.

**Aurora MySQL database engine updates 2018-04-27**

**Version:** 1.17.2

Aurora MySQL 1.17.2 is generally available. All new Aurora MySQL database clusters with MySQL 5.6 compatibility, including those restored from snapshots, will be created in Aurora MySQL 1.17.2. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.17.2. You can create new database clusters in Aurora MySQL 1.14.4, Aurora MySQL 1.15.1, or Aurora MySQL 1.16. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.
With version 1.17.2 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Improvements**

- Fixed an issue which was causing restarts during certain DDL partition operations.
- Fixed an issue which was causing support for invocation of AWS Lambda functions via native Aurora MySQL functions to be disabled.
- Fixed an issue with cache invalidation which was causing restarts on Aurora Replicas.
- Fixed an issue in lock manager which was causing restarts.

**Aurora MySQL database engine updates 2018-03-23**

**Version:** 1.17.1

Aurora MySQL 1.17.1 is generally available. All new database clusters, including those restored from snapshots, will be created in Aurora MySQL 1.17.1. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.17.1. You can create new DB clusters in Aurora MySQL 1.15.1, Aurora MySQL 1.16, or Aurora MySQL 1.17. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.17.1 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time. This release fixes some known engine issues as well as regressions.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

**Note**

There is an issue in the latest version of the Aurora MySQL engine. After upgrading to 1.17.1, the engine version is reported incorrectly as 1.17. If you upgraded to 1.17.1, you can confirm the upgrade by checking the Maintenance column for the DB cluster in the AWS Management Console. If it displays none, then the engine is upgraded to 1.17.1.

**Improvements**

- Fixed an issue in binary log recovery that resulted in longer recovery times for situations with large binary log index files which can happen if binary logs rotate very often.
- Fixed an issue in the query optimizer that generated an inefficient query plan for partitioned tables.
- Fixed an issue in the query optimizer due to which a range query resulted in a restart of the database engine.

**Aurora MySQL database engine updates 2018-03-13**

**Version:** 1.17

Aurora MySQL 1.17 is generally available. Aurora MySQL 1.x versions are only compatible with MySQL 5.6, and not MySQL 5.7. All new 5.6-compatible database clusters, including those restored from snapshots, will be created in Aurora 1.17. You have the option, but are not required, to upgrade existing database clusters to Aurora 1.17. You can create new DB clusters in Aurora 1.14.1, Aurora 1.15.1, or Aurora 1.16. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.
With version 1.17 of Aurora, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time. We support zero-downtime patching, which works on a best-effort basis to preserve client connections through the patching process. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support.

**Zero-downtime patching**

The zero-downtime patching (ZDP) feature attempts, on a best-effort basis, to preserve client connections through an engine patch. For more information about ZDP, see Using zero-downtime patching (p. 880).

**New features**

- Aurora MySQL now supports lock compression, which optimizes the lock manager's memory usage. Starting in version 1.17, you can use this feature without enabling lab mode.

**Improvements**

- Fixed an issue predominantly seen on instances with fewer cores where a single core might have 100% CPU utilization even when the database is idle.
- Improved the performance of fetching binary logs from Aurora clusters.
- Fixed an issue where Aurora Replicas attempt to write table statistics to persistent storage, and crash.
- Fixed an issue where query cache did not work as expected on Aurora Replicas.
- Fixed a race condition in lock manager that resulted in an engine restart.
- Fixed an issue where locks taken by read-only, auto-commit transactions resulted in an engine restart.
- Fixed an issue where some queries are not written to the audit logs.
- Fixed an issue with recovery of certain partition maintenance operations on failover.

**Integration of MySQL bug fixes**

- LAST_INSERT_ID is replicated incorrectly if replication filters are used (Bug #69861)
- Query returns different results depending on whether INDEX_MERGE setting (Bug #16862316)
- Query proc re-execute of stored routine, inefficient query plan (Bug #16346367)
- INNODB FTS : Assert in FTS_CACHE_APPEND_DELETED_DOC_IDS (BUG #18079671)
- Assert RBTEMPTY(INDEX_CACHE->WORDS) in ALTER TABLE CHANGE COLUMN (BUG #17536995)
- INNODB fulltext search doesn't find records when savepoints are involved (BUG #70333, BUG #17458835)

**Aurora MySQL database engine updates 2017-12-11**

**Version:** 1.16

Aurora MySQL 1.16 is generally available. All new database clusters, including those restored from snapshots, will be created in Aurora 1.16. You have the option, but are not required, to upgrade existing database clusters to Aurora 1.16. You can create new DB clusters in Aurora 1.14.1 or Aurora 1.15.1. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.16 of Aurora, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time. We are enabling zero-downtime patching, which works on a best-
effort basis to preserve client connections through the patching process. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support at http://aws.amazon.com/support.

Zero-downtime patching

The zero-downtime patching (ZDP) feature attempts, on a best-effort basis, to preserve client connections through an engine patch. For more information about ZDP, see Using zero-downtime patching (p. 880).

New features

- Aurora MySQL now supports synchronous AWS Lambda invocations via the native function `lambda_sync()`. Also available is native function `lambda_async()`, which can be used as an alternative to the existing stored procedure for asynchronous Lambda invocation. For more information, see Invoking a Lambda function from an Amazon Aurora MySQL DB cluster (p. 818).
- Aurora MySQL now supports hash joins to speed up equijoin queries. Aurora's cost-based optimizer can automatically decide when to use hash joins; you can also force their use in a query plan. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Aurora MySQL now supports scan batching to speed up in-memory scan-oriented queries significantly. The feature boosts the performance of table full scans, index full scans, and index range scans by batch processing.

Improvements

- Fixed an issue where read replicas crashed when running queries on tables that have just been dropped on the master.
- Fixed an issue where restarting the writer on a database cluster with a very large number of FULLTEXT indexes results in longer than expected recovery.
- Fixed an issue where flushing binary logs causes LOST_EVENTS incidents in binlog events.
- Fixed stability issues with the scheduler when performance schema is enabled.
- Fixed an issue where a subquery that uses temporary tables could return partial results.

Integration of MySQL bug fixes

None

Aurora MySQL database engine updates 2017-11-20

Version: 1.15.1

Aurora MySQL 1.15.1 is generally available. All new database clusters, including those restored from snapshots, will be created in Aurora 1.15.1. You have the option, but are not required, to upgrade existing DB clusters to Aurora 1.15.1. You can create new DB clusters in Aurora 1.14.1. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.15.1 of Aurora, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time. We are enabling zero-downtime patching, which works on a best-effort basis to preserve client connections through the patching process. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support at http://aws.amazon.com/support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).
Zero-downtime patching

The zero-downtime patching (ZDP) feature attempts, on a best-effort basis, to preserve client connections through an engine patch. For more information about ZDP, see Using zero-downtime patching (p. 880).

Improvements

- Fixed an issue in the adaptive segment selector for a read request that would cause it to choose the same segment twice causing a spike in read latency under certain conditions.
- Fixed an issue that stems from an optimization in Aurora MySQL for the thread scheduler. This problem manifests itself into what are spurious errors while writing to the slow log, while the associated queries themselves perform fine.
- Fixed an issue with stability of read replicas on large (> 5 TB) volumes.
- Fixed an issue where worker thread count increases continuously due to a bogus outstanding connection count.
- Fixed an issue with table locks that caused long semaphore waits during insert workloads.
- Reverted the following MySQL bug fixes included in Aurora MySQL 1.15:
  - MySQL instance stalling "doing SYNC index" (Bug #73816)
  - Assert RBT_EMPTY(INDEX_CACHE->WORDS) in ALTER TABLE CHANGE COLUMN (Bug #17536995)
  - InnoDB Fulltext search doesn't find records when savepoints are involved (Bug #70333)

Integration of MySQL bug fixes

None

Aurora MySQL database engine updates 2017-10-24

Version: 1.15

Aurora MySQL 1.15 is generally available. All new database clusters, including those restored from snapshots, will be created in Aurora 1.15. You have the option, but are not required, to upgrade existing DB clusters to Aurora 1.15. You can create new DB clusters in Aurora 1.14.1. You can do so using the AWS CLI or the Amazon RDS API and specifying the engine version.

With version 1.15 of Aurora, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time. Updates require a database restart, so you will experience 20 to 30 seconds of downtime, after which you can resume using your DB cluster or clusters. If your DB clusters are currently running Aurora 1.14 or Aurora 1.14.1, the zero-downtime patching feature in Aurora MySQL might allow client connections to your Aurora MySQL primary instance to persist through the upgrade, depending on your workload.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support at http://aws.amazon.com/support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Zero-downtime patching

The zero-downtime patching (ZDP) feature attempts, on a best-effort basis, to preserve client connections through an engine patch. For more information about ZDP, see Using zero-downtime patching (p. 880).

New features

- Asynchronous Key Prefetch – Asynchronous key prefetch (AKP) is a feature targeted to improve the performance of non-cached index joins, by prefetching keys in memory ahead of when they
are needed. The primary use case targeted by AKP is an index join between a small outer and large
inner table, where the index is highly selective on the larger table. Also, when the Multi-Range Read
(MRR) interface is enabled, AKP will be leveraged for a secondary to primary index lookup. Smaller
instances which have memory constraints might in some cases be able to leverage AKP, given the
right key cardinality. For more information, see Working with asynchronous key prefetch in Amazon
Aurora (p. 842).

- **Fast DDL** – We have extended the feature that was released in Aurora 1.13 (p. 961) to operations
  that include default values. With this extension, Fast DDL is applicable for operations that add
  a nullable column at the end of a table, with or without default values. The feature remains
  under Aurora lab mode. For more information, see Altering tables in Amazon Aurora using fast
  DDL (p. 693).

**Improvements**

- Fixed a calculation error during optimization of WITHIN/CONTAINS spatial queries which previously
  resulted in an empty result set.
- Fixed `SHOW VARIABLE` command to show the updated `innodb_buffer_pool_size` parameter value
  whenever it is changed in the parameter group.
- Improved stability of primary instance during bulk insert into a table altered using Fast DDL when
  adaptive hash indexing is disabled and the record to be inserted is the first record of a page.
- Improved stability of Aurora when the user attempts to set `server_audit_events` DB cluster parameter
  value to `default`.
- Fixed an issue in which a database character set change for an ALTER TABLE statement that ran on the
  Aurora primary instance was not being replicated on the Aurora Replicas until they were restarted.
- Improved stability by fixing a race condition on the primary instance which previously allowed it to
  register an Aurora Replica even if the primary instance had closed its own volume.
- Improved performance of the primary instance during index creation on a large table by changing the
  locking protocol to enable concurrent data manipulation language (DML) statements during index
  build.
- Fixed InnoDB metadata inconsistency during ALTER TABLE RENAME query which improved stability.
  Example: When columns of table t1(c1, c2) are renamed cyclically to t1(c2, c3) within the same ALTER
  statement.
- Improved stability of Aurora Replicas for the scenario where an Aurora Replica has no active workload
  and the primary instance is unresponsive.
- Improved availability of Aurora Replicas for a scenario in which the Aurora Replica holds an explicit
  lock on a table and blocks the replication thread from applying any DDL changes received from the
  primary instance.
- Improved stability of the primary instance when a foreign key and a column are being added to a table
  from two separate sessions at the same time and Fast DDL has been enabled.
- Improved stability of the purge thread on the primary instance during a heavy write workload by
  blocking truncate of undo records until they have been purged.
- Improved stability by fixing the lock release order during commit process of transactions which drop
  tables.
- Fixed a defect for Aurora Replicas in which the DB instance could not complete startup and
  complained that port 3306 was already in use.
- Fixed a race condition in which a SELECT query run on certain information_schema tables (innodb_trx,
innodb_lock, innodb_lock_waits) increased cluster instability.

**Integration of MySQL bug fixes**

- CREATE USER accepts plugin and password hash, but ignores the password hash (Bug #78033)
• The partitioning engine adds fields to the read bit set to be able to return entries sorted from a partitioned index. This leads to the join buffer will try to read unneeded fields. Fixed by not adding all partitioning fields to the read_set, but instead only sort on the already set prefix fields in the read_set. Added a DBUG_ASSERT that if doing key_cmp, at least the first field must be read (Bug #16367691).

• MySQL instance stalling "doing SYNC index" (Bug #73816)

• Assert RBT_EMPTY(INDEX_CACHE->WORDS) in ALTER TABLE CHANGE COLUMN (Bug #17536995)

• InnoDB Fulltext search doesn't find records when savepoints are involved (Bug #70333)

Aurora MySQL database engine updates: 2018-03-13

Version: 1.14.4

Aurora MySQL 1.14.4 is generally available. You can create new DB clusters in Aurora 1.14.4, using the AWS CLI or the Amazon RDS API and specifying the engine version. You have the option, but are not required, to upgrade existing 1.14.x DB clusters to Aurora 1.14.4.

With version 1.14.4 of Aurora, we are using a cluster-patching model where all nodes in an Aurora DB cluster are patched at the same time. We support zero-downtime patching, which works on a best-effort basis to preserve client connections through the patching process. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support at http://aws.amazon.com/support. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Zero-downtime patching

The zero-downtime patching (ZDP) feature attempts, on a best-effort basis, to preserve client connections through an engine patch. For more information about ZDP, see Using zero-downtime patching (p. 880).

New features

• Aurora MySQL now supports db.r4 instance classes.

Improvements

• Fixed an issue where LOST_EVENTS were generated when writing large binlog events.

Integration of MySQL bug fixes

• Ignorable events don't work and are not tested (Bug #74683)

• NEW->OLD ASSERT FAILURE 'GTID_MODE > 0' (Bug #20436436)

Aurora MySQL database engine updates: 2017-09-22

Version: 1.14.1

Aurora MySQL 1.14.1 is generally available. All new database clusters, including those restored from snapshots, will be created in Aurora MySQL 1.14.1. Aurora MySQL 1.14.1 is also a mandatory upgrade for existing Aurora MySQL DB clusters. For more information, see Announcement: Extension to mandatory upgrade schedule for Amazon Aurora on the AWS Developer Forums website.
With version 1.14.1 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora MySQL DB cluster are patched at the same time. Updates require a database restart, so you will experience 20 to 30 seconds of downtime, after which you can resume using your DB cluster or clusters.

If your DB clusters are currently running version 1.13 or greater, the zero-downtime patching feature in Aurora MySQL might allow client connections to your Aurora MySQL primary instance to persist through the upgrade, depending on your workload.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support at http://aws.amazon.com/support.

**Improvements**

- Fixed race conditions associated with inserts and purge to improve the stability of the Fast DDL feature, which remains in Aurora MySQL lab mode.

**Aurora MySQL database engine updates: 2017-08-07**

**Version:** 1.14

Aurora MySQL 1.14 is generally available. All new database clusters, including those restored from snapshots, will be created in Aurora MySQL 1.14. Aurora MySQL 1.14 is also a mandatory upgrade for existing Aurora MySQL DB clusters. We will send a separate announcement with the timeline for deprecating earlier versions of Aurora MySQL.

With version 1.14 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time. Updates require a database restart, so you will experience 20 to 30 seconds of downtime, after which you can resume using your DB cluster or clusters. If your DB clusters are currently running version 1.13, Aurora's zero-downtime patching feature may allow client connections to your Aurora primary instance to persist through the upgrade, depending on your workload.

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support at http://aws.amazon.com/support.

**Zero-downtime patching**

The zero-downtime patching (ZDP) feature attempts, on a best-effort basis, to preserve client connections through an engine patch. For more information about ZDP, see Using zero-downtime patching (p. 880).

**Improvements**

- Fixed an incorrect "record not found" error when a record is found in the secondary index but not in the primary index.
- Fixed a stability issue that can occur due to a defensive assertion (added in 1.12) that was too strong in the case when an individual write spans over 32 pages. Such a situation can occur, for instance, with large BLOB values.
- Fixed a stability issue because of inconsistencies between the tablespace cache and the dictionary cache.
- Fixed an issue in which an Aurora Replica becomes unresponsive after it has exceeded the maximum number of attempts to connect to the primary instance. An Aurora Replica now restarts if the period of inactivity is more than the heartbeat time period used for health check by the primary instance.
- Fixed a livelock that can occur under very high concurrency when one connection tries to acquire an exclusive meta data lock (MDL) while issuing a command, such as \texttt{ALTER TABLE}.
- Fixed a stability issue in an Aurora Read Replica in the presence of logical/parallel read ahead.
- Improved \texttt{LOAD FROM S3} in two ways:
1. Better handling of Amazon S3 timeout errors by using the SDK retry in addition to the existing retry.
2. Performance optimization when loading very big files or large numbers of files by caching and reusing client state.

   • Fixed the following stability issues with Fast DDL for `ALTER TABLE` operations:
     1. When the `ALTER TABLE` statement has multiple `ADD COLUMN` commands and the column names are not in ascending order.
     2. When the name string of the column to be updated and its corresponding name string, fetched from the internal system table, differs by a null terminating character (/0).
     3. Under certain B-tree split operations.
     4. When the table has a variable length primary key.

   • Fixed a stability issue with Aurora Replicas when it takes too long to make its Full Text Search (FTS) index cache consistent with that of the primary instance. This can happen if a large portion of the newly created FTS index entries on the primary instance have not yet been flushed to disk.
   • Fixed a stability issue that can happen during index creation.
   • New infrastructure that tracks memory consumption per connection and associated telemetry that will be used for building out Out-Of-Memory (OOM) avoidance strategies.
   • Fixed an issue where `ANALYZE TABLE` was incorrectly allowed on Aurora Replicas. This has now been blocked.
   • Fixed a stability issue caused by a rare deadlock as a result of a race condition between logical read-ahead and purge.

Integration of MySQL bug fixes

• A full-text search combined with derived tables (subqueries in the `FROM` clause) caused a server exit. Now, if a full-text operation depends on a derived table, the server produces an error indicating that a full-text search cannot be done on a materialized table. (Bug #68751, Bug #16539903)

Aurora MySQL database engine updates: 2017-05-15

Version: 1.13

Note
We enabled a new feature - `SELECT INTO OUTFILE S3` - in Aurora MySQL version 1.13 after the initial release, and have updated the release notes to reflect that change.

Aurora MySQL 1.13 is generally available. All new database clusters, including those restored from snapshots, will be created in Aurora MySQL 1.13. You have the option, but are not required, to upgrade existing database clusters to Aurora MySQL 1.13. With version 1.13 of Aurora, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time. We are enabling zero-downtime patching, which works on a best-effort basis to preserve client connections through the patching process. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Zero-downtime patching

The zero-downtime patching (ZDP) feature attempts, on a best-effort basis, to preserve client connections through an engine patch. For more information about ZDP, see Using zero-downtime patching (p. 880).

New features:

• `SELECT INTO OUTFILE S3` – Aurora MySQL now allows you to upload the results of a query to one or more files in an Amazon S3 bucket. For more information, see Saving data from an Amazon Aurora MySQL DB cluster into text files in an Amazon S3 bucket (p. 812).
Improvements:

- Implemented truncation of CSV format log files at engine startup to avoid long recovery time. The `general_log_backup`, `general_log`, `slow_log_backup`, and `slow_log` tables now don't survive a database restart.
- Fixed an issue where migration of a database named `test` would fail.
- Improved stability in the lock manager's garbage collector by reusing the correct lock segments.
- Improved stability of the lock manager by removing invalid assertions during deadlock detection algorithm.
- Re-enabled asynchronous replication, and fixed an associated issue which caused incorrect replica lag to be reported under no-load or read-only workload. The replication pipeline improvements that were introduced in version 1.10. These improvements were introduced in order to apply log stream updates to the buffer cache of an Aurora Replica, which helps to improve read performance and stability on Aurora Replicas.
- Fixed an issue where autocommit=OFF leads to scheduled events being blocked and long transactions being held open until the server reboots.
- Fixed an issue where general, audit, and slow query logs could not log queries handled by asynchronous commit.
- Improved the performance of the logical read ahead (LRA) feature by up to 2.5 times. This was done by allowing pre-fetches to continue across intermediate pages in a B-tree.
- Added parameter validation for audit variables to trim unnecessary spaces.
- Fixed a regression, introduced in Aurora MySQL version 1.11, in which queries can return incorrect results when using the `SQL_CALC_FOUND_ROWS` option and invoking the `FOUND_ROWS()` function.
- Fixed a stability issue when the Metadata Lock list was incorrectly formed.
- Improved stability when `sql_mode` is set to `PAD_CHAR_TO_FULL_LENGTH` and the command `SHOW FUNCTION STATUS WHERE Db='string'` is executed.
- Fixed a rare case when instances would not come up after Aurora version upgrade because of a false volume consistency check.
- Fixed the performance issue, introduced in Aurora MySQL version 1.12, where the performance of the Aurora writer was reduced when users have a large number of tables.
- Improved stability issue when the Aurora writer is configured as a binlog worker and the number of connections approaches 16,000.
- Fixed a rare issue where an Aurora Replica could restart when a connection gets blocked waiting for Metadata Lock when running DDL on the Aurora master.

Integration of MySQL bug fixes

- With an empty InnoDB table, it's not possible to decrease the auto_increment value using an `ALTER TABLE` statement, even when the table is empty. (Bug #69882)
- `MATCH() ... AGAINST queries that use a long string as an argument for AGAINST() could result in an error when run on an InnoDB table with a full-text search index. (Bug #17640261)
- Handling of `SQL_CALC_FOUND_ROWS` in combination with `ORDER BY` and `LIMIT` could lead to incorrect results for `FOUND_ROWS()`. (Bug #68458, Bug #16383173)
- `ALTER TABLE` does not allow to change nullability of the column if foreign key exists. (Bug #77591)

Aurora MySQL database engine updates: 2017-04-05

Version: 1.12
Aurora MySQL 1.12 is now the preferred version for the creation of new DB clusters, including restores from snapshots.

This is not a mandatory upgrade for existing clusters. You will have the option to upgrade existing clusters to version 1.12 after we complete the fleet-wide patch to 1.11 (see Aurora 1.11 release notes (p. 964) and corresponding forum announcement). With version 1.12 of Aurora, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

New features

- **Fast DDL** – Aurora MySQL now allows you to execute an ALTER TABLE `tbl_name` ADD COLUMN `col_name` `column_definition` operation nearly instantaneously. The operation completes without requiring the table to be copied and without materially impacting other DML statements. Since it does not consume temporary storage for a table copy, it makes DDL statements practical even for large tables on small instance classes. Fast DDL is currently only supported for adding a nullable column, without a default value, at the end of a table. This feature is currently available in Aurora lab mode. For more information, see Altering tables in Amazon Aurora using fast DDL (p. 693).

- **Show volume status** – We have added a new monitoring command, SHOW VOLUME STATUS, to display the number of nodes and disks in a volume. For more information, see Displaying volume status for an Aurora DB cluster (p. 696).

Improvements

- Implemented changes to lock compression to further reduce memory allocated per lock object. This improvement is available in lab mode.

- Fixed an issue where the `trx_active_transactions` metric decrements rapidly even when the database is idle.

- Fixed an invalid error message regarding fault injection query syntax when simulating failure in disks and nodes.

- Fixed multiple issues related to race conditions and dead latches in the lock manager.

- Fixed an issue causing a buffer overflow in the query optimizer.

- Fixed a stability issue in Aurora read replicas when the underlying storage nodes experience low available memory.

- Fixed an issue where idle connections persisted past the `wait_timeout` parameter setting.

- Fixed an issue where `query_cache_size` returns an unexpected value after reboot of the instance.

- Fixed a performance issue that is the result of a diagnostic thread probing the network too often in the event that writes are not progressing to storage.

Integration of MySQL bug fixes

- Reloading a table that was evicted while empty caused an AUTO_INCREMENT value to be reset. (Bug #21454472, Bug #77743)

- An index record was not found on rollback due to inconsistencies in the `purge_node_t` structure. The inconsistency resulted in warnings and error messages such as "error in sec index entry update", "unable to purge a record", and "tried to purge sec index entry not marked for deletion". (Bug #19138298, Bug #70214, Bug #21126772, Bug #21065746)

- Wrong stack size calculation for qsort operation leads to stack overflow. (Bug #73979)

- Record not found in an index upon rollback. (Bug #70214, Bug #72419)

- ALTER TABLE add column TIMESTAMP on update CURRENT_TIMESTAMP inserts ZERO-datas (Bug #17392)
Aurora MySQL database engine updates: 2017-02-23

Version: 1.11

We will patch all Aurora MySQL DB clusters with the latest version over a short period following the release. DB clusters are patched using the legacy procedure with a downtime of about 5-30 seconds.

Patching occurs during the system maintenance window that you have specified for each of your database instances. You can view or change this window using the AWS Management Console. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Alternatively, you can apply the patch immediately in the AWS Management Console by choosing a DB cluster, choosing Cluster Actions, and then choosing Upgrade Now.

With version 1.11 of Aurora MySQL, we are using a cluster patching model where all nodes in an Aurora DB cluster are patched at the same time.

New features

- **MANIFEST option for LOAD DATA FROM S3** – LOAD DATA FROM S3 was released in version 1.8. The options for this command have been expanded, and you can now specify a list of files to be loaded into an Aurora DB cluster from Amazon S3 by using a manifest file. This makes it easy to load data from specific files in one or more locations, as opposed to loading data from a single file by using the FILE option or loading data from multiple files that have the same location and prefix by using the PREFIX option. The manifest file format is the same as that used by Amazon Redshift. For more information about using LOAD DATA FROM S3 with the MANIFEST option, see Using a manifest to specify data files to load (p. 807).

- **Spatial indexing enabled by default** – This feature was released in lab mode in version 1.10, and is now turned on by default. Spatial indexing improves query performance on large datasets for queries that use spatial data. For more information about using spatial indexing, see Amazon Aurora MySQL and spatial data (p. 635).

- **Advanced Auditing timing change** – This feature was released in version 1.10.1 to provide a high-performance facility for auditing database activity. In this release, the precision of audit log timestamps has been changed from one second to one microsecond. The more accurate timestamps allow you to better understand when an audit event happened. For more information about audit, see Using advanced auditing with an Amazon Aurora MySQL DB cluster (p. 727).

Improvements

- Modified the thread_handling parameter to prevent you from setting it to anything other than multiple-connections-per-thread, which is the only supported model with Aurora’s thread pool.

- Fixed an issue caused when you set either the buffer_pool_size or the query_cache_size parameter to be larger than the DB cluster’s total memory. In this circumstance, Aurora sets the modified parameter to the default value, so the DB cluster can start up and not crash.

- Fixed an issue in the query cache where a transaction gets stale read results if the table is invalidated in another transaction.

- Fixed an issue where binlog files marked for deletion are removed after a small delay rather than right away.

- Fixed an issue where a database created with the name tmp is treated as a system database stored on ephemeral storage and not persisted to Aurora distributed storage.

- Modified the behavior of SHOW TABLES to exclude certain internal system tables. This change helps avoid an unnecessary failover caused by mysqldump locking all files listed in SHOW TABLES, which in turn prevents writes on the internal system table, causing the failover.
• Fixed an issue where an Aurora Replica incorrectly restarts when creating a temporary table from a query that invokes a function whose argument is a column of an InnoDB table.
• Fixed an issue related to a metadata lock conflict in an Aurora Replica node that causes the Aurora Replica to fall behind the primary DB cluster and eventually get restarted.
• Fixed a dead latch in the replication pipeline in reader nodes, which causes an Aurora Replica to fall behind and eventually get restarted.
• Fixed an issue where an Aurora Replica lags too much with encrypted volumes larger than 1 terabyte (TB).
• Improved Aurora Replica dead latch detection by using an improved way to read the system clock time.
• Fixed an issue where an Aurora Replica can restart twice instead of once following de-registration by the writer.
• Fixed a slow query performance issue on Aurora Replicas that occurs when transient statistics cause statistics discrepancy on non-unique index columns.
• Fixed an issue where an Aurora Replica can crash when a DDL statement is replicated on the Aurora Replica at the same time that the Aurora Replica is processing a related query.
• Changed the replication pipeline improvements that were introduced in version 1.10 from enabled by default to disabled by default. These improvements were introduced in order to apply log stream updates to the buffer cache of an Aurora Replica, and although this feature helps to improve read performance and stability on Aurora Replicas, it increases replica lag in certain workloads.
• Fixed an issue where the simultaneous occurrence of an ongoing DDL statement and pending Parallel Read Ahead on the same table causes an assertion failure during the commit phase of the DDL transaction.
• Enhanced the general log and slow query log to survive DB cluster restart.
• Fixed an out-of-memory issue for certain long running queries by reducing memory consumption in the ACL module.
• Fixed a restart issue that occurs when a table has non-spatial indexes, there are spatial predicates in the query, the planner chooses to use a non-spatial index, and the planner incorrectly pushes the spatial condition down to the index.
• Fixed an issue where the DB cluster restarts when there is a delete, update, or purge of very large geospatial objects that are stored externally (like LOBs).
• Fixed an issue where fault simulation using ALTER SYSTEM SIMULATE ... FOR INTERVAL isn't working properly.
• Fixed a stability issue caused by an invalid assertion on an incorrect invariant in the lock manager.
• Disabled the following two improvements to InnoDB Full-Text Search that were introduced in version 1.10 because they introduce stability issues for some demanding workloads:
  • Updating the cache only after a read request to an Aurora Replica in order to improve full-text search index cache replication speed.
  • Offloading the cache sync task to a separate thread as soon as the cache size crosses 10% of the total size, in order to avoid MySQL queries stalling for too long during FTS cache sync to disk. (Bugs #22516559, #73816).

Integration of MySQL bug fixes

• Running ALTER table DROP foreign key simultaneously with another DROP operation causes the table to disappear. (Bug #16095573)
• Some INFORMATION_SCHEMA queries that used ORDER BY did not use a filesort optimization as they did previously. (Bug #16423536)
• FOUND_ROWS () returns the wrong count of rows on a table. (Bug #68458)
• The server fails instead of giving an error when too many temp tables are open. (Bug #18948649)
Aurora MySQL database engine updates: 2017-01-12

Version: 1.10.1

Version 1.10.1 of Aurora MySQL is an opt-in version and is not used to patch your database instances. It is available for creating new Aurora instances and for upgrading existing instances. You can apply the patch by choosing a cluster in the Amazon RDS console, choosing Cluster Actions, and then choosing Upgrade Now. Patching requires a database restart with downtime typically lasting 5-30 seconds, after which you can resume using your DB clusters. This patch is using a cluster patching model where all nodes in an Aurora cluster are patched at the same time.

New features

• **Advanced Auditing** – Aurora MySQL provides a high-performance Advanced Auditing feature, which you can use to audit database activity. For more information about enabling and using Advanced Auditing, see Using advanced auditing with an Amazon Aurora MySQL DB cluster (p. 727).

Improvements

• Fixed an issue with spatial indexing when creating a column and adding an index on it in the same statement.
• Fixed an issue where spatial statistics aren't persisted across DB cluster restart.

Aurora MySQL database engine updates: 2016-12-14

Version: 1.10

New features

• **Zero downtime patch** – This feature allows a DB instance to be patched without any downtime. That is, database upgrades are performed without disconnecting client applications, or rebooting the database. This approach increases the availability of your Aurora DB clusters during the maintenance window. Note that temporary data like that in the performance schema is reset during the upgrade process. This feature applies to service-delivered patches during a maintenance window as well as user-initiated patches.

When a patch is initiated, the service ensures there are no open locks, transactions or temporary tables, and then waits for a suitable window during which the database can be patched and restarted. Application sessions are preserved, although there is a drop in throughput while the patch is in progress (for approximately 5 seconds). If no suitable window can be found, then patching defaults to the standard patching behavior.

Zero downtime patching takes place on a best-effort basis, subject to certain limitations as described following:

• This feature is currently applicable for patching single-node DB clusters or writer instances in multi-node DB clusters.
• SSL connections are not supported in conjunction with this feature. If there are active SSL connections, Amazon Aurora MySQL won't perform a zero downtime patch, and instead will retry periodically to see if the SSL connections have terminated. If they have, zero downtime patching proceeds. If the SSL connections persist after more than a couple seconds, standard patching with downtime proceeds.
• The feature is available in Aurora release 1.10 and beyond. Going forward, we will identify any releases or patches that can't be applied by using zero downtime patching.
• This feature is not applicable if replication based on binary logging is active.
• **Spatial indexing** – Spatial indexing improves query performance on large datasets for queries that use spatial data. For more information about using spatial indexing, see Amazon Aurora MySQL and spatial data (p. 635).

  This feature is disabled by default and can be activated by enabling Aurora lab mode. For information, see Amazon Aurora MySQL lab mode (p. 839).

• **Replication pipeline improvements** – Aurora MySQL now uses an improved mechanism to apply log stream updates to the buffer cache of an Aurora Replica. This feature improves the read performance and stability on Aurora Replicas when there is a heavy write load on the master as well as a significant read load on the Replica. This feature is enabled by default.

• **Throughput improvement for workloads with cached reads** – Aurora MySQL now uses a latch-free concurrent algorithm to implement read views, which leads to better throughput for read queries served by the buffer cache. As a result of this and other improvements, Amazon Aurora MySQL can achieve throughput of up to 625K reads per second compared to 164K reads per second by MySQL 5.7 for a SysBench SELECT-only workload.

• **Throughput improvement for workloads with hot row contention** – Aurora MySQL uses a new lock release algorithm that improves performance, particularly when there is hot page contention (that is, many transactions contending for the rows on the same page). In tests with the TPC-C benchmark, this can result in up to 16x throughput improvement in transactions per minute relative to MySQL 5.7. This feature is disabled by default and can be activated by enabling Aurora lab mode. For information, see Amazon Aurora MySQL lab mode (p. 839).

**Improvements**

• Full-text search index cache replication speed has been improved by updating the cache only after a read request to an Aurora Replica. This approach avoids any reads from disk by the replication thread.

• Fixed an issue where dictionary cache invalidation does not work on an Aurora Replica for tables that have a special character in the database name or table name.

• Fixed a **STUCK IO** issue during data migration for distributed storage nodes when storage heat management is enabled.

• Fixed an issue in the lock manager where an assertion check fails for the transaction lock wait thread when preparing to rollback or commit a transaction.

• Fixed an issue when opening a corrupted dictionary table by correctly updating the reference count to the dictionary table entries.

• Fixed a bug where the DB cluster minimum read point can be held by slow Aurora Replicas.

• Fixed a potential memory leak in the query cache.

• Fixed a bug where an Aurora Replica places a row-level lock on a table when a query is used in an IF statement of a stored procedure.

**Integration of MySQL bug fixes**

• UNION of derived tables returns wrong results with '1=0/false'-clauses. (Bug #69471)

• Server crashes in ITEM_FUNC_GROUP_CONCAT::FIX_FIELDS on 2nd execution of stored procedure. (Bug #20755389)

• Avoid MySQL queries from stalling for too long during FTS cache sync to disk by offloading the cache sync task to a separate thread, as soon as the cache size crosses 10% of the total size. (Bug #22516559, #73816)

**Aurora MySQL database engine updates: 2016-11-10**

**Version:** 1.9.0, 1.9.1
New features

- **Improved index build** – The implementation for building secondary indexes now operates by building the index in a bottom-up fashion, which eliminates unnecessary page splits. This can reduce the time needed to create an index or rebuild a table by up to 75% (based on an `db.r3.8xlarge` DB instance class). This feature was in lab mode in Aurora MySQL version 1.7 and is enabled by default in Aurora version 1.9 and later. For information, see Amazon Aurora MySQL lab mode (p. 839).

- **Lock compression (lab mode)** – This implementation significantly reduces the amount of memory that lock manager consumes by up to 66%. Lock manager can acquire more row locks without encountering an out-of-memory exception. This feature is disabled by default and can be activated by enabling Aurora lab mode. For information, see Amazon Aurora MySQL lab mode (p. 839).

- **Performance schema** – Aurora MySQL now includes support for performance schema with minimal impact on performance. In our testing using SysBench, enabling performance schema could degrade MySQL performance by up to 60%.

  SysBench testing of an Aurora DB cluster showed an impact on performance that is 4x less than MySQL. Running the `db.r3.8xlarge` DB instance class resulted in 100K SQL writes/sec and over 550K SQL reads/sec, even with performance schema enabled.

- **Hot row contention improvement** – This feature reduces CPU utilization and increases throughput when a small number of hot rows are accessed by a large number of connections. This feature also eliminates error 188 when there is hot row contention.

- **Improved out-of-memory handling** – When non-essential, locking SQL statements are executed and the reserved memory pool is breached, Aurora forces rollback of those SQL statements. This feature frees memory and prevents engine crashes due to out-of-memory exceptions.

- **Smart read selector** – This implementation improves read latency by choosing the optimal storage segment among different segments for every read, resulting in improved read throughput. SysBench testing has shown up to a 27% performance increase for write workloads.

Improvements

- Fixed an issue where an Aurora Replica encounters a shared lock during engine start up.
- Fixed a potential crash on an Aurora Replica when the read view pointer in the purge system is NULL.

Aurora MySQL database engine updates: 2016-10-26

**Version:** 1.8.1

**Improvements**

- Fixed an issue where bulk inserts that use triggers that invoke AWS Lambda procedures fail.
- Fixed an issue where catalog migration fails when autocommit is off globally.
- Resolved a connection failure to Aurora when using SSL and improved Diffie-Hellman group to deal with LogJam attacks.

Integration of MySQL bug fixes

- OpenSSL changed the Diffie-Hellman key length parameters due to the LogJam issue. (Bug #18367167)

Aurora MySQL database engine updates: 2016-10-18

**Version:** 1.8
New features

- **AWS Lambda integration** – You can now asynchronously invoke an AWS Lambda function from an Aurora DB cluster using the `mysql.lambda_async` procedure. For more information, see Invoking a Lambda function from an Amazon Aurora MySQL DB cluster (p. 818).

- **Load data from Amazon S3** – You can now load text or XML files from an Amazon S3 bucket into your Aurora DB cluster using the `LOAD DATA FROM S3` or `LOAD XML FROM S3` commands. For more information, see Loading data into an Amazon Aurora MySQL DB cluster from text files in an Amazon S3 bucket (p. 804).

- **Catalog migration** – Aurora now persists catalog metadata in the cluster volume to support versioning. This enables seamless catalog migration across versions and restores.

- **Cluster-level maintenance and patching** – Aurora now manages maintenance updates for an entire DB cluster. For more information, see Maintaining an Amazon Aurora DB cluster (p. 388).

Improvements

- Fixed an issue where an Aurora Replica crashes when not granting a metadata lock to an inflight DDL table.

- Allowed Aurora Replicas to modify non-InnoDB tables to facilitate rotation of the slow and general log CSV files where `log_output=TABLE`.

- Fixed a lag when updating statistics from the primary instance to an Aurora Replica. Without this fix, the statistics of the Aurora Replica can get out of sync with the statistics of the primary instance and result in a different (and possibly under-performing) query plan on an Aurora Replica.

- Fixed a race condition that ensures that an Aurora Replica does not acquire locks.

- Fixed a rare scenario where an Aurora Replica that registers or de-registers with the primary instance could fail.

- Fixed a race condition that could lead to a deadlock on `db.r3.large` instances when opening or closing a volume.

- Fixed an out-of-memory issue that can occur due to a combination of a large write workload and failures in the Aurora Distributed Storage service.

- Fixed an issue with high CPU consumption because of the purge thread spinning in the presence of a long-running transaction.

- Fixed an issue when running information schema queries to get information about locks under heavy load.

- Fixed an issue with a diagnostics process that could in rare cases cause Aurora writes to storage nodes to stall and restart/fail-over.

- Fixed a condition where a successfully created table might be deleted during crash recovery if the crash occurred while a `CREATE TABLE [if not exists]` statement was being handled.

- Fixed a case where the log rotation procedure is broken when the general log and slow log are not stored on disk using catalog mitigation.

- Fixed a crash when a user creates a temporary table within a user defined function, and then uses the user defined function in the select list of the query.

- Fixed a crash that occurred when replaying GTID events. GTID is not supported by Aurora MySQL.

Integration of MySQL bug fixes:

- When dropping all indexes on a column with multiple indexes, InnoDB failed to block a DROP INDEX operation when a foreign key constraint requires an index. (Bug #16896810)

- Solve add foreign key constraint crash. (Bug #16413976)

- Fixed a crash when fetching a cursor in a stored procedure, and analyzing or flushing the table at the same time. (Bug # 18158639)
• Fixed an auto-increment bug when a user alters a table to change the AUTO_INCREMENT value to less than the maximum auto-increment column value. (Bug # 16310273)

Aurora MySQL database engine updates: 2016-09-20

Version: 1.7.1

Improvements

• Fixes an issue where an Aurora Replica crashes if the InnoDB full-text search cache is full.
• Fixes an issue where the database engine crashes if a worker thread in the thread pool waits for itself.
• Fixes an issue where an Aurora Replica crashes if a metadata lock on a table causes a deadlock.
• Fixes an issue where the database engine crashes due to a race condition between two worker threads in the thread pool.
• Fixes an issue where an unnecessary failover occurs under heavy load if the monitoring agent doesn’t detect the advancement of write operations to the distributed storage subsystem.

Aurora MySQL database engine updates: 2016-08-30

Version: 1.7.0

New features

• NUMA aware scheduler – The task scheduler for the Aurora MySQL engine is now Non-Uniform Memory Access (NUMA) aware. This minimizes cross-CPU socket contention resulting in improved performance throughput for the db.r3.8xlarge DB instance class.
• Parallel read-ahead operates asynchronously in the background – Parallel read-ahead has been revised to improve performance by using a dedicated thread to reduce thread contention.
• Improved index build (lab mode) – The implementation for building secondary indexes now operates by building the index in a bottom-up fashion, which eliminates unnecessary page splits. This can reduce the time needed to create an index or rebuild a table. This feature is disabled by default and can be activated by enabling Aurora lab mode. For information, see Amazon Aurora MySQL lab mode (p. 839).

Improvements

• Fixed an issue where establishing a connection was taking a long time if there was a surge in the number of connections requested for an instance.
• Fixed an issue where a crash occurred if ALTER TABLE was run on a partitioned table that did not use InnoDB.
• Fixed an issue where heavy write workload can cause a failover.
• Fixed an erroneous assertion that caused a failure if RENAME TABLE was run on a partitioned table.
• Improved stability when rolling back a transaction during insert-heavy workload.
• Fixed an issue where full-text search indexes were not viable on an Aurora Replica.

Integration of MySQL bug fixes

• Improve scalability by partitioning LOCK_grant lock. (Port WL #8355)
• Opening cursor on SELECT in stored procedure causes segfault. (Port Bug #16499751)
• MySQL gives the wrong result with some special usage. (Bug #11751794)
• Crash in GET_SEL_ARG_FOR_KEYPART – caused by patch for bug #11751794. (Bug #16208709)
• Wrong results for a simple query with GROUP BY. (Bug #17909656)
• Extra rows on semijoin query with range predicates. (Bug #16221623)
• Adding an ORDER BY clause following an IN subquery could cause duplicate rows to be returned. (Bug #16308085)
• Crash with explain for a query with loose scan for GROUP BY, MyISAM. (Bug #16222245)
• Loose index scan with quoted int predicate returns random data. (Bug #16394084)
• If the optimizer was using a loose index scan, the server could exit while attempting to create a temporary table. (Bug #16436567)
• COUNT(DISTINCT) should not count NULL values, but they were counted when the optimizer used loose index scan. (Bug #17222452)
• If a query had both MIN()/MAX() and aggregate_function(DISTINCT) (for example, SUM(DISTINCT)) and was executed using loose index scan, the result values of MIN()/MAX() were set improperly. (Bug #17217128)

Aurora MySQL database engine updates: 2016-06-01

Version: 1.6.5

New features

• Efficient storage of Binary Logs – Efficient storage of binary logs is now enabled by default for all Aurora MySQL DB clusters, and is not configurable. Efficient storage of binary logs was introduced in the April 2016 update. For more information, see Aurora MySQL database engine updates: 2016-04-06 (p. 971).

Improvements

• Improved stability for Aurora Replicas when the primary instance is encountering a heavy workload.
• Improved stability for Aurora Replicas when running queries on partitioned tables and tables with special characters in the table name.
• Fixed connection issues when using secure connections.

Integration of MySQL bug fixes

• SLAVE CAN'T CONTINUE REPLICATION AFTER MASTER'S CRASH RECOVERY (Port Bug #17632285)

Aurora MySQL database engine updates: 2016-04-06

Version: 1.6

This update includes the following improvements:

New features

• Parallel read-ahead – Parallel read-ahead is now enabled by default for all Aurora MySQL DB clusters, and is not configurable. Parallel read-ahead was introduced in the December 2015 update. For more information, see Aurora MySQL database engine updates: 2015-12-03 (p. 973).
In addition to enabling parallel read-ahead by default, this release includes the following improvements to parallel read-ahead:

- Improved logic so that parallel read-ahead is less aggressive, which is beneficial when your DB cluster encounters many parallel workloads.
- Improved stability on smaller tables.

**Efficient storage of Binary Logs (lab mode)** – MySQL binary log files are now stored more efficiently in Aurora MySQL. The new storage implementation enables binary log files to be deleted much earlier and improves system performance for an instance in an Aurora MySQL DB cluster that is a binary log replication master.

To enable efficient storage of binary logs, set the `aurora_lab_mode` parameter to 1 in the parameter group for your primary instance or Aurora Replica. The `aurora_lab_mode` parameter is an instance-level parameter that is in the `default.aurora5.6` parameter group by default. For information on modifying a DB parameter group, see Modifying parameters in a DB parameter group (p. 303). For information on parameter groups and Aurora MySQL, see Aurora MySQL parameters (p. 848).

Only turn on efficient storage of binary logs for instances in an Aurora MySQL DB cluster that are MySQL binary log replication master instances.

**AURORA_VERSION system variable** – You can now get the Aurora version of your Aurora MySQL DB cluster by querying for the `AURORA_VERSION` system variable.

To get the Aurora version, use one of the following queries:

```
select AURORA_VERSION();
select @@aurora_version;
show variables like '%version';
```

You can also see the Aurora version in the AWS Management Console when you modify a DB cluster, or by calling the `describe-db-engine-versions` AWS CLI command or the DescribeDBEngineVersions API operation.

**Lock manager memory usage metric** – Information about lock manager memory usage is now available as a metric.

To get the lock manager memory usage metric, use one of the following queries:

```
show global status where variable_name in ('aurora_lockmgr_memory_used');
select * from INFORMATION_SCHEMA.GLOBAL_STATUS where variable_name in ('aurora_lockmgr_memory_used');
```

**Improvements**

- Improved stability during binlog and XA transaction recovery.
- Fixed a memory issue resulting from a large number of connections.
- Improved accuracy in the following metrics: Read Throughput, Read IOPS, Read Latency, Write Throughput, Write IOPS, Write Latency, and Disk Queue Depth.
- Fixed a stability issue causing slow startup for large instances after a crash.
- Improved concurrency in the data dictionary regarding synchronization mechanisms and cache eviction.
- Stability and performance improvements for Aurora Replicas:
  - Fixed a stability issue for Aurora Replicas during heavy or burst write workloads for the primary instance.
• Improved replica lag for db.r3.4xlarge and db.r3.8xlarge instances.
• Improved performance by reducing contention between application of log records and concurrent
  reads on an Aurora Replica.
• Fixed an issue for refreshing statistics on Aurora Replicas for newly created or updated statistics.
• Improved stability for Aurora Replicas when there are many transactions on the primary instance
  and concurrent reads on the Aurora Replicas across the same data.
• Improved stability for Aurora Replicas when running UPDATE and DELETE statements with JOIN
  statements.
• Improved stability for Aurora Replicas when running INSERT ... SELECT statements.

Integration of MySQL bug fixes

• BACKPORT Bug #18694052 FIX FOR ASSERTION `!M_ORDERED_REC_BUFFER' FAILED TO 5.6 (Port
  Bug #18305270)
• SEGV IN MEMCPY(), HA_PARTITION::POSITION (Port Bug # 18383840)
• WRONG RESULTS WITH PARTITIONING,INDEX_MERGE AND NO PK (Port Bug # 18167648)
• FLUSH TABLES FOR EXPORT: ASSERTION IN HA_PARTITION::EXTRA (Port Bug # 16943907)
• SERVER CRASH IN VIRTUAL HA_ROWS HANDLER::MULTI_RANGE_READ_INFO_CONST (Port Bug #
  16164031)
• RANGE OPTIMIZER CRASHES IN SEL_ARG::RB_INSERT() (Port Bug # 16241773)

Aurora MySQL database engine updates: 2016-01-11

Version: 1.5

This update includes the following improvements:

Improvements

• Fixed a 10 second pause of write operations for idle instances during Aurora storage deployments.
• Logical read-ahead now works when innodb_file_per_table is set to No. For more information on
  logical read-ahead, see Aurora MySQL database engine updates: 2015-12-03 (p. 973).
• Fixed issues with Aurora Replicas reconnecting with the primary instance. This improvement also
  fixes an issue when you specify a large value for the quantity parameter when testing Aurora
  Replica failures using fault-injection queries. For more information, see Testing an Aurora replica
  failure (p. 691).
• Improved monitoring of Aurora Replicas falling behind and restarting.
• Fixed an issue that caused an Aurora Replica to lag, become deregistered, and then restart.
• Fixed an issue when you run the show innodb status command during a deadlock.
• Fixed an issue with failovers for larger instances during high write throughput.

Integration of MySQL bug fixes

• Addressed incomplete fix in MySQL full text search affecting tables where the database name begins
  with a digit. (Port Bug #17607956)

Aurora MySQL database engine updates: 2015-12-03

Version: 1.4
This update includes the following improvements:

New features

- **Fast Insert** – Accelerates parallel inserts sorted by primary key. For more information, see Amazon Aurora MySQL performance enhancements (p. 634).
- **Large dataset read performance** – Aurora MySQL automatically detects an IO heavy workload and launches more threads in order to boost the performance of the DB cluster. The Aurora scheduler looks into IO activity and decides to dynamically adjust the optimal number of threads in the system, quickly adjusting between IO heavy and CPU heavy workloads with low overhead.
- **Parallel read-ahead** – Improves the performance of B-Tree scans that are too large for the memory available on your primary instance or Aurora Replica (including range queries). Parallel read-ahead automatically detects page read patterns and pre-fetches pages into the buffer cache in advance of when they are needed. Parallel read-ahead works multiple tables at the same time within the same transaction.

Improvements:

- Fixed brief Aurora database availability issues during Aurora storage deployments.
- Correctly enforce the `max_connection` limit.
- Improve binlog purging where Aurora is the binlog master and the database is restarting after a heavy data load.
- Fixed memory management issues with the table cache.
- Add support for huge pages in shared memory buffer cache for faster recovery.
- Fixed an issue with thread-local storage not being initialized.
- Allow 16K connections by default.
- Dynamic thread pool for IO heavy workloads.
- Fixed an issue with properly invalidating views involving UNION in the query cache.
- Fixed a stability issue with the dictionary stats thread.
- Fixed a memory leak in the dictionary subsystem related to cache eviction.
- Fixed high read latency issue on Aurora Replicas when there is very low write load on the master.
- Fixed stability issues on Aurora Replicas when performing operations on DDL partitioned tables such as `ALTER TABLE ... REORGANIZE PARTITION` on the master.
- Fixed stability issues on Aurora Replicas during volume growth.
- Fixed performance issue for scans on non-clustered indexes in Aurora Replicas.
- Fix stability issue that makes Aurora Replicas lag and eventually get deregistered and re-started.

Integration of MySQL bug fixes

- SEGV in FTSPARSE(). (Bug #16446108)
- InnoDB data dictionary is not updated while renaming the column. (Bug #19465984)
- FTS crash after renaming table to different database. (Bug #16834860)
- Failed preparing of trigger on truncated tables cause error 1054. (Bug #18596756)
- Metadata changes might cause problems with trigger execution. (Bug #18684393)
- Materialization is not chosen for long UTF8 VARCHAR field. (Bug #17566396)
- Poor execution plan when ORDER BY with limit X. (Bug #16697792)
- Backport bug #11765744 TO 5.1, 5.5 AND 5.6. (Bug #17083851)
- Mutex issue in SQL/SQL_SHOW.CC resulting in SIG6. Source likely FILL_VARIABLES. (Bug #20788853)
- Backport bug #18008907 to 5.5+ versions. (Bug #18903155)
• Adapt fix for a stack overflow error in MySQL 5.7. (Bug #19678930)

**Aurora MySQL database engine updates: 2015-10-16**

**Versions:** 1.2, 1.3

This update includes the following improvements:

**Fixes**

• Resolved out-of-memory issue in the new lock manager with long-running transactions
• Resolved security vulnerability when replicating with non-RDS MySQL databases
• Updated to ensure that quorum writes retry correctly with storage failures
• Updated to report replica lag more accurately
• Improved performance by reducing contention when many concurrent transactions are trying to modify the same row
• Resolved query cache invalidation for views that are created by joining two tables
• Disabled query cache for transactions with `UNCOMMITTED_READ` isolation

**Improvements**

• Better performance for slow catalog queries on warm caches
• Improved concurrency in dictionary statistics
• Better stability for the new query cache resource manager, extent management, files stored in Amazon Aurora smart storage, and batch writes of log records

**Integration of MySQL bug fixes**

• Killing a query inside innodb causes it to eventually crash with an assertion. (Bug #1608883)
• For failure to create a new thread for the event scheduler, event execution, or new connection, no message was written to the error log. (Bug #16865959)
• If one connection changed its default database and simultaneously another connection executed SHOW PROCESSLIST, the second connection could access invalid memory when attempting to display the first connection's default database memory. (Bug #11765252)
• PURGE BINARY LOGS by design does not remove binary log files that are in use or active, but did not provide any notice when this occurred. (Bug #13727933)
• For some statements, memory leaks could result when the optimizer removed unneeded subquery clauses. (Bug #15875919)
• During shutdown, the server could attempt to lock an uninitialized mutex. (Bug #16016493)
• A prepared statement that used GROUP_CONCAT() and an ORDER BY clause that named multiple columns could cause the server to exit. (Bug #16075310)
• Performance Schema instrumentation was missing for replica worker threads. (Bug #16083949)
• `STOP SLAVE` could cause a deadlock when issued concurrently with a statement such as `SHOW STATUS` that retrieved the values for one or more of the status variables `Slave_retried_transactions`, `Slave_heartbeat_period`, `Slave_received_heartbeats`, `Slave_last_heartbeat`, or `Slave_running`. (Bug #16088188)
• A full-text query using Boolean mode could return zero results in some cases where the search term was a quoted phrase. (Bug #16206253)
• The optimizer's attempt to remove redundant subquery clauses raised an assertion when executing a prepared statement with a subquery in the ON clause of a join in a subquery. (Bug #16318585)
• GROUP_CONCAT unstable, crash in ITEM_SUM::CLEAN_UP_AFTER_REMOVAL. (Bug #16347450)

• Attempting to replace the default InnoDB full-text search (FTS) stopword list by creating an InnoDB table with the same structure as INFORMATION_SCHEMA.INNODB_FT_DEFAULT_STOPWORD would result in an error. (Bug #16373868)

• After the client thread on a worker performed a FLUSH TABLES WITH READ LOCK and was followed by some updates on the master, the worker hung when executing SHOW SLAVE STATUS. (Bug #16387720)

• When parsing a delimited search string such as “abc-def” in a full-text search, InnoDB now uses the same word delimiters as MyISAM. (Bug #16419661)

• Crash in FTS_AST_TERM_SET_WILDCARD. (Bug #16429306)

• SEGFAULT in FTS_AST_VISIT() for FTS RQG test. (Bug #16435855)

• For debug builds, when the optimizer removed an Item_ref pointing to a subquery, it caused a server exit. (Bug #16509874)

• Full-text search on InnoDB tables failed on searches for literal phrases combined with + or - operators. (Bug #16516193)

• START SLAVE failed when the server was started with the options --master-info-repository=TABLE relay-log-info-repository=TABLE and with autocommit set to 0, together with --skip-slave-start. (Bug #16533802)

• Very large InnoDB full-text search (FTS) results could consume an excessive amount of memory. (Bug #16625973)

• In debug builds, an assertion could occur in OPT_CHECK_ORDER_BY when using binary directly in a search string, as binary might include NULL bytes and other non-meaningful characters. (Bug #16766016)

• For some statements, memory leaks could result when the optimizer removed unneeded subquery clauses. (Bug #16807641)

• It was possible to cause a deadlock after issuing FLUSH TABLES WITH READ LOCK by issuing STOP SLAVE in a new connection to the worker, then issuing SHOW SLAVE STATUS using the original connection. (Bug #16856735)

• GROUP_CONCAT() with an invalid separator could cause a server exit. (Bug #16870783)

• The server did excessive locking on the LOCK_active_mi and active_mi->rli->data_lock mutexes for any SHOW STATUS LIKE 'pattern' statement, even when the pattern did not match status variables that use those mutexes (Slave_heartbeat_period, Slave_last_heartbeat, Slave_received_heartbeats, Slave_retried_transactions, Slave_running). (Bug #16904035)

• A full-text search using the IN BOOLEAN MODE modifier would result in an assertion failure. (Bug #16927092)

• Full-text search on InnoDB tables failed on searches that used the + boolean operator. (Bug #17280122)

• 4-way deadlock: zombies, purging binlogs, show processlist, show binlogs. (Bug #17283409)

• When an SQL thread which was waiting for a commit lock was killed and restarted it caused a transaction to be skipped on worker. (Bug #17450876)

• An InnoDB full-text search failure would occur due to an "unended" token. The string and string length should be passed for string comparison. (Bug #17659310)

• Large numbers of partitioned InnoDB tables could consume much more memory when used in MySQL 5.6 or 5.7 than the memory used by the same tables used in previous releases of the MySQL Server. (Bug #17780517)

• For full-text queries, a failure to check that num_token is less than max_proximity_item could result in an assertion. (Bug #18233051)

• Certain queries for the INFORMATION_SCHEMA TABLES and COLUMNS tables could lead to excessive memory use when there were large numbers of empty InnoDB tables. (Bug #18592390)
• When committing a transaction, a flag is now used to check whether a thread has been created, rather than checking the thread itself, which uses more resources, particularly when running the server with master_info_repository=TABLE. (Bug #18684222)
• If a client thread on a worker executed FLUSH TABLES WITH READ LOCK while the master executed a DML, executing SHOW SLAVE STATUS in the same client became blocked, causing a deadlock. (Bug #19843808)
• Ordering by a GROUP_CONCAT() result could cause a server exit. (Bug #19880368)

Aurora MySQL database engine updates: 2015-08-24

Version: 1.1

This update includes the following improvements:

• Replication stability improvements when replicating with a MySQL database (binlog replication). For information on Aurora MySQL replication with MySQL, see Replication with Amazon Aurora (p. 57).
• A 1 gigabyte (GB) limit on the size of the relay logs accumulated for an Aurora MySQL DB cluster that is a replication worker. This improves the file management for the Aurora DB clusters.
• Stability improvements in the areas of read ahead, recursive foreign-key relationships, and Aurora replication.
• Integration of MySQL bug fixes.
  • InnoDB databases with names beginning with a digit cause a full-text search (FTS) parser error. (Bug #17607956)
  • InnoDB full-text searches fail in databases whose names began with a digit. (Bug #17161372)
  • For InnoDB databases on Windows, the full-text search (FTS) object ID is not in the expected hexadecimal format. (Bug #16559254)
  • A code regression introduced in MySQL 5.6 negatively impacted DROP TABLE and ALTER TABLE performance. This could cause a performance drop between MySQL Server 5.5.x and 5.6.x. (Bug #16864741)
• Simplified logging to reduce the size of log files and the amount of storage that they require.

Database engine updates for Aurora MySQL Serverless clusters

The following are Aurora MySQL database engine updates for Aurora MySQL Serverless DB clusters. These release notes provide information about bug fixes, updates to the database engine, and other critical information. Aurora Serverless v1 doesn't have its own version number. It shares the version number (and name) of the Aurora database engine that supports Aurora Serverless v1. For more information, see Aurora Serverless v1 and Aurora database engine versions (p. 161).

• Aurora MySQL Serverless 5.7 engine updates 2020-06-18 (version 2.07.1) (p. 977)

• Aurora MySQL Serverless 5.6 engine updates 2020-08-14 (version 1.21.0) (p. 978)

Aurora MySQL Serverless 5.7 engine updates 2020-06-18 (version 2.07.1)

Aurora Serverless 5.7 is generally available. It has the same features and bug fixes as Aurora MySQL 2.07.1.
You can restore a snapshot from a currently supported Aurora MySQL release into Aurora MySQL Serverless 5.7. By using a snapshot, you can also upgrade an Aurora MySQL-5.6 compatible Aurora Serverless v1 DB cluster to an Aurora MySQL-5.7 compatible Aurora Serverless v1 DB cluster. To do so:

- Create a snapshot from the Aurora MySQL 5.6 Serverless DB cluster. To learn how, see Creating a DB cluster snapshot (p. 418).
- Restore the snapshot to a new Aurora MySQL 5.7 Serverless cluster. For more information, see Restoring an Aurora Serverless v1 DB cluster (p. 150).

Aurora Serverless v1 doesn't have its own version number. It uses the number of Aurora MySQL version that supports it to distinguish between Aurora MySQL 5.7 and Aurora MySQL 5.6 updates. For more information, see Aurora Serverless v1 and Aurora database engine versions (p. 161).

For general information about Aurora Serverless, see Using Amazon Aurora Serverless v1 (p. 134).

If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support at http://aws.amazon.com/support. For more information, see Maintaining an Aurora DB cluster.

Bug fixes:

This Aurora Serverless release includes all bug fixes up to Aurora MySQL version 2.07.1. For details, see Aurora MySQL database engine updates 2019-12-23 (version 2.07.1) (p. 895) and the release notes for previous Aurora MySQL versions.

Features:

This Aurora Serverless release includes all new features up to Aurora MySQL version 2.07.1. For details, see Aurora MySQL database engine updates 2019-12-23 (version 2.07.1) (p. 895) and the release notes for previous Aurora MySQL versions. The following features are of particular interest for users of Aurora Serverless or Aurora MySQL with MySQL 5.7 compatibility:

- Aurora MySQL Serverless now supports the hot row contention feature. For more information, see Aurora MySQL database engine updates: 2016-12-14 (p. 966).
- Aurora MySQL Serverless now supports the hash join feature. To use this feature, you must specify the configuration setting `optimizer_switch='hash_join=on'`. For more information, see Working with hash joins in Aurora MySQL (p. 845).
- Aurora Serverless 5.7 can use the Data API. For more information, see Using the Data API for Aurora Serverless (p. 162).
- Aurora Serverless 5.7 can use the query editor. For more information, see Using the query editor for Aurora Serverless (p. 188).
- Aurora Serverless 5.7 supports the same JSON features as other Aurora MySQL versions that are compatible with MySQL 5.7.

**Aurora MySQL Serverless 5.6 engine updates 2020-08-14 (version 1.21.0)**

Aurora Serverless 5.6 is generally available. It has the same features and bug fixes as Aurora MySQL 1.21.0.

Aurora Serverless v1 doesn't have its own version number. It uses the number of Aurora MySQL version that supports it to distinguish between Aurora MySQL 5.6 and Aurora MySQL 5.7 updates. For more information, see Aurora Serverless v1 and Aurora database engine versions (p. 161). For general information about Aurora Serverless, see Using Amazon Aurora Serverless v1 (p. 134).
If you have any questions or concerns, AWS Support is available on the community forums and through AWS Premium Support at http://aws.amazon.com/support. For more information, see Maintaining an Aurora DB cluster.

Bug fixes:

This Aurora Serverless release includes all bug fixes up to Aurora MySQL version 1.21.0. For details, see Aurora MySQL database engine updates 2019-11-25 (version 1.21.0) (p. 941) and the release notes for previous Aurora MySQL versions.

Features:

This Aurora Serverless release improves CPU utilization across the Serverless fleet, especially benefiting clusters with one and two Aurora capacity units (ACUs). See Aurora Serverless v1 architecture (p. 139) for more information about ACUs.

MySQL bugs fixed by Aurora MySQL database engine updates

The following sections identify MySQL bugs that have been fixed by Aurora MySQL database engine updates.

Topics
- MySQL bugs fixed by Aurora MySQL 2.x database engine updates (p. 979)
- MySQL bugs fixed by Aurora MySQL 1.x database engine updates (p. 985)

MySQL bugs fixed by Aurora MySQL 2.x database engine updates

MySQL 5.7-compatible version Aurora contains all MySQL bug fixes through MySQL 5.7.12. The following table identifies additional MySQL bugs that have been fixed by Aurora MySQL database engine updates, and which update they were fixed in.

<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates 2020-12-11 (version 2.09.1) (p. 882) | 2.09.1 | • Replication: Interleaved transactions could sometimes deadlock the slave applier when the transaction isolation level was set to REPEATABLE READ. (Bug #25040331)  
  • For a table having a TIMESTAMP or DATETIME column having a default of CURRENT_TIMESTAMP, the column could be initialized to 0000-00-00 00:00:00 if the table had a BEFORE INSERT trigger. (Bug #25209512, Bug #84077)  
  • For an INSERT statement for which the VALUES list produced values for the second or later row using a subquery containing a join, the server could exit after failing to resolve the required privileges. (Bug #23762382) |
| Aurora MySQL database engine updates 2020-11-12 (version 2.08.3) (p. 887) | 2.08.3 | • Bug #23762382 - INSERT VALUES QUERY WITH JOIN IN A SELECT CAUSES INCORRECT BEHAVIOR.  
  • Bug #25209512 - CURRENT_TIMESTAMP PRODUCES ZEROS IN TRIGGER. |
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates 2020-06-02 (version 2.08.0) (p. 889) | 2.08.0 | - **Bug #25289359**: A full-text cache lock taken when data is synchronized was not released if the full-text cache size exceeded the full-text cache size limit.  
- **Bug #29138644**: Manually changing the system time while the MySQL server was running caused page cleaner thread delays.  
- **Bug #25222337**: A NULL virtual column field name in a virtual index caused a server exit during a field name comparison that occurs while populating virtual columns affected by a foreign key constraint.  
- **Bug #25053286**: Executing a stored procedure containing a query that accessed a view could allocate memory that was not freed until the session ended.  
- **Bug #25586773**: Executing a stored procedure containing a statement that created a table from the contents of certain SELECT statements could result in a memory leak.  
- **Bug #28834208**: During log application, after an OPTIMIZE TABLE operation, InnoDB did not populate virtual columns before checking for virtual column index updates.  
- **Bug #26666274**: Infinite loop in performance schema buffer container due to 32-bit unsigned integer overflow. |
### Database engine update

<table>
<thead>
<tr>
<th>Aurora MySQL database engine updates</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| 2020-11-10 (version 2.07.3) (p. 892) | 2.07.3 | - **InnoDB:** Concurrent XA transactions that ran successfully to the XA prepare stage on the master conflicted when replayed on the slave, resulting in a lock wait timeout in the applier thread. The conflict was due to the GAP lock range which differed when the transactions were replayed serially on the slave. To prevent this type of conflict, GAP locks taken by XA transactions in **READ COMMITTED** isolation level are now released (and no longer inherited) when XA transactions reach the prepare stage. (Bug #27189701, Bug #25866046)
- **InnoDB:** A gap lock was taken unnecessarily during foreign key validation while using the **READ COMMITTED** isolation level. (Bug #25082593)
- **Replication:** When using XA transactions, if a lock wait timeout or deadlock occurred for the applier (SQL) thread on a replication slave, the automatic retry did not work. The cause was that while the SQL thread would do a rollback, it would not roll the XA transaction back. This meant that when the transaction was retried, the first event was XA START which was invalid as the XA transaction was already in progress, leading to an XAER_RMFAIL error. (Bug #24764800)
- **Replication:** Interleaved transactions could sometimes deadlock the slave applier when the transaction isolation level was set to **REPEATABLE READ.** (Bug #25040331)
- **Replication:** The value returned by a **SHOW SLAVE STATUS** statement for the total combined size of all existing relay log files (Relay_Log_Space) could become much larger than the actual disk space used by the relay log files. The I/O thread did not lock the variable while it updated the value, so the SQL thread could automatically delete a relay log file and write a reduced value before the I/O thread finished updating the value. The I/O thread then wrote its original size calculation, ignoring the SQL thread’s update and so adding back the space for the deleted file. The Relay_Log_Space value is now locked during updates to prevent concurrent updates and ensure an accurate calculation. (Bug #26997096, Bug #87832)
- For an **INSERT** statement for which the VALUES list produced values for the second or later row using a subquery containing a join, the server could exit after failing to resolve the required privileges. (Bug #23762382)
- For a table having a **TIMESTAMP** or **DATETIME** column having a default of **CURRENT_TIMESTAMP**, the column could be initialized to **0000-00-00 00:00:00** if the table had a **BEFORE INSERT** trigger. (Bug #25209512, Bug #84077)
- A server exit could result from simultaneous attempts by multiple threads to register and deregister metadata Performance Schema objects. (Bug #26502135)
- Executing a stored procedure containing a statement that created a table from the contents of certain **SELECT** statements could result in a memory leak. (Bug #25586773) |
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Executing a stored procedure containing a query that accessed a view could allocate memory that was not freed until the session ended. (Bug #25053286)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Certain cases of subquery materialization could cause a server exit. These queries now produce an error suggesting that materialization be disabled. (Bug #26402045)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Queries with many left joins were slow if join buffering was used (for example, using the block nested loop algorithm). (Bug #18898433, Bug #72854)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The optimizer skipped the second column in a composite index when executing an inner join with a LIKE clause against the second column. (Bug #28086754)</td>
</tr>
<tr>
<td>Aurora MySQL database engine updates 2020-04-17 (version 2.07.2) (p. 894)</td>
<td>2.07.2</td>
<td>• Bug #23104498: Fixed an issue in Performance Schema in reporting total memory used. (<a href="https://github.com/mysql/mysql-server/commit/20b6840df5452f47313c6f9a6ca075bfbc00a96b">https://github.com/mysql/mysql-server/commit/20b6840df5452f47313c6f9a6ca075bfbc00a96b</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bug #22551677: Fixed an issue in Performance Schema that could lead to the database engine crashing when attempting to take it offline. (<a href="https://github.com/mysql/mysql-server/commit/05e2386eccd32b6b444b900c9f8a87a1d8d531e9">https://github.com/mysql/mysql-server/commit/05e2386eccd32b6b444b900c9f8a87a1d8d531e9</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bug #23550835, Bug #23298025, Bug #81464: Fixed an issue in Performance Schema that causes a database engine crash due to exceeding the capacity of an internal buffer. (<a href="https://github.com/mysql/mysql-server/commit/b4287f93857bf2f99b18fd06f555bbe5b12debf">https://github.com/mysql/mysql-server/commit/b4287f93857bf2f99b18fd06f555bbe5b12debf</a>, <a href="https://github.com/mysql/mysql-server/commit/b4287f93857bf2f99b18fd06f555bbe5b12debf">https://github.com/mysql/mysql-server/commit/b4287f93857bf2f99b18fd06f555bbe5b12debf</a>)</td>
</tr>
<tr>
<td>Aurora MySQL database engine updates 2019-11-25 (version 2.07.0) (p. 895)</td>
<td>2.07.0</td>
<td>• Bug #26251621: INCORRECT BEHAVIOR WITH TRIGGER AND GCOL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bug #22574695: ASSERTION `!TABLE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bug #25966845: INSERT ON DUPLICATE KEY GENERATE A DEADLOCK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bug #23070734: CONCURRENT TRUNCATE TABLES CAUSE STALL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bug #26191879: FOREIGN KEY CASCADES USE EXCESSIVE MEMORY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bug #20989615: INNODB AUTO_INCREMENT PRODUCES SAME VALUE TWICE</td>
</tr>
<tr>
<td>Aurora MySQL database engine updates 2019-11-11 (version 2.05.0) (p. 900)</td>
<td>2.05.0</td>
<td>• Bug#23054591: PURGE BINARY LOGS TO is reading the whole binlog file and causing MySql to Stall</td>
</tr>
<tr>
<td>Database engine update</td>
<td>Version</td>
<td>MySQL bugs fixed</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| Aurora MySQL database engine updates 2020-08-14 (version 2.04.9) (p. 902) | 2.04.9 | - Bug #23070734, Bug #80060: Concurrent TRUNCATE TABLEs cause stalls  
- Bug #23103937: PS_TRUNCATE_ALL_TABLES() DOES NOT WORK IN SUPER_READ_ONLY MODE  
- Bug#22551677: When taking the server offline, a race condition within the Performance Schema could lead to a server exit.  
- Bug #27082268: Invalid FTS sync synchronization.  
- Bug #12589870: Fixed an issues which causes a restart with multi-query statement when query cache is enabled.  
- Bug #26402045: Certain cases of subquery materialization could cause a server exit. These queries now produce an error suggesting that materialization be disabled.  
- Bug #1898433: Queries with many left joins were slow if join buffering was used (for example, using the block nested loop algorithm).  
- Bug #25222337: A NULL virtual column field name in a virtual index caused a server exit during a field name comparison that occurs while populating virtual columns affected by a foreign key constraint. ([https://github.com/mysql/mysql-server/commit/273d5c9d7072c63b6c47dbef6963d7d4c91d5131](https://github.com/mysql/mysql-server/commit/273d5c9d7072c63b6c47dbef6963d7d4c91d5131)  
- Bug #25053286: Executing a stored procedure containing a query that accessed a view could allocate memory that was not freed until the session ended. ([https://github.com/mysql/mysql-server/commit/d7bd37d4d141a95f577916448650c429f0d6e193d](https://github.com/mysql/mysql-server/commit/d7bd37d4d141a95f577916448650c429f0d6e193d))  
- Bug #25586773: Executing a stored procedure containing a statement that created a table from the contents of certain SELECT ([https://dev.mysql.com/doc/refman/5.7/en/select.html](https://dev.mysql.com/doc/refman/5.7/en/select.html)) statements could result in a memory leak. ([https://github.com/mysql/mysql-server/commit/88301e5adab65f6750f66a284be410c4369d0c1](https://github.com/mysql/mysql-server/commit/88301e5adab65f6750f66a284be410c4369d0c1))  
- Bug #26666274: INFINITE LOOP IN PERFORMANCE SCHEMA BUFFER CONTAINER.  
- Bug #23550835, Bug #2329025, Bug #81464: A SELECT Performance Schema tables when an internal buffer was full could cause a server exit.  |
<p>| Aurora MySQL database engine updates 2019-09-19 (version 2.04.6) (p. 909) | 2.04.6 | Bug#23054591: PURGE BINARY LOGS TO is reading the whole binlog file and causing MySql to Stall  |
| Aurora MySQL database engine updates 2019-05-02 (version 2.04.2) (p. 914) | 2.04.2 | Bug #24829050 - INDEX_MERGE_INTERSECTION OPTIMIZATION CAUSES WRONG QUERY RESULTS  |</p>
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates 2018-10-11 (p. 920) | 2.03 | • REVERSE SCAN ON A PARTITIONED TABLE DOES ICP - ORDER BY DESC (Bug #24929748).  
• JSON_OBJECT CREATES INVALID JSON CODE (Bug #26867509).  
• INSERTING LARGE JSON DATA TAKES AN INORDINATE AMOUNT OF TIME (Bug #22843444).  
• PARTITIONED TABLES USE MORE MEMORY IN 5.7 THAN 5.6 (Bug #25080442). |
| Aurora MySQL database engine updates 2018-09-21 (p. 921) | 2.02.4 | • BUG#13651665 INNODB MAY BE UNABLE TO LOAD TABLE DEFINITION AFTER RENAME  
• BUG#21371070 INNODB: CANNOT ALLOCATE 0 BYTES.  
• BUG#21378944 FTS ASSERT ENC.SRC_LIST_PTR != NULL, FTS_OPTIMIZE_WORD(), OPTIMIZE TABLE  
• BUG#21508537 ASSERTION FAILURE UT_A(!VICTIM_TRX->READ_ONLY)  
• BUG#21983865 UNEXPECTED DEADLOCK WITH INNODB_AUTOINC_LOCK_MODE=0  
• BUG#22679185 INVALID INNODB FTS DOC ID DURING INSERT  
• BUG#22899305 GCOLS: ASSERTION: !(COL->PR_TYPE & 256).  
• BUG#22956469 MEMORY LEAK INTRODUCED IN 5.7.8 IN MEMORY/INNODB/OS0FILE  
• BUG#22996488 CRASH IN FTS_SYNC_INDEX WHEN DOING DDL IN A LOOP  
• BUG#23014521 GCOL:INNODB: ASSERTION: !IS_V  
• BUG#23021168 REPLICATION STOPS AFTER TRX IS ROLLED BACK ASYNC  
• BUG#23052231 ASSERTION: ADD_AUTOINC < DICT_TABLE_GET_N_USER_COLS  
• BUG#23149683 ROTATE INNODB MASTER KEY WITH KEYRING_OKV_CONF_DIR MISSING: SIGSEGV; SIGNAL 11  
• BUG#23762382 INSERT VALUES QUERY WITH JOIN IN A SELECT CAUSES INCORRECT BEHAVIOR  
• BUG#25209512 CURRENT_TIMESTAMP PRODUCES ZEROS IN TRIGGER  
• BUG#26626277 BUG IN "INSERT... ON DUPLICATE KEY UPDATE" QUERY  
• BUG#26734162 INCORRECT BEHAVIOR WITH INSERT OF BLOB + ON DUPLICATE KEY UPDATE  
• BUG#27460607 INCORRECT WHEN INSERT SELECT's SOURCE TABLE IS EMPTY |
| Aurora MySQL database engine updates 2018-05-03 (p. 926) | 2.02.0 | Left join returns incorrect results on the outer side (Bug #22833644) |
MySQL bugs fixed by Aurora MySQL 1.x database engine updates

MySQL 5.6-compatible version Aurora contains all MySQL bug fixes through MySQL 5.6.10. The following table identifies additional MySQL bugs that have been fixed by Aurora MySQL database engine updates, and which update they were fixed in.

<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates 2020-09-02 (version 1.23.0) (p. 932) | 1.23.0 | • Binlog events with `ALTER TABLE ADD COLUMN ALGORITHM=QUICK` will be rewritten as `ALGORITHM=DEFAULT` to be compatible with the community edition.  
• BUG #22350047: IF CLIENT KILLED AFTER ROLLBACK TO SAVEPOINT PREVIOUS STMTS COMMITTED  
• Bug #29915479: RUNNING COM_REGISTER_SLAVE WITHOUT COM_BINLOG_DUMP CAN RESULTS IN SERVER EXIT  
• Bug #30441969: BUG #29723340: MYSQL SERVER CRASH AFTER SQL QUERY WITH DATA ?AST  
• Bug #30628268: OUT OF MEMORY CRASH  
• Bug #27081349: UNEXPECTED BEHAVIOUR WHEN DELETE WITH SPATIAL FUNCTION  
• Bug #27230859: UNEXPECTED BEHAVIOUR WHILE HANDLING INVALID POLYGON"  
• Bug #27081349: UNEXPECTED BEHAVIOUR WHEN DELETE WITH SPATIAL"  
• Bug #26935001: ALTER TABLE AUTO_INCREMENT TRIES TO READ INDEX FROM DISCARDED TABLESPACE  
• Bug #29770705: SERVER CRASHED WHILE EXECUTING SELECT WITH SPECIFIC WHERE CLAUSE  
• Bug #27659490: SELECT USING DYNAMIC RANGE AND INDEX MERGE USE TOO MUCH MEMORY(OOM)  
• Bug #24786290: REPLICATION BREAKS AFTER BUG #74145 HAPPENS IN MASTER  
• Bug #27703912: EXCESSIVE MEMORY USAGE WITH MANY PREPARE  
• Bug #20527363: TRUNCATE TEMPORARY TABLE CRASH: ! DICT_TF2_FLAG_IS_SET(TABLE, DICT_TF2_TEMPORARY)  
• Bug#23103937 PS_TRUNCATE_ALL_TABLES() DOES NOT WORK IN SUPER_READ_ONLY MODE  
• Bug #25053286: USE VIEW WITH CONDITION IN PROCEDURE CAUSES INCORRECT BEHAVIOR (fixed in 5.6.36)  
• Bug #25586773: INCORRECT BEHAVIOR FOR CREATE TABLE SELECT IN A LOOP IN SP (fixed in 5.6.39)  
• Bug #27407480: AUTOMATIC_SP_PRIVILEGES REQUIRES NEED THE INSERT PRIVILEGES FOR MYSQL_USER_TABLE  
• Bug #26997096: relay_log_space value is not updated in a synchronized manner so that its value is sometimes much higher than the actual disk space used by relay logs.  
• Bug#15831300 SLAVE_TYPE_CONVERSIONS=ALL_NON_LOSSY NOT WORKING AS EXPECTED |
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates 2020-11-09 (version 1.22.3) (p. 935) | 1.22.3 | • SSL Bug backport Bug #17087862, Bug #20551271  
• Bug #16894092: PERFORMANCE REGRESSION IN 5.6.6+ FOR INSERT INTO ... SELECT ... FROM (fixed in 5.6.15).  
• Port a bug fix related to SLAVE_TYPE_CONVERSIONS. |
| Aurora MySQL database engine updates 2019-11-25 (version 1.22.0) (p. 938) | 1.22.0 | • Bug #16346241 - SERVER CRASH IN ITEM_PARAM::QUERY_VAL_STR  
• Bug #17733850 - NAME_CONST() CRASH IN ITEM_NAME_CONST::ITEM_NAME_CONST()  
• Bug #20989615 - INNODB AUTO_INCREMENT PRODUCES SAME VALUE TWICE  
• Bug #20181776 - ACCESS CONTROL DOESN'T MATCH MOST SPECIFIC HOST WHEN IT CONTAINS WILDCARD  
• Bug #27326796 - MYSQL CRASH WITH INNODB ASSERTION FAILURE IN FILE PARS0PARS.CC  
• Bug #20590013 - IF YOU HAVE A FULLTEXT INDEX AND DROP IT YOU CAN NO LONGER PERFORM ONLINE DDL |
| Aurora MySQL database engine updates 2019-11-25 (version 1.21.0) (p. 941) | 1.21.0 | • Bug #19929406: HANDLE_FATAL_SIGNAL (SIG=11) IN __MEMMOVE_SSSE3_BACK FROM STRING::COPY  
• Bug #17059925: For UNION statements, the rows-examined value was calculated incorrectly. This was manifested as too-large values for the ROWS_EXAMINED column of Performance Schema statement tables (such as events_statements_current).  
• Bug #11827369: Some queries with SELECT ... FROM DUAL nested subqueries raised an assertion.  
• Bug #16311231: Incorrect results were returned if a query contained a subquery in an IN clause that contained an XOR operation in the WHERE clause. |
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates 2019-11-11 (version 1.20.0) (p. 943) | 1.20.0  | • Bug #19929406: HANDLE_FATAL_SIGNAL (SIG=11) IN __MEMMOVE_SSSE3_BACK FROM STRING::COPY  
• Bug #17059925: For UNION statements, the rows-examined value was calculated incorrectly. This was manifested as too-large values for the ROWS_examined column of Performance Schema statement tables (such as events_statements_current).  
• Bug #11827369: Some queries with SELECT ... FROM DUAL nested subqueries raised an assertion.  
• Bug #16311231: Incorrect results were returned if a query contained a subquery in an IN clause that contained an XOR operation in the WHERE clause. |
| Aurora MySQL database engine updates 2019-09-19 (version 1.19.5) (p. 945) | 1.19.5  | • CVE-2018-2696  
• CVE-2015-4737  
• Bug #19929406: HANDLE_FATAL_SIGNAL (SIG=11) IN __MEMMOVE_SSSE3_BACK FROM STRING::COPY  
• Bug #17059925: For UNION statements, the rows-examined value was calculated incorrectly. This was manifest as too-large values for the ROWS_examined column of Performance Schema statement tables (such as events_statements_current).  
• Bug #11827369: Some queries with SELECT ... FROM DUAL nested subqueries raised an assertion.  
• Bug #16311231: Incorrect results were returned if a query contained a subquery in an IN clause which contained an XOR operation in the WHERE clause. |
| Aurora MySQL database engine updates 2019-02-07 (version 1.19.0) (p. 947) | 1.19.0  | • BUG #32917: DETECT ORPHAN TEMP-POOL FILES, AND HANDLE GRACEFULLY  
• BUG #63144 CREATE TABLE IF NOT EXISTS METADATA LOCK IS TOO RESTRICTIVE |
| Aurora MySQL database engine updates 2019-01-17 (p. 949) | 1.17.8  | • BUG #13418638: CREATE TABLE IF NOT EXISTS METADATA LOCK IS TOO RESTRICTIVE |
| Aurora MySQL database engine updates 2018-10-08 (p. 950) | 1.17.7  | • Drop index on a foreign key column leads to missing table. (Bug #16208542)  
• Memory leak in add_derived_key(). (Bug #76349)  
• For partitioned tables, queries could return different results depending on whether Index Merge was used. (Bug #16862316)  
• Queries using the index_merge optimization (see Index merge optimization) could return invalid results when run against tables that were partitioned by HASH. (Bug #17588348) |
| Aurora MySQL database engine updates 2018-09-06 (p. 951) | 1.17.6  | • For an ALTER TABLE statement that renamed or changed the default value of a BINARY column, the alteration was done using a table copy and not in place. (Bug #67141, Bug #14735373, Bug #69580, Bug #17024290)  
• An outer join between a regular table and a derived table that is implicitly groups could cause a server exit. (Bug #16177639) |
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates 2018-03-13 (p. 954) | 1.17.0 | - LAST_INSERT_ID is replicated incorrectly if replication filters are used (Bug #69861)
- Query returns different results depending on whether INDEX_MERGE setting (Bug #16862316)
- Query proc re-execute of stored routine, inefficient query plan (Bug #16346367)
- InnoDB FTS : Assert in FTS_CACHE_APPEND_DELETED_DOC_IDS (Bug #18079671)
- Assert RBT_EMPTY(INDEX_CACHE->WORDS) in ALTER TABLE CHANGE COLUMN (Bug #17536995)
- InnoDB fulltext search doesn't find records when savepoints are involved (Bug #70333, Bug #17458835) |
| Aurora MySQL database engine updates 2017-11-20 (p. 956) | 1.15.1 | - Reverted — MySQL instance stalling "doing SYNC index" (Bug #73816)
- Reverted — Assert RBT_EMPTY(INDEX_CACHE->WORDS) in ALTER TABLE CHANGE COLUMN (Bug #17536995)
- Reverted — InnoDB Fulltext search doesn't find records when savepoints are involved (Bug #70333) |
| Aurora MySQL database engine updates 2017-10-24 (p. 957) | 1.15.0 | - CREATE USER accepts plugin and password hash, but ignores the password hash (Bug #78033)
- The partitioning engine adds fields to the read bit set to be able to return entries sorted from a partitioned index. This leads to the join buffer will try to read unneeded fields. Fixed by not adding all partitioning fields to the read_set, but instead only sort on the already set prefix fields in the read_set. Added a DBUG_ASSERT that if doing key_cmp, at least the first field must be read (Bug #16367691).
- MySQL instance stalling "doing SYNC index" (Bug #73816)
- Assert RBT_EMPTY(INDEX_CACHE->WORDS) in ALTER TABLE CHANGE COLUMN (Bug #17536995)
- InnoDB Fulltext search doesn't find records when savepoints are involved (Bug #70333) |
| Aurora MySQL database engine updates: 2018-03-13 (p. 959) | 1.14.4 | - Ignorable events don't work and are not tested (Bug #74683)
- NEW->OLD ASSERT FAILURE ‘GTID_MODE > 0’ (Bug #20436436) |
<p>| Aurora MySQL database engine updates: 2017-08-07 (p. 960) | 1.14.0 | A full-text search combined with derived tables (subqueries in the FROM clause) caused a server exit. Now, if a full-text operation depends on a derived table, the server produces an error indicating that a full-text search cannot be done on a materialized table. (Bug #68751, Bug #16539903) |</p>
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates: 2017-05-15 (p. 961) | 1.13.0 | • Reloading a table that was evicted while empty caused an AUTO_INCREMENT value to be reset. (Bug #21454472, Bug #77743)  
• An index record was not found on rollback due to inconsistencies in the purge_node_t structure. The inconsistency resulted in warnings and error messages such as "error in sec index entry update", "unable to purge a record", and "tried to purge sec index entry not marked for deletion". (Bug #19138298, Bug #70214, Bug #21126772, Bug #21065746)  
• Wrong stack size calculation for qsort operation leads to stack overflow. (Bug #73979)  
• Record not found in an index upon rollback. (Bug #70214, Bug #72419)  
• ALTER TABLE add column TIMESTAMP on update CURRENT_TIMESTAMP inserts ZERO-datas (Bug #17392) |
| Aurora MySQL database engine updates: 2017-04-05 (p. 962) | 1.12.0 | • Reloading a table that was evicted while empty caused an AUTO_INCREMENT value to be reset. (Bug #21454472, Bug #77743)  
• An index record was not found on rollback due to inconsistencies in the purge_node_t structure. The inconsistency resulted in warnings and error messages such as "error in sec index entry update", "unable to purge a record", and "tried to purge sec index entry not marked for deletion". (Bug #19138298, Bug #70214, Bug #21126772, Bug #21065746)  
• Wrong stack size calculation for qsort operation leads to stack overflow. (Bug #73979)  
• Record not found in an index upon rollback. (Bug #70214, Bug #72419)  
• ALTER TABLE add column TIMESTAMP on update CURRENT_TIMESTAMP inserts ZERO-datas (Bug #17392) |
| Aurora MySQL database engine updates: 2017-02-23 (p. 964) | 1.11.0 | • Running ALTER table DROP foreign key simultaneously with another DROP operation causes the table to disappear. (Bug #16095573)  
• Some INFORMATION_SCHEMA queries that used ORDER BY did not use a filesort optimization as they did previously. (Bug #16423536)  
• FOUND_ROWS () returns the wrong count of rows on a table. (Bug #68458)  
• The server fails instead of giving an error when too many temp tables are open. (Bug #18948649) |
| Aurora MySQL database engine updates: 2016-12-14 (p. 966) | 1.10.0 | • UNION of derived tables returns wrong results with '1=0/false'-clauses. (Bug #69471)  
• Server crashes in ITEM_FUNC_GROUP_CONCAT::FIX_FIELDS on 2nd execution of stored procedure. (Bug #20755389)  
• Avoid MySQL queries from stalling for too long during FTS cache sync to disk by offloading the cache sync task to a separate thread, as soon as the cache size crosses 10% of the total size. (Bugs #22516559, #73816) |
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aurora MySQL database engine updates: 2016-10-26 (p. 968)</td>
<td>1.8.1</td>
<td>• OpenSSL changed the Diffie-Hellman key length parameters due to the LogJam issue. (Bug #18367167)</td>
</tr>
</tbody>
</table>
| Aurora MySQL database engine updates: 2016-10-18 (p. 968) | 1.8.0 | • When dropping all indexes on a column with multiple indexes, InnoDB failed to block a DROP INDEX operation when a foreign key constraint requires an index. (Bug #16896810)  
• Solve add foreign key constraint crash. (Bug #16413976)  
• Fixed a crash when fetching a cursor in a stored procedure, and analyzing or flushing the table at the same time. (Bug #18158639)  
• Fixed an auto-increment bug when a user alters a table to change the AUTO_INCREMENT value to less than the maximum auto-increment column value. (Bug #16310273) |
| Aurora MySQL database engine updates: 2016-08-30 (p. 970) | 1.7.0 | • Improve scalability by partitioning LOCK_grant lock. (Port WL #8355)  
• Opening cursor on SELECT in stored procedure causes segfault. (Port Bug #16499751)  
• MySQL gives the wrong result with some special usage. (Bug #11751794)  
• Crash in GET_SEL_ARG_FOR_KEYPART – caused by patch for bug #11751794. (Bug #16208709)  
• Wrong results for a simple query with GROUP BY. (Bug #17909656)  
• Extra rows on semijoin query with range predicates. (Bug #16221623)  
• Adding an ORDER BY clause following an IN subquery could cause duplicate rows to be returned. (Bug #16308085)  
• Crash with explain for a query with loose scan for GROUP BY, MyISAM. (Bug #16222245)  
• Loose index scan with quoted int predicate returns random data. (Bug #16394084)  
• If the optimizer was using a loose index scan, the server could exit while attempting to create a temporary table. (Bug #16436567)  
• COUNT(DISTINCT) should not count NULL values, but they were counted when the optimizer used loose index scan. (Bug #17222452)  
• If a query had both MIN()/MAX() and aggregate_function(DISTINCT) (for example, SUM(DISTINCT)) and was executed using loose index scan, the result values of MIN()/MAX() were set improperly. (Bug #17217128) |
<p>| Aurora MySQL database engine updates: 2016-06-01 (p. 971) | 1.6.5 | • SLAVE CAN'T CONTINUE REPLICATION AFTER MASTER'S CRASH RECOVERY (Port Bug #17632285) |</p>
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates: 2016-04-06 (p. 971) | 1.6.0 | • BACKPORT Bug #18694052 FIX FOR ASSERTION `!M_ORDERED_REC_BUFFER' FAILED TO 5.6 (Port Bug #18305270)  
• SEGV IN MEMCPY(), HA_PARTITION::POSITION (Port Bug #18383840)  
• WRONG RESULTS WITH PARTITIONING,INDEX_MERGE AND NO PK (Port Bug #18167648)  
• FLUSH TABLES FOR EXPORT: ASSERTION IN HA_PARTITION::EXTRA (Port Bug #16943907)  
• SERVER CRASH IN VIRTUAL HA_ROWS HANDLER::MULTI_RANGE_READ_INFO_CONST (Port Bug #16164031)  
• RANGE OPTIMIZER CRASHES IN SEL_ARG::RB_INSERT() (Port Bug #16241773) |
| Aurora MySQL database engine updates: 2016-01-11 (p. 973) | 1.5.0 | • Addressed incomplete fix in MySQL full text search affecting tables where the database name begins with a digit. (Port Bug #17607956) |
| Aurora MySQL database engine updates: 2015-12-03 (p. 973) | 1.4 | • SEGV in FTSPARSE(). (Bug #16446108)  
• InnoDB data dictionary is not updated while renaming the column. (Bug #19465984)  
• FTS crash after renaming table to different database. (Bug #168349860)  
• Failed preparing of trigger on truncated tables cause error 1054. (Bug #18596756)  
• Metadata changes might cause problems with trigger execution. (Bug #18684393)  
• Materialization is not chosen for long UTF8 VARCHAR field. (Bug #17566396)  
• Poor execution plan when ORDER BY with limit X. (Bug #16697792)  
• Backport bug #11765744 TO 5.1, 5.5 AND 5.6. (Bug #17083851)  
• Mutex issue in SQL/SQL_SHOW.CC resulting in SIG6. Source likely FILL_VARIABLES. (Bug #20788853)  
• Backport bug #18008907 to 5.5+ versions. (Bug #18903155)  
• Adapt fix for a stack overflow error in MySQL 5.7. (Bug #19678930) |
### Aurora MySQL database engine updates: 2015-10-16 (p. 975)

<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| **Aurora MySQL**       | 1.2, 1.3| • Killing a query inside innodb causes it to eventually crash with an assertion. (Bug #1608883)  
• For failure to create a new thread for the event scheduler, event execution, or new connection, no message was written to the error log. (Bug #16865959)  
• If one connection changed its default database and simultaneously another connection executed SHOW PROCESSLIST, the second connection could access invalid memory when attempting to display the first connection's default database memory. (Bug #11765252)  
• PURGE BINARY LOGS by design does not remove binary log files that are in use or active, but did not provide any notice when this occurred. (Bug #13727933)  
• For some statements, memory leaks could result when the optimizer removed unneeded subquery clauses. (Bug #15875919)  
• During shutdown, the server could attempt to lock an uninitialized mutex. (Bug #16016493)  
• A prepared statement that used GROUP_CONCAT() and an ORDER BY clause that named multiple columns could cause the server to exit. (Bug #16075310)  
• Performance Schema instrumentation was missing for replica worker threads. (Bug #16083949)  
• **STOP SLAVE** could cause a deadlock when issued concurrently with a statement such as SHOW STATUS that retrieved the values for one or more of the status variables Slave_retried_transactions, Slave_heartbeat_period, Slave_received_heartbeats, Slave_last_heartbeat, or Slave_running. (Bug #16088188)  
• A full-text query using Boolean mode could return zero results in some cases where the search term was a quoted phrase. (Bug #16206253)  
• The optimizer's attempt to remove redundant subquery clauses raised an assertion when executing a prepared statement with a subquery in the ON clause of a join in a subquery. (Bug #16318585)  
• GROUP_CONCAT unstable, crash in ITEM_SUM::CLEAN_UP_AFTER_REMOVAL. (Bug #16347450)  
• Attempting to replace the default InnoDB full-text search (FTS) stopword list by creating an InnoDB table with the same structure as INFORMATION_SCHEMA.INNODB_FT_DEFAULT_STOPWORD would result in an error. (Bug #16373868)  
• After the client thread on a worker performed a FLUSH TABLES WITH READ LOCK and was followed by some updates on the master, the worker hung when executing SHOW SLAVE STATUS. (Bug #16387720)  
• When parsing a delimited search string such as "abc-def" in a full-text search, InnoDB now uses the same word delimiters as MyISAM. (Bug #16419661)  
• Crash in FTS_AST_TERM_SET_WILDCARD. (Bug #16429306) |
<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• SEGFAULT in FTS_AST_VISIT() for FTS RQG test. (Bug #16435855)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For debug builds, when the optimizer removed an Item_ref pointing to a subquery, it caused a server exit. (Bug #16509874)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Full-text search on InnoDB tables failed on searches for literal phrases combined with + or - operators. (Bug #16516193)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• START SLAVE failed when the server was started with the options --master-info-repository=TABLE relay-log-info-repository=TABLE and with autocommit set to 0, together with --skip-slave-start. (Bug #16533802)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Very large InnoDB full-text search (FTS) results could consume an excessive amount of memory. (Bug #16625973)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In debug builds, an assertion could occur in OPT_CHECK_ORDER_BY when using binary directly in a search string, as binary might include NULL bytes and other non-meaningful characters. (Bug #16766016)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For some statements, memory leaks could result when the optimizer removed unneeded subquery clauses. (Bug #16807641)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• It was possible to cause a deadlock after issuing FLUSH TABLES WITH READ LOCK by issuing STOP SLAVE in a new connection to the worker, then issuing SHOW SLAVE STATUS using the original connection. (Bug #16856735)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• GROUP_CONCAT() with an invalid separator could cause a server exit. (Bug #16870783)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The server did excessive locking on the LOCK_active_mi and active_mi-&gt;rli-&gt;data_lock mutexes for any SHOW STATUS LIKE 'pattern' statement, even when the pattern did not match status variables that use those mutexes (Slave_heartbeat_period, Slave_last_heartbeat, Slave_received_heartbeats, Slave_retried_transactions, Slave_running). (Bug #16904035)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A full-text search using the IN BOOLEAN MODE modifier would result in an assertion failure. (Bug #16927092)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Full-text search on InnoDB tables failed on searches that used the + boolean operator. (Bug #17280122)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4-way deadlock: zombies, purging binlogs, show processlist, show binlogs. (Bug #17283409)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When an SQL thread which was waiting for a commit lock was killed and restarted it caused a transaction to be skipped on worker. (Bug #17450876)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• An InnoDB full-text search failure would occur due to an &quot;unended&quot; token. The string and string length should be passed for string comparison. (Bug #17659310)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Large numbers of partitioned InnoDB tables could consume much more memory when used in MySQL 5.6 or 5.7 than the memory used by the same tables used in previous releases of the MySQL Server. (Bug #17780517)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For full-text queries, a failure to check that num_token is less than max_proximity_item could result in an assertion. (Bug #18233051)</td>
</tr>
</tbody>
</table>
## Security vulnerabilities fixed in Amazon Aurora MySQL

CVE (Common Vulnerabilities and Exposures) is a list of entries for publicly known cybersecurity vulnerabilities. Each entry contains an identification number, a description, and at least one public reference.

You can find on this page a list of security vulnerabilities fixed in Aurora MySQL. For general information about security for Aurora, see Security in Amazon Aurora (p. 1205). For additional security information for Amazon Aurora MySQL, see Security with Amazon Aurora MySQL (p. 637).

We recommend that you always upgrade to the latest Aurora release to be protected against known vulnerabilities. You can use this page to verify whether a particular version of Aurora MySQL has a fix for a specific security vulnerability. If your cluster doesn't have the security fix, you can see which Aurora MySQL version you should upgrade to for that fix.

Any CVEs fixed in a specific Aurora MySQL version are also listed in the release notes for that version:

- Database engine updates for Amazon Aurora MySQL 2.0 (p. 881)
- Database engine updates for Amazon Aurora MySQL 1.1 (p. 930)

### CVEs and minimum fixed Aurora MySQL versions

- CVE-2020-14567: 2.09.1, 2.08.3, 2.07.3

<table>
<thead>
<tr>
<th>Database engine update</th>
<th>Version</th>
<th>MySQL bugs fixed</th>
</tr>
</thead>
</table>
| Aurora MySQL database engine updates: 2015-08-24 (p. 977) | 1.1 | • InnoDB databases with names beginning with a digit cause a full-text search (FTS) parser error. (Bug #17607956)  
• InnoDB full-text searches fail in databases whose names began with a digit. (Bug #17161372)  
• For InnoDB databases on Windows, the full-text search (FTS) object ID is not in the expected hexadecimal format. (Bug #16559254)  
• A code regression introduced in MySQL 5.6 negatively impacted DROP TABLE and ALTER TABLE performance. This could cause a performance drop between MySQL Server 5.5.x and 5.6.x. (Bug #16864741)  

• CVE-2020-14559: 2.09.1, 2.08.3, 2.07.3, 1.23.1, 1.22.3
• CVE-2020-14553: 2.09.1, 2.08.3, 2.07.3
• CVE-2020-14547: 2.09.1, 2.08.3, 2.07.3
• CVE-2020-14540: 2.09.1, 2.08.3, 2.07.3
• CVE-2020-14539: 1.23.1, 1.22.3
• CVE-2020-2812: 2.09.1, 2.08.3, 2.07.3, 1.22.3
• CVE-2020-2806: 2.09.1, 2.08.3, 2.07.3
• CVE-2020-2780: 2.09.1, 2.08.3, 2.07.3, 1.22.3
• CVE-2020-2765: 2.09.1, 2.08.3, 2.07.3
• CVE-2020-2763: 2.09.1, 2.08.3, 2.07.3, 1.22.3
• CVE-2020-2760: 2.09.1, 2.08.3, 2.07.3, 2.04.9
• CVE-2019-2740: 2.07.3
• CVE-2020-2579: 2.09.1, 2.08.3, 2.07.3, 1.22.3
• CVE-2019-5443: 2.08.0, 2.04.9
• CVE-2019-3822: 2.08.0, 2.04.9
• CVE-2019-2948: 2.09.0
• CVE-2019-2924: 2.07.0, 2.04.9, 1.22.0
• CVE-2019-2923: 2.07.0, 2.04.9, 1.22.0
• CVE-2019-2922: 2.07.0, 2.04.9, 1.22.0
• CVE-2019-2911: 2.09.0, 2.04.9, 1.23.0
• CVE-2019-2910: 2.07.0, 2.04.9, 1.22.0
• CVE-2019-2805: 2.06.0, 2.04.9, 1.22.0
• CVE-2019-2778: 2.06.0, 2.04.9
• CVE-2019-2758: 2.06.0, 2.04.9
• CVE-2019-2740: 2.04.9, 1.22.0
• CVE-2019-2739: 2.06.0, 2.04.9
• CVE-2019-2731: 2.09.0
• CVE-2019-2730: 2.06.0, 2.04.9, 1.22.0
• CVE-2019-2628: 2.04.9
• CVE-2019-2581: 2.09.0
• CVE-2019-2537: 2.09.0, 1.23.0
• CVE-2019-2534: 2.05.0, 2.04.3 (p. 913), 1.21.0, 1.20.0, 1.19.1
• CVE-2019-2482: 2.09.0
• CVE-2019-2434: 2.09.0
• CVE-2019-2420: 2.09.0
• CVE-2018-3284: 2.09.0
• CVE-2018-3155: 2.05.0, 2.04.3 (p. 913)
• CVE-2018-3065: 2.09.0
• CVE-2018-3064: 2.06.0, 2.04.9, 1.22.0
• CVE-2018-3058: 2.06.0, 2.04.9, 1.22.0
• CVE-2018-3056: 2.05.0, 2.04.4 (p. 912)
• CVE-2018-2813: 2.04.9
• CVE-2018-2787: 2.09.0, 1.23.0
• CVE-2018-2786: 2.06.0, 2.04.9
• CVE-2018-2784: 2.09.0, 1.23.0
• CVE-2018-2696: 2.05.0, 2.04.5 (p. 910), 1.21.0, 1.20.0, 1.19.5
• CVE-2018-2645: 2.09.0, 1.23.0
• CVE-2018-2640: 2.09.0, 1.23.0
• CVE-2018-2612: 2.05.0, 2.04.3 (p. 913), 1.21.0, 1.20.0, 1.19.1
• CVE-2018-2562: 2.05.0, 2.04.4 (p. 912), 1.21.0, 1.20.0, 1.19.2
• CVE-2018-0734: 2.05.0, 2.04.3 (p. 913), 1.21.0, 1.20.0, 1.19.1
• CVE-2017-3653: 2.06.0, 2.04.9, 1.22.0
• CVE-2017-3599: 2.05.0, 2.04.3 (p. 913), 1.21.0, 1.20.0, 1.19.1
• CVE-2017-3465: 2.06.0, 2.04.9
• CVE-2017-3464: 1.22.0, 2.04.9
• CVE-2017-3455: 2.06.0, 2.04.9
• CVE-2017-3329: 2.05.0, 2.04.4 (p. 912), 1.21.0, 1.20.0, 1.19.2
• CVE-2017-3244: 2.06.0, 2.04.9, 1.22.0
• CVE-2016-5612: 2.06.0, 2.04.9, 1.22.0
• CVE-2016-5439: 1.22.0
• CVE-2016-0606: 1.22.0
• CVE-2015-4904: 1.22.0
• CVE-2015-4879: 1.22.0
• CVE-2015-4864: 1.22.0
• CVE-2015-4830: 1.22.0
• CVE-2015-4826: 1.22.0
• CVE-2015-4737: 1.21.0, 1.20.0, 1.19.5
• CVE-2015-2620: 1.22.0
• CVE-2015-0382: 1.22.0
• CVE-2015-0381: 1.22.0
• CVE-2014-6555: 1.22.0
• CVE-2014-6489: 1.22.0
• CVE-2014-4260: 1.22.0
• CVE-2014-4258: 1.22.0
• CVE-2014-4244: 1.22.0
• CVE-2014-2436: 1.22.0
• CVE-2014-0393: 1.22.0
• CVE-2013-5908: 1.22.0
• CVE-2013-5881: 1.22.0
• CVE-2013-5807: 1.22.0
• CVE-2013-3811: 1.22.0
• CVE-2013-3807: 1.22.0
• CVE-2013-3806: 1.22.0
• CVE-2013-3804: 1.22.0
• CVE-2013-2381: 1.22.0
• CVE-2013-2378: 1.22.0
• CVE-2013-2375: 1.22.0
• CVE-2013-1523: 1.22.0
• CVE-2012-5615: 1.22.0
Working with Amazon Aurora PostgreSQL

Amazon Aurora PostgreSQL is a fully managed, PostgreSQL-compatible, and ACID-compliant relational database engine that combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. Aurora PostgreSQL is a drop-in replacement for PostgreSQL and makes it simple and cost-effective to set up, operate, and scale your new and existing PostgreSQL deployments, thus freeing you to focus on your business and applications. Amazon RDS provides administration for Aurora by handling routine database tasks such as provisioning, patching, backup, recovery, failure detection, and repair. Amazon RDS also provides push-button migration tools to convert your existing Amazon RDS for PostgreSQL applications to Aurora PostgreSQL.

Aurora PostgreSQL can work with many industry standards. For example, you can use Aurora PostgreSQL databases to build HIPAA-compliant applications and to store healthcare related information, including protected health information (PHI), under a completed Business Associate Agreement (BAA) with AWS. Aurora PostgreSQL is FedRAMP HIGH eligible. For details about AWS and compliance efforts, see AWS services in scope by compliance program.

Topics
- Security with Amazon Aurora PostgreSQL (p. 997)
- Updating applications to connect to Aurora PostgreSQL DB clusters using new SSL/TLS certificates (p. 1001)
- Migrating data to Amazon Aurora with PostgreSQL compatibility (p. 1005)
- Managing Amazon Aurora PostgreSQL (p. 1028)
- Replication with Amazon Aurora PostgreSQL (p. 1034)
- Integrating Amazon Aurora PostgreSQL with other AWS services (p. 1040)
- Exporting data from an Aurora PostgreSQL DB cluster to Amazon S3 (p. 1040)
- Managing query execution plans for Aurora PostgreSQL (p. 1049)
- Publishing Aurora PostgreSQL logs to Amazon CloudWatch Logs (p. 1075)
- Using machine learning (ML) with Aurora PostgreSQL (p. 1079)
- Fast recovery after failover with cluster cache management for Aurora PostgreSQL (p. 1097)
- Invoking an AWS Lambda function from an Aurora PostgreSQL DB cluster (p. 1101)
- Upgrading the PostgreSQL DB engine for Aurora PostgreSQL (p. 1109)
- Best practices with Amazon Aurora PostgreSQL (p. 1116)
- Using Kerberos authentication with Aurora PostgreSQL (p. 1124)
- Amazon Aurora PostgreSQL reference (p. 1137)
- Database engine updates for Amazon Aurora PostgreSQL (p. 1147)

Security with Amazon Aurora PostgreSQL

Security for Amazon Aurora PostgreSQL is managed at three levels:
To control who can perform Amazon RDS management actions on Aurora PostgreSQL DB clusters and DB instances, you use AWS Identity and Access Management (IAM). When you connect to AWS using IAM credentials, your AWS account must have IAM policies that grant the permissions required to perform Amazon RDS management operations. For more information, see Identity and access management in Amazon Aurora (p. 1222).

If you are using IAM to access the Amazon RDS console, you must first sign on to the AWS Management Console with your IAM user credentials. Then go to the Amazon RDS console at https://console.aws.amazon.com/rds/.

Aurora DB clusters must be created in an Amazon Virtual Private Cloud (VPC). To control which devices and Amazon EC2 instances can open connections to the endpoint and port of the DB instance for Aurora DB clusters in a VPC, you use a VPC security group. These endpoint and port connections can be made using Secure Sockets Layer (SSL). In addition, firewall rules at your company can control whether devices running at your company can open connections to a DB instance. For more information on VPCs, see Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281).

Aurora PostgreSQL supports db.r4 and db.t3 instance classes with default VPC only. With default VPC tenancy, the VPC runs on shared hardware. With dedicated VPC tenancy, the VPC runs on a dedicated hardware instance. For more information about instance classes, see DB instance classes (p. 46). For more information about default and dedicated VPC tenancy, see Dedicated instances in the Amazon EC2 User Guide for Linux Instances.

To authenticate login and permissions for an Amazon Aurora DB cluster, you can take the same approach as with a stand-alone instance of PostgreSQL.

Commands such as CREATE ROLE, ALTER ROLE, GRANT, and REVOKE work just as they do in on-premises databases, as does directly modifying database schema tables. For more information, see Client authentication in the PostgreSQL documentation.

Note
The Salted Challenge Response Authentication Mechanism (SCRAM) is not supported with Aurora PostgreSQL.

When you create an Amazon Aurora PostgreSQL DB instance, the master user has the following default privileges:

- LOGIN
- NOSUPERUSER
- INHERIT
- CREATEDB
- CREATEROLE
- NOREPLICATION
- VALID UNTIL 'infinity'

To provide management services for each DB cluster, the rdsadmin user is created when the DB cluster is created. Attempting to drop, rename, change the password, or change privileges for the rdsadmin account will result in an error.

Restricting password management

You can restrict who can manage database user passwords to a special role. By doing this, you can have more control over password management on the client side.

You enable restricted password management with the static parameter rds.restrict_password_commands and use a role called rds_password. When the parameter rds.restrict_password_commands is set to 1, only users that are members of the rds_password role can perform password changes or other related tasks.
role can run certain SQL commands. The restricted SQL commands are commands that modify database
user passwords and password expiration time.

To use restricted password management, your DB cluster must be running Amazon Aurora for
PostgreSQL 10.6 or higher. Because the `rds.restrict_password_commands` parameter is static,
changing this parameter requires a database restart.

When a database has restricted password management enabled, if you try to run restricted SQL
commands you get the following error: ERROR: must be a member of rds_password to alter passwords.

Following are some examples of SQL commands that are restricted when restricted password
management is enabled.

```sql
postgres=> CREATE ROLE myrole WITH PASSWORD 'mypassword';
postgres=> CREATE ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2020-01-01';
postgres=> ALTER ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2020-01-01';
postgres=> ALTER ROLE myrole WITH PASSWORD 'mypassword';
postgres=> ALTER ROLE myrole VALID UNTIL '2020-01-01';
postgres=> ALTER ROLE myrole RENAME TO myrole2;
```

Some `ALTER ROLE` commands that include `RENAME TO` might also be restricted. They might be
restricted because renaming a PostgreSQL role that has an MD5 password clears the password.

The `rds_superuser` role has membership for the `rds_password` role by default, and you can't
change this. You can give other roles membership for the `rds_password` role by using the `GRANT` SQL
command. We recommend that you give membership to `rds_password` to only a few roles that you use
solely for password management. These roles require the `CREATEROLE` attribute to modify other roles.

Make sure that you verify password requirements such as expiration and needed complexity on the
client side. We recommend that you restrict password-related changes by using your own client-side
utility. This utility should have a role that is a member of `rds_password` and has the `CREATEROLE` role
attribute.

### Securing Aurora PostgreSQL data with SSL

Amazon RDS supports Secure Socket Layer (SSL) encryption for Aurora PostgreSQL DB clusters. Using
SSL, you can encrypt a connection between your applications and your Aurora PostgreSQL DB clusters.
You can also force all connections to your Aurora PostgreSQL DB cluster to use SSL.

For general information about SSL support and PostgreSQL databases, see SSL support in the
PostgreSQL documentation. For information about using an SSL connection over JDBC, see Configuring
the client in the PostgreSQL documentation.

**Topics**

- [Requiring an SSL connection to an Aurora PostgreSQL DB cluster](#)
- [Determining the SSL connection status](#)

SSL support is available in all AWS Regions for Aurora PostgreSQL. Amazon RDS creates an SSL
certificate for your Aurora PostgreSQL DB cluster when the DB cluster is created. If you enable SSL
certificate verification, then the SSL certificate includes the DB cluster endpoint as the Common Name
(CN) for the SSL certificate to guard against spoofing attacks.

**To connect to an Aurora PostgreSQL DB cluster over SSL**

1. Download the certificate.
   
   For information about downloading certificates, see Using SSL/TLS to encrypt a connection to a DB
   cluster (p. 1211).
2. Import the certificate into your operating system.
3. Connect to your Aurora PostgreSQL DB cluster over SSL.

   When you connect using SSL, your client can choose to verify the certificate chain or not. If your connection parameters specify `sslmode=verify-ca` or `sslmode=verify-full`, then your client requires the RDS CA certificates to be in their trust store or referenced in the connection URL. This requirement is to verify the certificate chain that signs your database certificate.

   When a client, such as psql or JDBC, is configured with SSL support, the client first tries to connect to the database with SSL by default. If the client can't connect with SSL, it reverts to connecting without SSL. The default `sslmode` mode used is different between libpq-based clients (such as psql) and JDBC. The libpq-based clients default to `prefer`, while JDBC clients default to `verify-full`.

   Use the `sslrootcert` parameter to reference the certificate, for example `sslrootcert=rds-ssl-ca-cert.pem`.

   The following is an example of using psql to connect to an Aurora PostgreSQL DB cluster.

   ```bash
   $ 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"
   ```

**Requiring an SSL connection to an Aurora PostgreSQL DB cluster**

You can require that connections to your Aurora PostgreSQL DB cluster use SSL by using the `rds.force_ssl` parameter. By default, the `rds.force_ssl` parameter is set to 0 (off). You can set the `rds.force_ssl` parameter to 1 (on) to require SSL for connections to your DB cluster. Updating the `rds.force_ssl` parameter also sets the PostgreSQL `ssl` parameter to 1 (on) and modifies your DB cluster's `pg_hba.conf` file to support the new SSL configuration.

You can set the `rds.force_ssl` parameter value by updating the DB cluster parameter group for your DB cluster. If the DB cluster parameter group isn't the default one, and the `ssl` parameter is already set to 1 when you set `rds.force_ssl` to 1, you don't need to reboot your DB cluster. Otherwise, you must reboot your DB cluster for the change to take effect. For more information on parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

When the `rds.force_ssl` parameter is set to 1 for a DB cluster, you see output similar to the following when you connect, indicating that SSL is now required:

```bash
# psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser
psql (9.3.12, server 9.4.4)
Some psql features might not work.
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.
postgres=>
```

**Determining the SSL connection status**

The encrypted status of your connection is shown in the logon banner when you connect to the DB cluster.
Updating applications to connect to Aurora PostgreSQL DB clusters using new SSL/TLS certificates

As of September 19, 2019, Amazon RDS has published new Certificate Authority (CA) certificates for connecting to your Aurora DB clusters using Secure Socket Layer or Transport Layer Security (SSL/TLS). Following, you can find information about updating your applications to use the new certificates.

This topic can help you to determine whether any client applications use SSL/TLS to connect to your DB clusters. If they do, you can further check whether those applications require certificate verification to connect.
Determining whether applications are connecting to Aurora PostgreSQL DB clusters using SSL

Note
Some applications are configured to connect to Aurora PostgreSQL DB clusters only if they can successfully verify the certificate on the server. For such applications, you must update your client application trust stores to include the new CA certificates.

After you update your CA certificates in the client application trust stores, you can rotate the certificates on your DB clusters. We strongly recommend testing these procedures in a development or staging environment before implementing them in your production environments.

For more information about certificate rotation, see Rotating your SSL/TLS certificate (p. 1213). For more information about downloading certificates, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211). For information about using SSL/TLS with PostgreSQL DB clusters, see Securing Aurora PostgreSQL data with SSL (p. 999).

Topics
- Determining whether applications are connecting to Aurora PostgreSQL DB clusters using SSL (p. 1002)
- Determining whether a client requires certificate verification in order to connect (p. 1003)
- Updating your application trust store (p. 1003)
- Using SSL/TLS connections for different types of applications (p. 1004)

Determining whether applications are connecting to Aurora PostgreSQL DB clusters using SSL

Check the DB cluster configuration for the value of the `rds.force_ssl` parameter. By default, the `rds.force_ssl` parameter is set to 0 (off). If the `rds.force_ssl` parameter is set to 1 (on), clients are required to use SSL/TLS for connections. For more information about parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

If `rds.force_ssl` isn't set to 1 (on), query the `pg_stat_ssl` view to check connections using SSL. For example, the following query returns only SSL connections and information about the clients using SSL.

```sql
select datname, usename, 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 usename<>'rdsadmin';
```

Only rows using SSL/TLS connections are displayed with information about the connection. The following is sample output.

```
data | usename | ssl | client_addr
-------+---------+-----+------------
benchdb | pgadmin | t   | 53.95.6.13
postgres | pgadmin | t   | 53.95.6.13
(2 rows)
```

The preceding query displays only the current connections at the time of the query. The absence of results doesn't indicate that no applications are using SSL connections. Other SSL connections might be established at a different time.
Determining whether a client requires certificate verification in order to connect

When a client, such as psql or JDBC, is configured with SSL support, the client first tries to connect to the database with SSL by default. If the client can't connect with SSL, it reverts to connecting without SSL. The default sslmode mode used is different between libpq-based clients (such as psql) and JDBC. The libpq-based clients default to prefer, where JDBC clients default to verify-full. The certificate on the server is verified only when sslrootcert is provided with sslmode set to require, verify-ca, or verify-full. An error is thrown if the certificate is invalid.

Use PGSSLMODE to verify the certificate with the PGSSLMODE environment variable, with PGSSLMODE set to require, verify-ca, or verify-full.

```
```

Use the sslrootcert argument to verify the certificate with sslmode in connection string format, with sslmode set to require, verify-ca, or verify-full.

```
psql "host=pgdbidentifier.cxxxxxxxx.us-east-2.rds.amazonaws.com sslmode=require sslrootcert=/fullpath/rds-ca-2019-root.pem user=primaryuser dbname=postgres"
```

For example, in the preceding case, if you use an invalid root certificate, you see an error similar to the following on your client.

```
psql: SSL error: certificate verify failed
```

Updating your application trust store

For information about updating the trust store for PostgreSQL applications, see Secure TCP/IP connections with SSL in the PostgreSQL documentation.

**Note**
When you update the trust store, you can retain older certificates in addition to adding the new certificates.

Updating your application trust store for JDBC

You can update the trust store for applications that use JDBC for SSL/TLS connections.

**To update the trust store for JDBC applications**

1. Download the 2019 root certificate that works for all AWS Regions and put the file in your trust store directory.

   For information about downloading the root certificate, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).
2. Convert the certificate to .der format using the following command.

```bash
```

Replace the file name with the one that you downloaded.

3. Import the certificate into the key store using the following command.

```bash
```

4. Confirm that the key store was updated successfully.

```bash
keytool -list -v -keystore clientkeystore.jks
```

Enter the key store password when you are prompted for it.

Your output should contain the following.

```
  rds-root, date, trustedCertEntry, 
 Certificate fingerprint (SHA1): 
 # This fingerprint should match the output from the below command 
 openssl x509 -fingerprint -in rds-ca-2019-root.pem -noout
```

---

**Using SSL/TLS connections for different types of applications**

The following provides information about using SSL/TLS connections for different types of applications:

- **psql**

  The client is invoked from the command line by specifying options either as a connection string or as environment variables. For SSL/TLS connections, the relevant options are `sslmode` (environment variable `PGSSLMODE`), `sslrootcert` (environment variable `PGSSLROOTCERT`).

  For the complete list of options, see Parameter key words in the PostgreSQL documentation. For the complete list of environment variables, see Environment variables in the PostgreSQL documentation.

- **pgAdmin**

  This browser-based client is a more user-friendly interface for connecting to a PostgreSQL database.

  For information about configuring connections, see the pgAdmin documentation.

- **JDBC**

  JDBC enables database connections with Java applications.
For general information about connecting to a PostgreSQL database with JDBC, see Connecting to the database in the PostgreSQL documentation. For information about connecting with SSL/TLS, see Configuring the client in the PostgreSQL documentation.

- **Python**

  A popular Python library for connecting to PostgreSQL databases is **psycopg2**.

  For information about using **psycopg2**, see the **psycopg2 documentation**. For a short tutorial on how to connect to a PostgreSQL database, see **Psycopg2 tutorial**. You can find information about the options the connect command accepts in The psycopg2 module content.

**Important**

After you have determined that your database connections use SSL/TLS and have updated your application trust store, you can update your database to use the rds-ca-2019 certificates. For instructions, see step 3 in **Updating your CA certificate by modifying your DB instance (p. 1214)**.

---

**Migrating data to Amazon Aurora with PostgreSQL compatibility**

You have several options for migrating data from your existing database to an Amazon Aurora with PostgreSQL compatibility DB cluster. Your migration options also depend on the database that you are migrating from and the size of the data that you are migrating. Following are your options:

**Migrating from an RDS PostgreSQL DB instance**

You can migrate data directly from an Amazon RDS PostgreSQL DB snapshot to an Aurora PostgreSQL DB cluster. For more information, see **Migrating an RDS PostgreSQL DB snapshot to an Aurora PostgreSQL DB cluster (p. 1006)**.

You can also migrate from an RDS PostgreSQL DB instance by creating an Aurora PostgreSQL Read Replica of a PostgreSQL DB instance. When the replica lag between the PostgreSQL DB instance and the Aurora PostgreSQL Read Replica is zero, you can stop replication. At this point, you can make the Aurora Read Replica a standalone Aurora PostgreSQL DB cluster for reading and writing. For more information, see **Migrating data from an RDS PostgreSQL DB instance to an Aurora PostgreSQL DB cluster by using an Aurora read replica (p. 1008)**.

**Migrating from a database that is not PostgreSQL-compatible**

You can use AWS Database Migration Service (AWS DMS) to migrate data from a database that is not PostgreSQL-compatible. For more information on AWS DMS, see **What is AWS Database Migration Service?**

**Importing Amazon S3 data**

You can migrate by importing data from Amazon S3 into a table belonging to an Aurora PostgreSQL DB cluster for an RDS PostgreSQL DB instance. For more information, see **Importing Amazon S3 data into an Aurora PostgreSQL DB cluster (p. 1017)**.

For a list of AWS Regions where Aurora is available, see **Amazon Aurora in the AWS General Reference**.
Migrating an RDS PostgreSQL DB snapshot to an Aurora PostgreSQL DB cluster

To create an Aurora PostgreSQL DB cluster, you can migrate a DB snapshot of an RDS PostgreSQL DB instance. The new Aurora PostgreSQL DB cluster is populated with the data from the original RDS PostgreSQL DB instance. The DB snapshot must be from an RDS DB instance running PostgreSQL 9.6.1 or 9.6.3. For information about creating a DB snapshot, see Creating a DB snapshot.

In some cases, the DB snapshot might not be in the AWS Region where you want to locate your data. If so, use the Amazon RDS console to copy the DB snapshot to that AWS Region. For information about copying a DB snapshot, see Copying a DB snapshot.

When you migrate the DB snapshot by using the console, the console takes the actions necessary to create both the DB cluster and the primary instance.

You can also choose for your new Aurora PostgreSQL DB cluster to be encrypted at rest by using an AWS Key Management Service (AWS KMS) customer master key (CMK). This option is available only for unencrypted DB snapshots.

To migrate a PostgreSQL DB snapshot by using the RDS console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose Snapshots.
3. On the Snapshots page, choose the snapshot that you want to migrate into an Aurora PostgreSQL DB cluster.
4. Choose Migrate Database.
5. Set the following values on the Migrate Database page:
   - **DB Instance Class**: Choose a DB instance class that has the required storage and capacity for your database, for example `db.r3.large`. Aurora cluster volumes automatically grow as the amount of data in your database increases. 128 tebibytes (TiB) So you only need to choose a DB instance class that meets your current storage requirements. For more information, see Overview of Aurora storage (p. 51).
   - **DB Instance Identifier**: Enter a name for the DB cluster that is unique for your account in the AWS Region that you chose. This identifier is used in the endpoint addresses for the instances in your DB cluster. You might choose to add some intelligence to the name, such as including the AWS Region and DB engine that you chose, for example `aurora-cluster1`. The DB instance identifier has the following constraints:
     - It must contain 1–63 alphanumeric characters or hyphens.
     - It can't end with a hyphen or contain two consecutive hyphens.
     - It must be unique for all DB instances per AWS account, per AWS Region.
   - **VPC**: If you have an existing VPC, then you can use that VPC with your Aurora PostgreSQL DB cluster by choosing your VPC identifier, for example `vpc-a464d1c1`. For information on using an existing VPC, see How to create a VPC for use with Amazon Aurora (p. 1281).
     Otherwise, you can choose to have Amazon RDS create a VPC for you by choosing Create a new VPC.
   - **Subnet Group**: If you have an existing subnet group, then you can use that subnet group with your Aurora PostgreSQL DB cluster by choosing your subnet group identifier, for example `gs-subnet-group1`.
Otherwise, you can choose to have Amazon RDS create a subnet group for you by choosing **Create a new subnet group**.

- **Publicly Accessible**: Choose **No** to specify that instances in your DB cluster can only be accessed by resources inside of your VPC. Choose **Yes** to specify that instances in your DB cluster can be accessed by resources on the public network. The default is **Yes**.

  **Note**
  
  Your production DB cluster might not need to be in a public subnet, because only your application servers require access to your DB cluster. If your DB cluster doesn't need to be in a public subnet, set **Publicly Accessible** to **No**.

- **Availability Zone**: Choose the Availability Zone to host the primary instance for your Aurora PostgreSQL DB cluster. To have Amazon RDS choose an Availability Zone for you, choose **No Preference**.

- **Database Port**: Enter the default port to be used when connecting to instances in the Aurora PostgreSQL DB cluster. The default is **5432**.

  **Note**
  
  You might be behind a corporate firewall that doesn't allow access to default ports such as the PostgreSQL default port, 5432. In this case, provide a port value that your corporate firewall allows. Remember that port value later when you connect to the Aurora PostgreSQL DB cluster.

- **Enable Encryption**: Choose **Yes** for your new Aurora PostgreSQL DB cluster to be encrypted at rest. If you choose **Yes**, also choose an AWS KMS customer master key (CMK) as the **Master Key** value.

- **Auto minor version upgrade**: Choose **Enable auto minor version upgrade** to enable your Aurora PostgreSQL DB cluster to receive minor PostgreSQL DB engine version upgrades automatically when they become available.

  The **Auto Minor Version Upgrade** option only applies to upgrades to PostgreSQL minor engine versions for your Aurora PostgreSQL DB cluster. It doesn't apply to regular patches applied to maintain system stability.

6. Choose **Migrate** to migrate your DB snapshot.

7. Choose **Instances**, and then choose the arrow icon to show the DB cluster details and monitor the progress of the migration. On the details page, you can find the cluster endpoint used to connect to the primary instance of the DB cluster. For more information on connecting to an Aurora PostgreSQL DB cluster, see **Connecting to an Amazon Aurora DB cluster (p. 253)**.
Migrating data from an RDS PostgreSQL DB instance to an Aurora PostgreSQL DB cluster by using an Aurora read replica

You can migrate from a PostgreSQL DB instance to an Aurora PostgreSQL DB cluster by using an Aurora Read Replica. When you need to migrate from an RDS PostgreSQL DB instance to an Aurora PostgreSQL DB cluster, we recommend using this approach.

In this case, Amazon RDS uses the PostgreSQL DB engine's streaming replication functionality to create a special type of DB cluster for the source PostgreSQL DB instance. This type of DB cluster is called an Aurora Read Replica. Updates made to the source PostgreSQL DB instance are asynchronously replicated to the Aurora Read Replica.

Topics
- Overview of migrating data by using an Aurora read replica  (p. 1008)
- Preparing to migrate data by using an Aurora read replica  (p. 1009)
- Creating an Aurora read replica (p. 1009)
- Promoting an Aurora read replica (p. 1015)

Overview of migrating data by using an Aurora read replica

To migrate from an RDS PostgreSQL DB instance to an Aurora PostgreSQL DB cluster, we recommend creating an Aurora Read Replica of your source PostgreSQL DB instance. When the replica lag between the PostgreSQL DB instance and the Aurora PostgreSQL Read Replica is zero, you can stop replication. At this point, you can promote the Aurora Read Replica to be a standalone Aurora PostgreSQL DB cluster. This standalone DB cluster can then accept write loads.

Be prepared for migration to take a while, roughly several hours per tebibyte (TiB) of data. While the migration is in progress, your Amazon RDS PostgreSQL instance accumulates write ahead log (WAL) segments. Make sure that your Amazon RDS instance has sufficient storage capacity for these segments.

When you create an Aurora Read Replica of a PostgreSQL DB instance, Amazon RDS creates a DB snapshot of your source PostgreSQL DB instance. This snapshot is private to Amazon RDS and incurs no charges. Amazon RDS then migrates the data from the DB snapshot to the Aurora Read Replica. After the DB snapshot data is migrated to the new Aurora PostgreSQL DB cluster, RDS starts replication between your PostgreSQL DB instance and the Aurora PostgreSQL DB cluster.

You can only have one Aurora Read Replica for a PostgreSQL DB instance. If you try to create an Aurora Read Replica for your Amazon RDS PostgreSQL instance and you already have an Aurora Read Replica or a cross-region Read Replica, the request is rejected.

Note
Replication issues can arise due to feature differences between Aurora PostgreSQL and the PostgreSQL engine version of your RDS PostgreSQL DB instance that is the replication source. You can replicate only from an Amazon RDS PostgreSQL instance that is compatible with the Aurora PostgreSQL version in question. For example, if the supported Aurora PostgreSQL version is 9.6.3, the Amazon RDS PostgreSQL DB instance must be running version 9.6.1 or greater. If you encounter an error, you can find help in the Amazon RDS community forum or by contacting AWS Support.

For more information on PostgreSQL read replicas, see Working with read replicas in the Amazon RDS User Guide.
Preparing to migrate data by using an Aurora read replica

Before you migrate data from your RDS PostgreSQL instance to an Aurora PostgreSQL cluster, make sure that your instance has sufficient storage capacity. This storage capacity is for the write ahead log (WAL) segments that accumulate during the migration. There are several metrics to check for this, described following.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FreeStorageSpace</td>
<td>The available storage space.</td>
</tr>
<tr>
<td></td>
<td>Units: Bytes</td>
</tr>
<tr>
<td>OldestReplicationSlotLag</td>
<td>The size of the lag for WAL data in the replica that is lagging the most.</td>
</tr>
<tr>
<td></td>
<td>Units: Megabytes</td>
</tr>
<tr>
<td>RDSToAuroraPostgreSQLReplicaLag</td>
<td>The amount of time in seconds that an Aurora PostgreSQL DB cluster lags behind the source RDS DB instance.</td>
</tr>
<tr>
<td>TransactionLogsDiskUsage</td>
<td>The disk space used by the transaction logs.</td>
</tr>
<tr>
<td></td>
<td>Units: Megabytes</td>
</tr>
</tbody>
</table>

For more information about monitoring your RDS instance, see Monitoring in the Amazon RDS User Guide.

Creating an Aurora read replica

You can create an Aurora Read Replica for a PostgreSQL DB instance by using the console or the AWS CLI.

Console

To create an Aurora read replica from a source PostgreSQL DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose the PostgreSQL DB instance that you want to use as the source for your Aurora Read Replica, and choose Create Aurora read replica for Actions.
4. Choose the DB cluster specifications that you want to use for the Aurora Read Replica, as described in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB instance class</td>
<td>Choose a DB instance class that defines the processing and memory requirements for the primary instance in the DB cluster. For more information about DB instance class options, see DB instance classes (p. 46).</td>
</tr>
<tr>
<td>Multi-AZ deployment</td>
<td>Not available for PostgreSQL</td>
</tr>
</tbody>
</table>
| DB instance identifier | Enter a name for the primary instance in your Aurora Read Replica DB cluster. This identifier is used in the endpoint address for the primary instance of the new DB cluster. The DB instance identifier has the following constraints:  
  • It must contain 1–63 alphanumeric characters or hyphens.  
  • Its first character must be a letter.  
  • It can't end with a hyphen or contain two consecutive hyphens.  
  • It must be unique for all DB instances for each AWS account, for each AWS Region.  

The Aurora Read Replica DB cluster is created from a snapshot of the source DB instance. Thus, the master user name and master password for the Aurora Read
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>replica</td>
<td>Replica are the same as the master user name and master password for the source DB instance.</td>
</tr>
<tr>
<td>Virtual Private Cloud (VPC)</td>
<td>Choose the VPC to host the DB cluster. Choose <strong>Create new VPC</strong> to have Amazon RDS create a VPC for you. For more information, see DB cluster prerequisites (p. 118).</td>
</tr>
<tr>
<td>Subnet group</td>
<td>Choose the DB subnet group to use for the DB cluster. Choose <strong>Create new DB Subnet Group</strong> to have Amazon RDS create a DB subnet group for you. For more information, see DB cluster prerequisites (p. 118).</td>
</tr>
<tr>
<td>Public accessibility</td>
<td>Choose <strong>Yes</strong> to give the DB cluster a public IP address; otherwise, choose <strong>No</strong>. The instances in your DB cluster can be a mix of both public and private DB instances. For more information about hiding instances from public access, see <strong>Hiding a DB instance in a VPC from the internet</strong> (p. 1293).</td>
</tr>
<tr>
<td>Availability zone</td>
<td>Determine if you want to specify a particular Availability Zone. For more information about Availability Zones, see Regions and Availability Zones (p. 5).</td>
</tr>
<tr>
<td>VPC security groups</td>
<td>Choose one or more VPC security groups to secure network access to the DB cluster. Choose <strong>Create new VPC security group</strong> to have Amazon RDS create a VPC security group for you. For more information, see DB cluster prerequisites (p. 118).</td>
</tr>
<tr>
<td>Database port</td>
<td>Specify the port for applications and utilities to use to access the database. Aurora PostgreSQL DB clusters default to the default PostgreSQL port, 5432. Firewalls at some companies block connections to this port. If your company firewall blocks the default port, choose another port for the new DB cluster.</td>
</tr>
<tr>
<td>DB parameter group</td>
<td>Choose a DB parameter group for the Aurora PostgreSQL DB cluster. Aurora has a default DB parameter group you can use, or you can create your own DB parameter group. For more information about DB parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).</td>
</tr>
<tr>
<td>DB cluster parameter group</td>
<td>Choose a DB cluster parameter group for the Aurora PostgreSQL DB cluster. Aurora has a default DB cluster parameter group you can use, or you can create your own DB cluster parameter group. For more information about DB cluster parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).</td>
</tr>
<tr>
<td>Encryption</td>
<td>Choose <strong>Enable encryption</strong> for your new Aurora DB cluster to be encrypted at rest. If you choose <strong>Enable encryption</strong>, also choose an AWS KMS customer master key (CMK) as the <strong>Master key</strong> value.</td>
</tr>
</tbody>
</table>
### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Choose a failover priority for the DB cluster. If you don’t choose a value, the default is <em>tier-1</em>. This priority determines the order in which Aurora Replicas are promoted when recovering from a primary instance failure. For more information, see [Fault tolerance for an Aurora DB cluster](p. 56).</td>
</tr>
<tr>
<td>Backup retention period</td>
<td>Choose the length of time, 1–35 days, for Aurora to retain backup copies of the database. Backup copies can be used for point-in-time restores (PITR) of your database down to the second.</td>
</tr>
<tr>
<td>Enhanced monitoring</td>
<td>Choose <a href="#">Enable enhanced monitoring</a> to enable gathering metrics in real time for the operating system that your DB cluster runs on. For more information, see [Enhanced Monitoring](p. 504).</td>
</tr>
<tr>
<td>Monitoring Role</td>
<td>Only available if you chose <a href="#">Enable enhanced monitoring</a>. The AWS Identity and Access Management (IAM) role to use for Enhanced Monitoring. For more information, see [Setting up and enabling Enhanced Monitoring](p. 504).</td>
</tr>
<tr>
<td>Granularity</td>
<td>Only available if you chose <a href="#">Enable enhanced monitoring</a>. Set the interval, in seconds, between when metrics are collected for your DB cluster.</td>
</tr>
<tr>
<td>Auto minor version upgrade</td>
<td>Choose <a href="#">Yes</a> to enable your Aurora PostgreSQL DB cluster to receive minor PostgreSQL DB engine version upgrades automatically when they become available.</td>
</tr>
<tr>
<td>Maintenance window</td>
<td>Choose the weekly time range during which system maintenance can occur.</td>
</tr>
</tbody>
</table>

5. Choose Create read replica.

**AWS CLI**

To create an Aurora Read Replica from a source PostgreSQL DB instance, use the `create-db-cluster` and `create-db-instance` AWS CLI commands to create a new Aurora PostgreSQL DB cluster. When you call the `create-db-cluster` command, include the `--replication-source-identifier` parameter to identify the Amazon Resource Name (ARN) for the source PostgreSQL DB instance. For more information about Amazon RDS ARNs, see [Amazon Relational Database Service (Amazon RDS)](Amazon RDS) in the [AWS General Reference](#).

Don't specify the master user name, master password, or database name. The Aurora Read Replica uses the same master user name, master password, and database name as the source PostgreSQL DB instance.

For Linux, macOS, or Unix:

```
aws rds create-db-cluster --db-cluster-identifier sample-replica-cluster --engine aurora-postgresql \
```
Migrating an RDS PostgreSQL DB instance using an Aurora read replica

```
--db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2 \
```

For Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-replica-cluster --engine aurora-postgresql ^
   --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2 ^
```

If you use the console to create an Aurora Read Replica, then RDS automatically creates the primary instance for your DB cluster Aurora Read Replica. If you use the CLI to create an Aurora Read Replica, you must explicitly create the primary instance for your DB cluster. The primary instance is the first instance that is created in a DB cluster.

You can create a primary instance for your DB cluster by using the `create-db-instance` CLI command with the following parameters:

- `--db-cluster-identifier` The name of your DB cluster.
- `--db-instance-class` The name of the DB instance class to use for your primary instance.
- `--db-instance-identifier` The name of your primary instance.
- `--engine aurora-postgresql` The database engine to use.

In the following example, you create a primary instance named `myreadreplicainstance` for the DB cluster named `myreadreplicacluster`. You do this using the DB instance class specified in `myinstanceclass`.

**Example**

For Linux, macOS, or Unix:

```
aws rds create-db-instance \ 
   --db-cluster-identifier myreadreplicacluster \ 
   --db-instance-class myinstanceclass \ 
   --db-instance-identifier myreadreplicainstance \ 
   --engine aurora-postgresql
```

For Windows:

```
aws rds create-db-instance \ 
   --db-cluster-identifier myreadreplicacluster \ 
   --db-instance-class myinstanceclass \ 
   --db-instance-identifier myreadreplicainstance \ 
   --engine aurora-postgresql
```
RDS API

To create an Aurora Read Replica from a source PostgreSQL DB instance, use the RDS API operations `CreateDBCluster` and `CreateDBInstance` to create a new Aurora DB cluster and primary instance. Don't specify the master user name, master password, or database name. The Aurora Read Replica uses the same master user name, master password, and database name as the source PostgreSQL DB instance.

You can create a new Aurora DB cluster for an Aurora Read Replica from a source PostgreSQL DB instance. To do so, use the RDS API operation `CreateDBCluster` with the following parameters:

- **DBClusterIdentifier**
  
  The name of the DB cluster to create.

- **DBSubnetGroupName**
  
  The name of the DB subnet group to associate with this DB cluster.

- **Engine=aurora-postgresql**
  
  The name of the engine to use.

- **ReplicationSourceIdentifier**
  
  The Amazon Resource Name (ARN) for the source PostgreSQL DB instance. For more information about Amazon RDS ARNs, see Amazon Relational Database Service (Amazon RDS) in the Amazon Web Services General Reference.

- **VpcSecurityGroupIds**
  
  The list of Amazon EC2 VPC security groups to associate with this DB cluster.

In the following example, you create a DB cluster named `myreadreplicaccluster` from a source PostgreSQL DB instance. This cluster has an ARN set to `mysqlARN`. The cluster is associated with a DB subnet group named `mysubnetgroup` and a VPC security group named `mysecuritygroup`.

Example

```plaintext
https://rds.us-east-1.amazonaws.com/
?Action=CreateDBCluster
&DBClusterIdentifier=myreadreplicaccluster
&DBSubnetGroupName=mysubnetgroup
&Engine=aurora-postgresql
&ReplicationSourceIdentifier=mysqlARN
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&Version=2014-10-31
&VpcSecurityGroupIds=mysecuritygroup
&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=6a8f4bd6a98f649c75ea0a6b3929ecc75ac09739588391cd7250f5280e716db
```

If you use the console to create an Aurora Read Replica, then Amazon RDS automatically creates the primary instance for your DB cluster Aurora Read Replica. If you use the CLI to create an Aurora Read Replica, you must explicitly create the primary instance for your DB cluster. The primary instance is the first instance that is created in a DB cluster.

You can create a primary instance for your DB cluster by using the RDS API operation `CreateDBInstance` with the following parameters:
Migrating an RDS PostgreSQL DB instance using an Aurora read replica

- **DBClusterIdentifier**
  The name of your DB cluster.
- **DBInstanceClass**
  The name of the DB instance class to use for your primary instance.
- **DBInstanceIdentifier**
  The name of your primary instance.
- **Engine=aurora-postgresql**
  The name of the engine to use.

In this example, you create a primary instance named `myreadreplicainstance` for the DB cluster named `myreadreplicacluster`. You do this using the DB instance class specified in `myinstanceclass`.

Example

```plaintext
https://rds.us-east-1.amazonaws.com/
?Action=CreateDBInstance
&DBClusterIdentifier=myreadreplicacluster
&DBInstanceClass=myinstanceclass
&DBInstanceIdentifier=myreadreplicainstance
&Engine=aurora-postgresql
&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=bee4aabc750bf7dad0cd9e22b952bd6089d91e2a16592c2293e532eeab8bc77
```

Promoting an Aurora read replica

After migration completes, you can promote the Aurora Read Replica to a standalone DB cluster. You then direct your client applications to the endpoint for the Aurora Read Replica. For more information on the Aurora endpoints, see Amazon Aurora connection management (p. 24). Promotion should complete fairly quickly. You can't delete the primary PostgreSQL DB instance or unlink the DB instance and the Aurora Read Replica until the promotion is complete.

Before you promote your Aurora Read Replica, stop any transactions from being written to the source PostgreSQL DB instance. Then wait for the replica lag on the Aurora Read Replica to reach zero.

After you promote your read replica, confirm that the promotion has completed. To do this, choose Instances in the navigation pane and confirm that there is a Promoted Read Replica cluster to standalone database cluster event for your read replica. After promotion is complete, the primary PostgreSQL DB Instance and the Aurora Read Replica are unlinked. At this point, you can safely delete the DB instance if you want to.

**Console**

**To promote an Aurora read replica to an Aurora DB cluster**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Instances**.
3. Choose the DB instance for the Aurora Read Replica and choose **Promote** for **Actions**.
4. Choose **Promote Read Replica**.

**AWS CLI**

To promote an Aurora Read Replica to a stand-alone DB cluster, use the `promote-read-replica-db-cluster` AWS CLI command.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds promote-read-replica-db-cluster
    --db-cluster-identifier myreadreplicacluster
```

For Windows:

```bash
aws rds promote-read-replica-db-cluster
    --db-cluster-identifier myreadreplicacluster
```
Importing Amazon S3 data into an Aurora PostgreSQL DB cluster

You can import data from Amazon S3 into a table belonging to an Aurora PostgreSQL DB cluster. To do this, you use the aws_s3 PostgreSQL extension that Aurora PostgreSQL provides.

**Note**
To import from Amazon S3 into Aurora PostgreSQL, your database must be running PostgreSQL version 10.7 or later.

For more information on storing data with Amazon S3, see Create a bucket in the Amazon Simple Storage Service Getting Started Guide. For instructions on how to upload a file to an Amazon S3 bucket, see Add an object to a bucket in the Amazon Simple Storage Service Getting Started Guide.

**Topics**
- Overview of importing Amazon S3 data (p. 1017)
- Setting up access to an Amazon S3 bucket (p. 1018)
- Using the aws_s3.table_import_from_s3 function to import Amazon S3 data (p. 1023)
- Function reference (p. 1025)

**Overview of importing Amazon S3 data**

To import data stored in an Amazon S3 bucket to a PostgreSQL database table, follow these steps.

**To import S3 data into Aurora PostgreSQL**

1. Install the required PostgreSQL extensions. These include the aws_s3 and aws_commons extensions. To do so, start psql and use the following command.

   ```sql
   psql=> CREATE EXTENSION aws_s3 CASCADE;
   NOTICE: installing required extension "aws_commons"
   ```

   The aws_s3 extension provides the aws_s3.table_import_from_s3 (p. 1025) function that you use to import Amazon S3 data. The aws_commons extension provides additional helper functions.

2. Identify the database table and Amazon S3 file to use.

   The aws_s3.table_import_from_s3 (p. 1025) function requires the name of the PostgreSQL database table that you want to import data into. The function also requires that you identify the Amazon S3 file to import. To provide this information, take the following steps.

   a. Identify the PostgreSQL database table to put the data in. For example, the following is a sample t1 database table used in the examples for this topic.

   ```sql
   psql=> CREATE TABLE t1 (col1 varchar(80), col2 varchar(80), col3 varchar(80));
   ```

   b. Get the following information to identify the Amazon S3 file that you want to import:

   - Bucket name – A bucket is a container for Amazon S3 objects or files.
   - File path – The file path locates the file in the Amazon S3 bucket.
   - AWS Region – The AWS Region is the location of the Amazon S3 bucket. For example, if the S3 bucket is in the US East (N. Virginia) Region, use us-east-1. For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).
To find how to get this information, see View an object in the Amazon Simple Storage Service Getting Started Guide. You can confirm the information by using the AWS CLI command `aws s3 cp`. If the information is correct, this command downloads a copy of the Amazon S3 file.

```
aws s3 cp s3://sample_s3_bucket/sample_file_path ./
```

c. Use the `aws_commons.create_s3_uri` function to create an `aws_commons._s3_uri_1` structure to hold the Amazon S3 file information. You provide this `aws_commons._s3_uri_1` structure as a parameter in the call to the `aws_s3.table_import_from_s3` function.

For a psql example, see the following.

```
psql=> SELECT aws_commons.create_s3_uri('sample_s3_bucket', 'sample.csv', 'us-east-1') AS s3_uri \
       \gset
```

3. Provide permission to access the Amazon S3 file.

To import data from an Amazon S3 file, give the Aurora PostgreSQL DB cluster permission to access the Amazon S3 bucket the file is in. To do this, you use either an AWS Identity and Access Management (IAM) role or security credentials. For more information, see Setting up access to an Amazon S3 bucket (p. 1018).

4. Import the Amazon S3 data by calling the `aws_s3.table_import_from_s3` function.

After you complete the previous preparation tasks, use the `aws_s3.table_import_from_s3` function to import the Amazon S3 data. For more information, see Using the `aws_s3.table_import_from_s3` function to import Amazon S3 data (p. 1023).

**Setting up access to an Amazon S3 bucket**

To import data from an Amazon S3 file, give the Aurora PostgreSQL DB cluster permission to access the Amazon S3 bucket the file is in. You provide access to an Amazon S3 bucket in one of two ways, as described in the following topics.

**Topics**

- Using an IAM role to access an Amazon S3 bucket (p. 1018)
- Using security credentials to access an Amazon S3 bucket (p. 1022)
- Troubleshooting access to Amazon S3 (p. 1022)

**Using an IAM role to access an Amazon S3 bucket**

Before you load data from an Amazon S3 file, give your Aurora PostgreSQL DB cluster permission to access the Amazon S3 bucket the file is in. This way, you don't have to manage additional credential information or provide it in the `aws_s3.table_import_from_s3` function call.

To do this, create an IAM policy that provides access to the Amazon S3 bucket. Create an IAM role and attach the policy to the role. Then assign the IAM role to your DB cluster.

**To give an Aurora PostgreSQL DB cluster access to Amazon S3 through an IAM role**

1. Create an IAM policy.
This policy provides the bucket and object permissions that allow your Aurora PostgreSQL DB cluster to access Amazon S3.

Include in the policy the following required actions to allow the transfer of files from an Amazon S3 bucket to Aurora PostgreSQL:

- s3:GetObject
- s3:ListBucket

Include in the policy the following resources to identify the Amazon S3 bucket and objects in the bucket. This shows the Amazon Resource Name (ARN) format for accessing Amazon S3.

- arn:aws:s3:::your-s3-bucket
- arn:aws:s3:::your-s3-bucket/*

For more information on creating an IAM policy for Aurora PostgreSQL, see Creating and using an IAM policy for IAM database access (p. 1241). See also Tutorial: Create and attach your first customer managed policy in the IAM User Guide.

The following AWS CLI command creates an IAM policy named rds-s3-import-policy with these options. It grants access to a bucket named your-s3-bucket.

**Note**

After you create the policy, note the Amazon Resource Name (ARN) of the policy. You need the ARN for a subsequent step when you attach the policy to an IAM role.

**Example**

For Linux, macOS, or Unix:

```bash
aws iam create-policy \
--policy-name rds-s3-import-policy \n--policy-document '{
 "Version": "2012-10-17",
 "Statement": [
 { 
 "Sid": "s3import",
 "Action": [ 
 "s3:GetObject",
 "s3:ListBucket"
 ],
 "Effect": "Allow",
 "Resource": [
 "arn:aws:s3:::your-s3-bucket",
 "arn:aws:s3:::your-s3-bucket/*"
 ]
 }
 ]
}
```

For Windows:

```bash
aws iam create-policy ^
--policy-name rds-s3-import-policy ^
--policy-document '{
 "Version": "2012-10-17",
 "Statement": [
 
}^)
```

1019
2. Create an IAM role.

You do this so Aurora PostgreSQL can assume this IAM role on your behalf to access your Amazon S3 buckets. For more information, see Creating a role to delegate permissions to an IAM user in the IAM User Guide.

The following example shows using the AWS CLI command to create a role named `rds-s3-import-role`.

**Example**

For Linux, macOS, or Unix:

```bash
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"
        }
    ]
}'
```

For Windows:

```bash
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"
        }
    ]
}'
```

3. Attach the IAM policy that you created to the IAM role that you created.
The following AWS CLI command attaches the policy created earlier to the role named rds-s3-import-role. Replace `your-policy-arn` with the policy ARN that you noted in an earlier step.

**Example**

For Linux, macOS, or Unix:

```bash
aws iam attach-role-policy
--policy-arn your-policy-arn
--role-name rds-s3-import-role
```

For Windows:

```bash
aws iam attach-role-policy
--policy-arn your-policy-arn
--role-name rds-s3-import-role
```

4. Add the IAM role to the DB cluster.

You do so by using the AWS Management Console or AWS CLI, as described following.

**Note**

You can't associate an IAM role with an Aurora Serverless DB cluster. For more information, see [Using Amazon Aurora Serverless v1](p. 134). Also, be sure the database you use doesn't have any restrictions noted in [Importing Amazon S3 data into an Aurora PostgreSQL DB cluster](p. 1017).

**Console**

**To add an IAM role for a PostgreSQL DB cluster using the console**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose the PostgreSQL DB cluster name to display its details.
3. On the Connectivity & security tab, in the Manage IAM roles section, choose the role to add under Add IAM roles to this cluster.
4. Under Feature, choose s3Import.
5. Choose Add role.

**AWS CLI**

**To add an IAM role for a PostgreSQL DB cluster using the CLI**

- Use the following command to add the role to the PostgreSQL DB cluster named my-db-cluster. Replace `your-role-arn` with the role ARN that you noted in a previous step. Use s3Import for the value of the --feature-name option.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds add-role-to-db-cluster
--db-cluster-identifier my-db-cluster
--feature-name s3Import
--role-arn your-role-arn
```
For Windows:

```bash
aws rds add-role-to-db-cluster ^
--db-cluster-identifier my-db-cluster ^
--feature-name s3Import ^
--role-arn your-role-arn ^
--region your-region
```

Using security credentials to access an Amazon S3 bucket

If you prefer, you can use security credentials to provide access to an Amazon S3 bucket instead of providing access with an IAM role. To do this, use the `credentials` parameter in the `aws_s3.table_import_from_s3` function call.

The `credentials` parameter is a structure of type `aws_commons._aws_credentials_1`, which contains AWS credentials. Use the `aws_commons.create_aws_credentials` function to set the access key and secret key in an `aws_commons._aws_credentials_1` structure, as shown following.

```sql
psql=> SELECT aws_commons.create_aws_credentials(  
    'sample_access_key', 'sample_secret_key', ''
) AS creds \gset
```

After creating the `aws_commons._aws_credentials_1` structure, use the `aws_s3.table_import_from_s3` function with the `credentials` parameter to import the data, as shown following.

```sql
psql=> SELECT aws_s3.table_import_from_s3(  
    't', '', '(format csv)',  
    :s3_uri,  
    :creds
);
```

Or you can include the `aws_commons.create_aws_credentials` function call inline within the `aws_s3.table_import_from_s3` function call.

```sql
psql=> SELECT aws_s3.table_import_from_s3(  
    't', '', '(format csv)',  
    :s3_uri,  
    aws_commons.create_aws_credentials('sample_access_key', 'sample_secret_key', '')
);
```

Troubleshooting access to Amazon S3

If you encounter connection problems when attempting to import Amazon S3 file data, see the following for recommendations:

- Troubleshooting Amazon Aurora identity and access (p. 1263)
- Troubleshooting Amazon S3
- Troubleshooting Amazon S3 and IAM
Using the **aws_s3.table_import_from_s3** function to import Amazon S3 data

Import your Amazon S3 data by calling the **aws_s3.table_import_from_s3** (p. 1025) function.

**Note**
The following examples use the IAM role method for providing access to the Amazon S3 bucket. Thus, the **aws_s3.table_import_from_s3** function calls don’t include credential parameters.

The following shows a typical PostgreSQL example using psql.

```
psql=> SELECT aws_s3.table_import_from_s3(
   't1',
   '',
   '({format csv})',
   :'s3_uri'
);
```

The parameters are the following:

- **t1** – The name for the table in the PostgreSQL DB cluster to copy the data into.
- **''** – An optional list of columns in the database table. You can use this parameter to indicate which columns of the S3 data go in which table columns. If no columns are specified, all the columns are copied to the table. For an example of using a column list, see Importing an Amazon S3 file that uses a custom delimiter (p. 1023).
- **{format csv}** – PostgreSQL COPY arguments. The copy process uses the arguments and format of the PostgreSQL COPY command. In the preceding example, the COPY command uses the comma-separated value (CSV) file format to copy the data.
- **s3_uri** – A structure that contains the information identifying the Amazon S3 file. For an example of using the **aws_commons.create_s3_uri** (p. 1027) function to create an s3_uri structure, see Overview of importing Amazon S3 data (p. 1017).

The return value is text. For the full reference of this function, see **aws_s3.table_import_from_s3** (p. 1025).

The following examples show how to specify different kinds of files when importing Amazon S3 data.

**Topics**
- Importing an Amazon S3 file that uses a custom delimiter (p. 1023)
- Importing an Amazon S3 compressed (gzip) file (p. 1024)
- Importing an encoded Amazon S3 file (p. 1024)

**Importing an Amazon S3 file that uses a custom delimiter**

The following example shows how to import a file that uses a custom delimiter. It also shows how to control where to put the data in the database table using the **column_list** parameter of the **aws_s3.table_import_from_s3** (p. 1025) function.

For this example, assume that the following information is organized into pipe-delimited columns in the Amazon S3 file.

```
1|foo1|bar1|elephant1
2|foo2|bar2|elephant2
3|foo3|bar3|elephant3
4|foo4|bar4|elephant4
```
To import a file that uses a custom delimiter

1. Create a table in the database for the imported data.

   ```sql
   psql=> CREATE TABLE test (a text, b text, c text, d text, e text);
   CREATE TABLE
   ```

2. Use the following form of the `aws_s3.table_import_from_s3` (p. 1025) function to import data from the Amazon S3 file.

   You can include the `aws_commons.create_s3_uri` (p. 1027) function call inline within the `aws_s3.table_import_from_s3` function call to specify the file.

   ```sql
   psql=> SELECT aws_s3.table_import_from_s3(
             'test',
             'a,b,d,e',
             'DELIMITER ''|''',
             aws_commons.create_s3_uri('sampleBucket', 'pipeDelimitedSampleFile', 'us-east-2'))
   ```

   The data is now in the table in the following columns.

   ```sql
   psql=> SELECT * FROM test;
   a | b   | c | d     | e
   ------+-----+---+-------+-----
   1    | foo1|   | bar1  | elephant1
   2    | foo2|   | bar2  | elephant2
   3    | foo3|   | bar3  | elephant3
   4    | foo4|   | bar4  | elephant4
   ```

### Importing an Amazon S3 compressed (gzip) file

The following example shows how to import a file from Amazon S3 that is compressed with gzip.

Ensure that the file contains the following Amazon S3 metadata:

- **Key**: Content-Encoding
- **Value**: gzip

For more about adding these values to Amazon S3 metadata, see How do I add metadata to an S3 object? in the Amazon Simple Storage Service Console User Guide.

Import the gzip file into your Aurora PostgreSQL DB cluster as shown following.

```sql
psql=> CREATE TABLE test_gzip(id int, a text, b text, c text, d text);
CREATE TABLE
psql=> SELECT aws_s3.table_import_from_s3(
             'test_gzip',
             '',
             '(format csv)',
             'myS3Bucket', 'test-data.gz', 'us-east-2')
``` 

### Importing an encoded Amazon S3 file

The following example shows how to import a file from Amazon S3 that has Windows-1252 encoding.
psql=> SELECT aws_s3.table_import_from_s3(
  'test_table', '', 'encoding 'WIN1252'',
  aws_commons.create_s3_uri('sampleBucket', 'SampleFile', 'us-east-2'))
);

**Function reference**

**Functions**

- `aws_s3.table_import_from_s3 (p. 1025)`
- `aws_commons.create_s3_uri (p. 1027)`
- `aws_commons.create_aws_credentials (p. 1027)`

**aws_s3.table_import_from_s3**

Imports Amazon S3 data into an Aurora PostgreSQL table. The `aws_s3` extension provides the `aws_s3.table_import_from_s3` function. The return value is text.

**Syntax**

The required parameters are `table_name`, `column_list` and `options`. These identify the database table and specify how the data is copied into the table.

You can also use the following parameters:

- The `s3_info` parameter specifies the Amazon S3 file to import. When you use this parameter, access to Amazon S3 is provided by an IAM role for the PostgreSQL DB cluster.

  ```
  aws_s3.table_import_from_s3 (table_name text,
                           column_list text,
                           options text,
                           s3_info aws_commons._s3_uri_1)
  ```

- The `credentials` parameter specifies the credentials to access Amazon S3. When you use this parameter, you don’t use an IAM role.

  ```
  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)
  ```

**Parameters**

**`table_name`**

A required text string containing the name of the PostgreSQL database table to import the data into.

**`column_list`**

A required text string containing an optional list of the PostgreSQL database table columns in which to copy the data. If the string is empty, all columns of the table are used. For an example, see Importing an Amazon S3 file that uses a custom delimiter (p. 1023).
options

A required text string containing arguments for the PostgreSQL COPY command. These arguments specify how the data is to be copied into the PostgreSQL table. For more details, see the PostgreSQL COPY documentation.

s3_info

An aws_commons._s3_uri_1 composite type containing the following information about the S3 object:
- **bucket** – The name of the Amazon S3 bucket containing the file.
- **file_path** – The Amazon S3 file name including the path of the file.
- **region** – The AWS Region that the file is in. For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).

credentials

An aws_commons._aws_credentials_1 composite type containing the following credentials to use for the import operation:
- Access key
- Secret key
- Session token

For information about creating an aws_commons._aws_credentials_1 composite structure, see aws_commons.create_aws_credentials (p. 1027).

Alternate syntax

To help with testing, you can use an expanded set of parameters instead of the s3_info and credentials parameters. Following are additional syntax variations for the aws_s3.table_import_from_s3 function:

- Instead of using the s3_info parameter to identify an Amazon S3 file, use the combination of the bucket, file_path, and region parameters. With this form of the function, access to Amazon S3 is provided by an IAM role on the PostgreSQL DB instance.

```python
aws_s3.table_import_from_s3 (  
    table_name text,  
    column_list text,  
    options text,  
    bucket text,  
    file_path text,  
    region text
)
```

- Instead of using the credentials parameter to specify Amazon S3 access, use the combination of the access_key, session_key, and session_token parameters.

```python
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
)
```
Alternate parameters

bucket

A text string containing the name of the Amazon S3 bucket that contains the file.

file_path

A text string containing the Amazon S3 file name including the path of the file.

region

A text string containing the AWS Region that the file is in. For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).

access_key

A text string containing the access key to use for the import operation. The default is NULL.

secret_key

A text string containing the secret key to use for the import operation. The default is NULL.

session_token

(Optional) A text string containing the session key to use for the import operation. The default is NULL.

aws_commons.create_s3_uri

Creates an aws_commons._s3_uri_1 structure to hold Amazon S3 file information. Use the results of the aws_commons.create_s3_uri function in the s3_info parameter of the aws_s3.table_import_from_s3 (p. 1025) function.

Syntax

```python
aws_commons.create_s3_uri(
    bucket text,
    file_path text,
    region text
)
```

Parameters

bucket

A required text string containing the Amazon S3 bucket name for the file.

file_path

A required text string containing the Amazon S3 file name including the path of the file.

region

A required text string containing the AWS Region that the file is in. For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).

aws_commons.create_aws_credentials

Sets an access key and secret key in an aws_commons._aws_credentials_1 structure. Use the results of the aws_commons.create_aws_credentials function in the credentials parameter of the aws_s3.table_import_from_s3 (p. 1025) function.
Syntax

```python
aws_commons.create_aws_credentials(
    access_key text,
    secret_key text,
    session_token text
)
```

Parameters

**access_key**

A required text string containing the access key to use for importing an Amazon S3 file. The default is NULL.

**secret_key**

A required text string containing the secret key to use for importing an Amazon S3 file. The default is NULL.

**session_token**

An optional text string containing the session token to use for importing an Amazon S3 file. The default is NULL. If you provide an optional `session_token`, you can use temporary credentials.

Managing Amazon Aurora PostgreSQL

The following sections discuss managing performance and scaling for an Amazon Aurora PostgreSQL DB cluster.

Topics

- Scaling Aurora PostgreSQL DB instances (p. 1028)
- Maximum connections to an Aurora PostgreSQL DB instance (p. 1028)
- Temporary storage limits for Aurora PostgreSQL (p. 1029)
- Testing Amazon Aurora PostgreSQL using fault injection queries (p. 1030)
- Displaying volume status for an Aurora DB cluster (p. 1034)

Scaling Aurora PostgreSQL DB instances

You can scale Aurora PostgreSQL DB instances in two ways, instance scaling and read scaling. For more information about read scaling, see Read scaling (p. 353).

You can scale your Aurora PostgreSQL DB cluster by modifying the DB instance class for each DB instance in the DB cluster. Aurora PostgreSQL supports several DB instance classes optimized for Aurora. Don't use db.t2 or db.t3 instance classes for larger Aurora clusters of size greater than 40 terabytes (TB). For detailed specifications of the DB instance classes supported by Aurora PostgreSQL, see Supported DB engines for DB instance classes (p. 47).

Maximum connections to an Aurora PostgreSQL DB instance

The maximum number of connections allowed to an Aurora PostgreSQL DB instance is determined by the `max_connections` parameter in the instance-level parameter group for the DB instance. By default, this value is set to the following equation:
Temporary storage limits for Aurora PostgreSQL

Aurora PostgreSQL stores tables and indexes in the Aurora storage subsystem. Aurora PostgreSQL uses separate temporary storage for non-persistent temporary files. This includes files that are used for such purposes as sorting large datasets during query processing or for index build operations. For more about storage, see Amazon Aurora storage and reliability (p. 51).

The following table shows the maximum amount of temporary storage available for each Aurora PostgreSQL DB instance class.
You can monitor the temporary storage available for a DB instance with the `FreeLocalStorage` CloudWatch metric, described in Amazon Aurora metrics (p. 489).

For some workloads, you can reduce the amount of temporary storage by allocating more memory to the processes that are performing the operation. To increase the memory available to an operation, increasing the values of the `work_mem` or `maintenance_work_mem` PostgreSQL parameters.

### Testing Amazon Aurora PostgreSQL using fault injection queries

You can test the fault tolerance of your Aurora PostgreSQL DB cluster by using fault injection queries. Fault injection queries are issued as SQL commands to an Amazon Aurora instance. Fault injection queries enable you to schedule simulated tests of the following events:

**Topics**
- Testing an instance crash (p. 1031)
- Testing an Aurora replica failure (p. 1031)
- Testing a disk failure (p. 1032)
- Testing disk congestion (p. 1033)

When a fault injection query specifies a crash, it forces a crash of the Aurora PostgreSQL DB instance. The other fault injection queries result in simulations of failure events, but don't cause the event to occur. When you submit a fault injection query, you also specify an amount of time for the failure event simulation to occur.

You can submit a fault injection query to one of your Aurora Replica instances by connecting to the endpoint for the Aurora Replica. For more information, see Amazon Aurora connection management (p. 24).
Note
Fault injection queries for Aurora PostgreSQL are currently supported for the following versions:

- Version 2.4, which is compatible with PostgreSQL version 10.11.
- Version 3.2, which is compatible with PostgreSQL version 11.7.

Testing an instance crash

You can force a crash of an Aurora PostgreSQL instance using the fault injection query function `aurora_inject_crash()`.

For this fault injection query, a failover will not occur. If you want to test a failover, then you can choose the Failover instance action for your DB cluster in the RDS console, or use the `failover-db-cluster` AWS CLI command or the `FailoverDBCluster` RDS API operation.

Syntax

```
SELECT aurora_inject_crash ('instance' | 'dispatcher' | 'node');
```

Options

This fault injection query takes one of the following crash types. The crash type is not case sensitive:

- **'instance'**
  
  A crash of the PostgreSQL-compatible database for the Amazon Aurora instance is simulated.

- **'dispatcher'**
  
  A crash of the dispatcher on the primary instance for the Aurora DB cluster is simulated. The dispatcher writes updates to the cluster volume for an Amazon Aurora DB cluster.

- **'node'**
  
  A crash of both the PostgreSQL-compatible database and the dispatcher for the Amazon Aurora instance is simulated.

Testing an Aurora replica failure

You can simulate the failure of an Aurora Replica using the fault injection query function `aurora_inject_replica_failure()`.

An Aurora Replica failure will block all requests to an Aurora Replica or all Aurora Replicas in the DB cluster for a specified time interval. When the time interval completes, the affected Aurora Replicas will be automatically synchronized with the primary instance.

Syntax

```
SELECT aurora_inject_replica_failure(
    percentage_of_failure,
    quantity,
    'replica_name'
);
```

Options

This fault injection query takes the following parameters:
percentage_of_failure

The percentage of requests to block during the failure event. This value can be a double between 0 and 100. If you specify 0, then no requests are blocked. If you specify 100, then all requests are blocked.

quantity

The amount of time to simulate the Aurora Replica failure. The interval is in seconds. For example, if the value is 20 the simulation will run for 20 seconds.

Note

Take care when specifying the time interval for your Aurora Replica failure event. If you specify too long an interval, and your writer instance writes a large amount of data during the failure event, then your Aurora DB cluster might assume that your Aurora Replica has crashed and replace it.

replica_name

The Aurora Replica in which to inject the failure simulation. Specify the name of an Aurora Replica to simulate a failure of the single Aurora Replica. Specify an empty string to simulate failures for all Aurora Replicas in the DB cluster.

To identify replica names, see the server_id column from the aurora_replica_status() function. For example:

```sql
postgres=> SELECT server_id FROM aurora_replica_status();
```

Testing a disk failure

You can simulate a disk failure for an Aurora PostgreSQL DB cluster using the fault injection query function `aurora_inject_disk_failure()`.

During a disk failure simulation, the Aurora PostgreSQL DB cluster randomly marks disk segments as faulting. Requests to those segments will be blocked for the duration of the simulation.

Syntax

```sql
SELECT aurora_inject_disk_failure(
    percentage_of_failure,
    index,
    is_disk,
    quantity
);
```

Options

This fault injection query takes the following parameters:

percentage_of_failure

The percentage of the disk to mark as faulting during the failure event. This value can be a double between 0 and 100. If you specify 0, then none of the disk is marked as faulting. If you specify 100, then the entire disk is marked as faulting.

index

A specific logical block of data in which to simulate the failure event. If you exceed the range of available logical blocks or storage nodes data, you will receive an error that tells you the maximum
Testing disk congestion

You can simulate a disk failure for an Aurora PostgreSQL DB cluster using the fault injection query function `aurora_inject_disk_congestion()`. During a disk congestion simulation, the Aurora PostgreSQL DB cluster randomly marks disk segments as congested. Requests to those segments will be delayed between the specified minimum and maximum delay time for the duration of the simulation.

**Syntax**

```sql
SELECT aurora_inject_disk_congestion(
percentage_of_failure,
index,
is_disk,
quantity,
minimum,
maximum
);
```

**Options**

This fault injection query takes the following parameters:

- **percentage_of_failure**
  
  The percentage of the disk to mark as congested during the failure event. This is a double value between 0 and 100. If you specify 0, then none of the disk is marked as congested. If you specify 100, then the entire disk is marked as congested.

- **index**
  
  A specific logical block of data or storage node to use to simulate the failure event.

  If you exceed the range of available logical blocks or storage nodes of data, you will receive an error that tells you the maximum index value that you can specify. To avoid this error, see Displaying volume status for an Aurora DB cluster (p. 1034).

- **is_disk**
  
  Indicates whether the injection failure is to a logical block or a storage node. Specifying true means injection failures are to a logical block. Specifying false means injection failures are to a storage node.

- **quantity**
  
  The amount of time to simulate the Aurora Replica failure. The interval is in seconds. For example, if the value is 20 the simulation will run for 20 seconds.
minimum, maximum

The minimum and maximum amount of congestion delay, in milliseconds. Valid values range from 0.0 to 100.0 milliseconds. Disk segments marked as congested will be delayed for a random amount of time within the minimum and maximum range for the duration of the simulation. The maximum value must be greater than the minimum value.

Displaying volume status for an Aurora DB cluster

In Amazon Aurora, a DB cluster volume consists of a collection of logical blocks. Each of these represents 10 gigabytes of allocated storage. These blocks are called protection groups.

The data in each protection group is replicated across six physical storage devices, called storage nodes. These storage nodes are allocated across three Availability Zones (AZs) in the region where the DB cluster resides. In turn, each storage node contains one or more logical blocks of data for the DB cluster volume. For more information about protection groups and storage nodes, see Introducing the Aurora storage engine on the AWS Database Blog.

Use the aurora_show_volume_status() function to return the following server status variables:

- Disks — The total number of logical blocks of data for the DB cluster volume.
- Nodes — The total number of storage nodes for the DB cluster volume.

You can use the aurora_show_volume_status() function to help avoid an error when using the aurora_inject_disk_failure() fault injection function. The aurora_inject_disk_failure() fault injection function simulates the failure of an entire storage node, or a single logical block of data within a storage node. In the function, you specify the index value of a specific logical block of data or storage node. However, the statement returns an error if you specify an index value greater than the number of logical blocks of data or storage nodes used by the DB cluster volume. For more information about fault injection queries, see Testing Amazon Aurora PostgreSQL using fault injection queries (p. 1030).

Note

The aurora_show_volume_status() function is available for Aurora PostgreSQL version 10.11. For more information about Aurora PostgreSQL versions, see Engine versions for Amazon Aurora PostgreSQL (p. 1148).

Syntax

```
SELECT * FROM aurora_show_volume_status();
```

Example

```
customer_database=> SELECT * FROM aurora_show_volume_status();
  disks | nodes
  ------+-------
      96 |    45
```

Replication with Amazon Aurora PostgreSQL

Following, you can find a description of replication with Amazon Aurora PostgreSQL, including how to monitor replication.

Topics
Using Aurora replicas

An *Aurora Replica* is an independent endpoint in an Aurora DB cluster, best used for scaling read operations and increasing availability. An Aurora DB cluster can include up to 15 Aurora Replicas located throughout the Availability Zones of the Aurora DB cluster's AWS Region.

The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary writer DB instance and to Aurora Replicas in the DB cluster. For more information about Aurora Replicas, see [Aurora Replicas (p. 57)](#).

Aurora Replicas work well for read scaling because they're fully dedicated to read operations on your cluster volume. The writer DB instance manages write operations. The cluster volume is shared among all instances in your Aurora PostgreSQL DB cluster. Thus, no extra work is needed to replicate a copy of the data for each Aurora Replica.

Aurora PostgreSQL–based DB clusters don't support Aurora Replicas in different AWS Regions. That means you can't configure your Aurora PostgreSQL DB cluster for cross-region replication. However, you can scale reads and achieve high availability for an Aurora PostgreSQL DB cluster by using the Aurora global database feature. Aurora global databases have a single read/write primary DB cluster in one AWS Region and up to five read-only secondary DB clusters in different Regions. For more information, see [Using Amazon Aurora global databases (p. 206)](#).

In addition to supporting Aurora Replicas, PostgreSQL has its own native replication capabilities, such as [logical replication](#). Unlike an Aurora Replica, PostgreSQL read replicas use a single thread to apply all write operations from the primary DB instance to their local data store. This limitation can affect the ability of PostgreSQL read replicas to support large volumes of write traffic.

**Note**

Rebooting the writer DB instance of an Amazon Aurora DB cluster also automatically reboots the Aurora Replicas for that DB cluster. The automatic reboot re-establishes an entry point that guarantees read/write consistency across the DB cluster.

Monitoring Aurora PostgreSQL replication

Read scaling and high availability depend on minimal lag time. You can monitor how far an Aurora Replica is lagging behind the writer DB instance of your Aurora PostgreSQL DB cluster by monitoring the Amazon CloudWatch *ReplicaLag* metric. Because Aurora Replicas read from the same cluster volume as the writer DB instance, the *ReplicaLag* metric has a different meaning for an Aurora PostgreSQL DB cluster. The *ReplicaLag* metric for an Aurora Replica indicates the lag for the page cache of the Aurora Replica compared to that of the writer DB instance.

For more information on monitoring RDS instances and CloudWatch metrics, see [Monitoring an Amazon Aurora DB cluster (p. 459)](#).

Using PostgreSQL logical replication with Aurora

PostgreSQL logical replication provides fine-grained control over replicating and synchronizing parts of a database. For example, you can use logical replication to replicate an individual table of a database.

Following, you can find information about how to work with PostgreSQL logical replication and Amazon Aurora. For more detailed information about the PostgreSQL implementation of logical replication, see [Logical replication](#) and [Logical decoding concepts](#) in the PostgreSQL documentation.
Note
Logical replication is available with Aurora PostgreSQL version 2.2.0 (compatible with PostgreSQL 10.6) and later.

Following, you can find information about how to work with PostgreSQL logical replication and Amazon Aurora.

Topics
• Configuring logical replication (p. 1036)
• Example of logical replication of a database table (p. 1037)
• Logical replication using the AWS Database Migration Service (p. 1038)

Configuring logical replication

To use logical replication, you first set the rds.logical_replication parameter for a cluster parameter group. You then set up the publisher and subscriber.

Logical replication uses a publish and subscribe model. Publishers and subscribers are the nodes. A publication is a set of changes generated from one or more database tables. You specify a publication on a publisher. A subscription defines the connection to another database and one or more publications to which it subscribes. You specify a subscription on a subscriber. The publication and subscription make the connection between the publisher and subscriber.

Note
To perform logical replication for a PostgreSQL database, your AWS user account needs the rds_superuser role.

To enable PostgreSQL logical replication with Aurora

1. Create a new DB cluster parameter group to use for logical replication, as described in Creating a DB cluster parameter group (p. 302). Use the following settings:
   • For Parameter group family, choose aurora-postgres10 or later.
   • For Type, choose DB Cluster Parameter Group.
2. Modify the cluster parameter group, as described in Modifying parameters in a DB cluster parameter group (p. 305). Set the rds.logical_replication static parameter to 1.

   Enabling the rds.logical_replication parameter affects the DB cluster’s performance.

To configure a publisher for logical replication

1. Set the publisher’s cluster parameter group:
   • To use an existing Aurora PostgreSQL DB cluster for the publisher, the engine version must be 10.6 or later. Do the following:
     1. Modify the cluster parameter group to set it to the group that you created when you enabled logical replication. For details about modifying an Aurora PostgreSQL DB cluster, see Modifying an Amazon Aurora DB cluster (p. 327).
     2. Restart the DB cluster for static parameter changes to take effect. The cluster parameter group includes a change to the static parameter rds.logical_replication.
   • To use a new Aurora PostgreSQL DB cluster for the publisher, create the DB cluster using the following settings. For details about creating an Aurora PostgreSQL DB cluster, see Creating a DB cluster (p. 119).
     1. Choose the Amazon Aurora engine and choose the PostgreSQL-compatible edition.
2. For **DB engine version**, choose an Aurora PostgreSQL engine that is compatible with PostgreSQL 10.6 or greater.

3. For **DB cluster parameter group**, choose the group that you created when you enabled logical replication.

2. Modify the inbound rules of the security group for the publisher to allow the subscriber to connect. Usually, you do this by including the IP address of the subscriber in the security group. For details about modifying a security group, see Security groups for your VPC in the Amazon Virtual Private Cloud User Guide.

---

### Example of logical replication of a database table

To implement logical replication, use the PostgreSQL commands `CREATE PUBLICATION` and `CREATE SUBSCRIPTION`.

For this example, table data is replicated from an Aurora PostgreSQL database as the publisher to a PostgreSQL database as the subscriber. Note that a subscriber database can be an RDS PostgreSQL database or an Aurora PostgreSQL database. A subscriber can also be an application that uses PostgreSQL logical replication. After the logical replication mechanism is set up, changes on the publisher are continually sent to the subscriber as they occur.

To set up logical replication for this example, do the following:

1. Configure an Aurora PostgreSQL DB cluster as the publisher. To do so, create a new Aurora PostgreSQL DB cluster, as described when configuring the publisher in Configuring logical replication (p. 1036).

2. Set up the publisher database.

   For example, create a table using the following SQL statement on the publisher database.

```
CREATE TABLE LogicalReplicationTest (a int PRIMARY KEY);
```

3. Insert data into the publisher database by using the following SQL statement.

```
INSERT INTO LogicalReplicationTest VALUES (generate_series(1,10000));
```

4. Create a publication on the publisher by using the following SQL statement.

```
CREATE PUBLICATION testpub FOR TABLE LogicalReplicationTest;
```

5. Create your subscriber. A subscriber database can be either of the following:
   - Aurora PostgreSQL database version 2.2.0 (compatible with PostgreSQL 10.6) or later.
   - Amazon RDS for PostgreSQL database with the PostgreSQL DB engine version 10.4 or later.

   For this example, we create an Amazon RDS for PostgreSQL database as the subscriber. For details on creating a DB instance, see Creating a DB instance in the Amazon RDS User Guide.

6. Set up the subscriber database.

   For this example, create a table like the one created for the publisher by using the following SQL statement.

```
CREATE TABLE LogicalReplicationTest (a int PRIMARY KEY);
```

7. Verify that there is data in the table at the publisher but no data yet at the subscriber by using the following SQL statement on both databases.
8. Create a subscription on the subscriber.

Use the following SQL statement on the subscriber database and the following settings from the publisher cluster:

- **host** – The publisher cluster's writer DB instance.
- **port** – The port on which the writer DB instance is listening. The default for PostgreSQL is 5432.
- **dbname** – The DB name of the publisher cluster.

```sql
CREATE SUBSCRIPTION testsub CONNECTION
  'host=publisher-cluster-writer-endpoint port=5432 dbname=db-name user=user
  password=password'
PUBLICATION testpub;
```

After the subscription is created, a logical replication slot is created at the publisher.

9. To verify for this example that the initial data is replicated on the subscriber, use the following SQL statement on the subscriber database.

```sql
SELECT count(*) FROM LogicalReplicationTest;
```

Any further changes on the publisher are replicated to the subscriber.

**Logical replication using the AWS Database Migration Service**

You can use the AWS Database Migration Service (AWS DMS) to replicate a database or a portion of a database. Use AWS DMS to migrate your data from an Aurora PostgreSQL database to another open source or commercial database. For more information about AWS DMS, see the AWS Database Migration Service User Guide.

The following example shows how to set up logical replication from an Aurora PostgreSQL database as the publisher and then use AWS DMS for migration. This example uses the same publisher and subscriber that were created in Example of logical replication of a database table (p. 1037).

To set up logical replication with AWS DMS, you need details about your publisher and subscriber from Amazon RDS. In particular, you need details about the publisher's writer DB instance and the subscriber's DB instance.

Get the following information for the publisher's writer DB instance:

- The virtual private cloud (VPC) identifier
- The subnet group
- The Availability Zone (AZ)
- The VPC security group
- The DB instance ID

Get the following information for the subscriber's DB instance:

- The DB instance ID
- The source engine
To use AWS DMS for logical replication with Aurora PostgreSQL

1. Prepare the publisher database to work with AWS DMS.

   To do this, PostgreSQL 10.x and later databases require that you apply AWS DMS wrapper functions to the publisher database. For details on this and later steps, see the instructions in Using PostgreSQL version 10.x and later as a source for AWS DMS in the AWS Database Migration Service User Guide.

2. Sign in to the AWS Management Console and open the AWS DMS console at https://console.aws.amazon.com/dms. At top right, choose the same AWS Region in which the publisher and subscriber are located.

3. Create an AWS DMS replication instance.

   Choose values that are the same as for your publisher's writer DB instance. These include the following settings:
   
   - For VPC, choose the same VPC as for the writer DB instance.
   - For Replication Subnet Group, choose the same subnet group as for the writer DB instance.
   - For Availability zone, choose the same zone as for the writer DB instance.
   - For VPC Security Group, choose the same group as for the writer DB instance.

4. Create an AWS DMS endpoint for the source.

   Specify the publisher as the source endpoint by using the following settings:
   
   - For Endpoint type, choose Source endpoint.
   - Choose Select RDS DB Instance.
   - For RDS Instance, choose the DB identifier of the publisher's writer DB instance.
   - For Source engine, choose postgres.

5. Create an AWS DMS endpoint for the target.

   Specify the subscriber as the target endpoint by using the following settings:
   
   - For Endpoint type, choose Target endpoint.
   - Choose Select RDS DB Instance.
   - For RDS Instance, choose the DB identifier of the subscriber DB instance.
   - Choose a value for Source engine. For example, if the subscriber is an RDS PostgreSQL database, choose postgres. If the subscriber is an Aurora PostgreSQL database, choose aurora-postgresql.

6. Create an AWS DMS database migration task.

   You use a database migration task to specify what database tables to migrate, to map data using the target schema, and to create new tables on the target database. At a minimum, use the following settings for Task configuration:
   
   - For Replication instance, choose the replication instance that you created in an earlier step.
   - For Source database endpoint, choose the publisher source that you created in an earlier step.
   - For Target database endpoint, choose the subscriber target that you created in an earlier step.

   The rest of the task details depend on your migration project. For more information about specifying all the details for DMS tasks, see Working with AWS DMS tasks in the AWS Database Migration Service User Guide.

After AWS DMS creates the task, it begins migrating data from the publisher to the subscriber.
Integrating Amazon Aurora PostgreSQL with other AWS services

Amazon Aurora integrates with other AWS services so that you can extend your Aurora PostgreSQL DB cluster to use additional capabilities in the AWS Cloud. Your Aurora PostgreSQL DB cluster can use AWS services to do the following:

- Quickly collect, view, and assess performance for your Aurora PostgreSQL DB instances with Amazon RDS Performance Insights. Performance Insights expands on existing Amazon RDS monitoring features to illustrate your database's performance and help you analyze any issues that affect it. With the Performance Insights dashboard, you can visualize the database load and filter the load by waits, SQL statements, hosts, or users.

For more information about Performance Insights, see Using Amazon RDS Performance Insights (p. 514).

- Automatically add or remove Aurora Replicas with Aurora Auto Scaling. For more information, see Using Amazon Aurora Auto Scaling with Aurora replicas (p. 372).

- Configure your Aurora PostgreSQL DB cluster to publish log data to Amazon CloudWatch Logs. CloudWatch Logs provide highly durable storage for your log records. With CloudWatch Logs, you can perform real-time analysis of the log data, and use CloudWatch to create alarms and view metrics. For more information, see Publishing Aurora PostgreSQL logs to Amazon CloudWatch Logs (p. 1075).

Exporting data from an Aurora PostgreSQL DB cluster to Amazon S3

You can query data from an Aurora PostgreSQL DB cluster and export it directly into files stored in an Amazon S3 bucket. To do this, you use the `aws_s3` PostgreSQL extension that Aurora PostgreSQL provides.

**Note**

To export data to Amazon S3 from Aurora PostgreSQL, your database must be running one of the following PostgreSQL engine versions:

- PostgreSQL version 10.11 or higher
- PostgreSQL version 11.6 or higher

For more information on storing data with Amazon S3, see Create a bucket in the Amazon Simple Storage Service Getting Started Guide.

**Topics**

- Overview of exporting data to Amazon S3 (p. 1041)
- Specifying the Amazon S3 file path to export to (p. 1041)
- Setting up access to an Amazon S3 bucket (p. 1042)
- Exporting query data using the `aws_s3.query_export_to_s3` function (p. 1044)
- Function reference (p. 1047)
Overview of exporting data to Amazon S3

To export data stored in an Aurora PostgreSQL database to an Amazon S3 bucket, use the following procedure.

To export Aurora PostgreSQL data to S3

1. Install the required PostgreSQL extensions. These include the `aws_s3` and `aws_commons` extensions. To do so, start psql and use the following commands.

   ```sql
   CREATE EXTENSION IF NOT EXISTS aws_s3 CASCADE;
   ```

   The `aws_s3` extension provides the `aws_s3.query_export_to_s3` function that you use to export data to Amazon S3. The `aws_commons` extension is included to provide additional helper functions.

2. Identify an Amazon S3 file path to use for exporting data. For details about this process, see Specifying the Amazon S3 file path to export to.

3. Provide permission to access the Amazon S3 bucket.

   To export data to an Amazon S3 file, give the Aurora PostgreSQL DB cluster permission to access the Amazon S3 bucket that the export will use for storage. Doing this includes the following steps:
   
   1. Create an IAM policy that provides access to an Amazon S3 bucket that you want to export to.
   2. Create an IAM role.
   3. Attach the policy you created to the role you created.
   4. Add this IAM role to your DB cluster.

   For details about this process, see Setting up access to an Amazon S3 bucket.

4. Identify a database query to get the data. Export the query data by calling the `aws_s3.query_export_to_s3` function.

   After you complete the preceding preparation tasks, use the `aws_s3.query_export_to_s3` function to export query results to Amazon S3. For details about this process, see Exporting query data using the `aws_s3.query_export_to_s3` function.

Specifying the Amazon S3 file path to export to

Specify the following information to identify the location in Amazon S3 where you want to export data to:

- Bucket name – A bucket is a container for Amazon S3 objects or files.

  For more information on storing data with Amazon S3, see Create a bucket and View an object in the Amazon Simple Storage Service Getting Started Guide.

- File path – The file path identifies where the export is stored in the Amazon S3 bucket. The file path consists of the following:
  
  - An optional path prefix that identifies a virtual folder path.
  - A file prefix that identifies one or more files to be stored. Larger exports are stored in multiple files, each with a maximum size of approximately 6 GB. The additional file names have the same file prefix but with `_partXX` appended. The `XX` represents 2, then 3, and so on.

  For example, a file path with an `exports` folder and a `query-1-export` file prefix is `/exports/query-1-export`.


• AWS Region (optional) – The AWS Region where the Amazon S3 bucket is located. If you don't specify an AWS Region value, then Aurora saves your files into Amazon S3 in the same AWS Region as the exporting DB cluster.

  **Note**

  Currently, the AWS Region must be the same as the region of the exporting DB cluster.

  For a listing of AWS Region names and associated values, see [Regions and Availability Zones](p. 5).

To hold the Amazon S3 file information about where the export is to be stored, you can use the `aws_commons.create_s3_uri` function to create an `aws_commons._s3_uri_1` composite structure as follows.

```sql
psql=> SELECT aws_commons.create_s3_uri(  
  'sample-bucket',  
  'sample-filepath',  
  'us-west-2'  
) AS s3_uri_1 \gset
```

You later provide this `s3_uri_1` value as a parameter in the call to the `aws_s3.query_export_to_s3` function. For examples, see [Exporting query data using the `aws_s3.query_export_to_s3` function](p. 1044).

### Setting up access to an Amazon S3 bucket

To export data to Amazon S3, give your PostgreSQL DB cluster permission to access the Amazon S3 bucket that the files are to go in.

To do this, use the following procedure.

**To give a PostgreSQL DB cluster access to Amazon S3 through an IAM role**

1. Create an IAM policy.

   This policy provides the bucket and object permissions that allow your PostgreSQL DB cluster to access Amazon S3.

   As part of creating this policy, take the following steps:

   a. Include in the policy the following required actions to allow the transfer of files from your PostgreSQL DB cluster to an Amazon S3 bucket:

      - `s3:PutObject`
      - `s3:AbortMultipartUpload`

   b. Include the Amazon Resource Name (ARN) that identifies the Amazon S3 bucket and objects in the bucket. The ARN format for accessing Amazon S3 is: `arn:aws:s3:::your-s3-bucket/*`

   For more information on creating an IAM policy for Aurora PostgreSQL, see [Creating and using an IAM policy for IAM database access](p. 1241). See also Tutorial: Create and attach your first customer managed policy in the IAM User Guide.

   The following AWS CLI command creates an IAM policy named `rds-s3-export-policy` with these options. It grants access to a bucket named `your-s3-bucket`.

   **Warning**

   We recommend that you set up your database within a private VPC that has endpoint policies configured for accessing specific buckets. For more information, see [Using endpoint policies for Amazon S3](in the Amazon VPC User Guide).
We strongly recommend that you do not create a policy with all-resource access. This access can pose a threat for data security. If you create a policy that gives S3:PutObject access to all resources using "Resource":"*", then a user with export privileges can export data to all buckets in your account. In addition, the user can export data to any publicly writable bucket within your AWS Region.

After you create the policy, note the Amazon Resource Name (ARN) of the policy. You need the ARN for a subsequent step when you attach the policy to an IAM role.

```
aws iam create-policy --policy-name rds-s3-export-policy --policy-document '{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "s3export",
     "Action": [ "S3:PutObject"
     ],
     "Effect": "Allow",
     "Resource": [ "arn:aws:s3:::your-s3-bucket/*" ]
   }]
}
```

2. Create an IAM role.

You do this so Aurora PostgreSQL can assume this IAM role on your behalf to access your Amazon S3 buckets. For more information, see Creating a role to delegate permissions to an IAM user in the IAM User Guide.

The following example shows using the AWS CLI command to create a role named 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": "rds.amazonaws.com" },
     "Action": "sts:AssumeRole"
   }
  ]
}
```

3. Attach the IAM policy that you created to the IAM role that you created.

The following AWS CLI command attaches the policy created earlier to the role named rds-s3-export-role. Replace your-policy-arn with the policy ARN that you noted in an earlier step.

```
aws iam attach-role-policy --policy-arn your-policy-arn --role-name rds-s3-export-role
```

4. Add the IAM role to the DB cluster. You do so by using the AWS Management Console or AWS CLI, as described following.
Amazon Aurora User Guide for Aurora

Exporting query data using the
aws_s3.query_export_to_s3 function

Console

To add an IAM role for a PostgreSQL DB cluster using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose the PostgreSQL DB cluster name to display its details.
3. On the Connectivity & security tab, in the Manage IAM roles section, choose the role to add under Add IAM roles to this instance.
4. Under Feature, choose s3Export.
5. Choose Add role.

AWS CLI

To add an IAM role for a PostgreSQL DB cluster using the CLI

- Use the following command to add the role to the PostgreSQL DB cluster named my-db-cluster. Replace your-role-arn with the role ARN that you noted in a previous step. Use s3Export for the value of the --feature-name option.

Example

For Linux, macOS, or Unix:

```bash
aws rds add-role-to-db-cluster \
--db-cluster-identifier my-db-cluster \
--feature-name s3Export \
--role-arn your-role-arn \
--region your-region
```

For Windows:

```bash
aws rds add-role-to-db-cluster ^
   --db-cluster-identifier my-db-cluster ^
   --feature-name s3Export ^
   --role-arn your-role-arn ^
   --region your-region
```

Exporting query data using the
aws_s3.query_export_to_s3 function

Export your PostgreSQL data to Amazon S3 by calling the aws_s3.query_export_to_s3 (p. 1047) function.

Topics

- Prerequisites (p. 1045)
- Calling aws_s3.query_export_to_s3 (p. 1045)
- Exporting to a CSV file that uses a custom delimiter (p. 1046)
- Exporting to a binary file with encoding (p. 1046)
- Troubleshooting access to Amazon S3 (p. 1046)
Prerequisites

Before you use the `aws_s3.query_export_to_s3` function, be sure to complete the following prerequisites:

- Install the required PostgreSQL extensions as described in Overview of exporting data to Amazon S3 (p. 1041).
- Determine where to export your data to Amazon S3 as described in Specifying the Amazon S3 file path to export to (p. 1041).
- Make sure that the DB cluster has export access to Amazon S3 as described in Setting up access to an Amazon S3 bucket (p. 1042).

The examples following use a database table called `sample_table`. These examples export the data into a bucket called `sample-bucket`. The example table and data are created with the following SQL statements in psql.

```
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');
```

Calling `aws_s3.query_export_to_s3`

The following shows the basic ways of calling the `aws_s3.query_export_to_s3` (p. 1047) function.

These examples use the variable `s3_uri_1` to identify a structure that contains the information identifying the Amazon S3 file. Use the `aws_commons.create_s3_uri` (p. 1049) function to create the structure.

```
psql=> SELECT aws_commons.create_s3_uri(
     'sample-bucket',
     'sample-filepath',
     'us-west-2'
 ) AS s3_uri_1 \gset
```

Although the parameters vary for the following two `aws_s3.query_export_to_s3` function calls, the results are the same for these examples. All rows of the `sample_table` table are exported into a bucket called `sample-bucket`.

```
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');
```

The parameters are described as follows:

- `SELECT * FROM sample_table` – The first parameter is a required text string containing an SQL query. The PostgreSQL engine runs this query. The results of the query are copied to the S3 bucket identified in other parameters.
- `:'s3_uri_1` – This parameter is a structure that identifies the Amazon S3 file. This example uses a variable to identify the previously created structure. You can instead create the structure by including the `aws_commons.create_s3_uri` function call inline within the `aws_s3.query_export_to_s3` function call as follows.

```
SELECT * from aws_s3.query_export_to_s3('select * from sample_table',
    aws_commons.create_s3_uri('sample-bucket', 'sample-filepath', 'us-west-2')
```
• `options :='format text'` – The `options` parameter is an optional text string containing PostgreSQL `COPY` arguments. The copy process uses the arguments and format of the PostgreSQL `COPY` command.

If the file specified doesn't exist in the Amazon S3 bucket, it's created. If the file already exists, it's overwritten. The syntax for accessing the exported data in Amazon S3 is the following.

```
s3-region://bucket-name[/path-prefix]/file-prefix
```

Larger exports are stored in multiple files, each with a maximum size of approximately 6 GB. The additional file names have the same file prefix but with `_partXX` appended. The `XX` represents 2, then 3, and so on. For example, suppose that you specify the path where you store data files as the following.

```
s3-us-west-2://my-bucket/my-prefix
```

If the export has to create three data files, the Amazon S3 bucket contains the following data files.

```
s3-us-west-2://my-bucket/my-prefix
s3-us-west-2://my-bucket/my-prefix_part2
s3-us-west-2://my-bucket/my-prefix_part3
```

For the full reference for this function and additional ways to call it, see `awss3.query_export_to_s3 (p. 1047)`. For more about accessing files in Amazon S3, see View an object in the Amazon Simple Storage Service Getting Started Guide.

### Exporting to a CSV file that uses a custom delimiter

The following example shows how to call the `aws_s3.query_export_to_s3 (p. 1047)` function to export data to a file that uses a custom delimiter. The example uses arguments of the PostgreSQL `COPY` command to specify the comma-separated value (CSV) format and a colon (:) delimiter.

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
  options :='format csv, delimiter $$:$$');
```

### Exporting to a binary file with encoding

The following example shows how to call the `aws_s3.query_export_to_s3 (p. 1047)` function to export data to a binary file that has Windows-1253 encoding.

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
  options :='format binary, encoding WIN1253');
```

### Troubleshooting access to Amazon S3

If you encounter connection problems when attempting to export data to Amazon S3, see the following for recommendations:

- Troubleshooting Amazon Aurora identity and access (p. 1263)
- Troubleshooting Amazon S3 in the Amazon Simple Storage Service Developer Guide.
- Troubleshooting Amazon S3 and IAM in the IAM User Guide.
Function reference

Functions

• `aws_s3.query_export_to_s3` (p. 1047)
• `aws_commons.create_s3_uri` (p. 1049)

**aws_s3.query_export_to_s3**

Exports a PostgreSQL query result to an Amazon S3 bucket. The `aws_s3` extension provides the `aws_s3.query_export_to_s3` function.

The two required parameters are `query` and `s3_info`. These define the query to be exported and identify the Amazon S3 bucket to export to. An optional parameter called `options` provides for defining various export parameters. For examples of using the `aws_s3.query_export_to_s3` function, see Exporting query data using the `aws_s3.query_export_to_s3` function (p. 1044).

**Syntax**

```sql
aws_s3.query_export_to_s3(
    query text,
    s3_info aws_commons._s3_uri_1,
    options text
)
```

**Input parameters**

`query`

A required text string containing an SQL query that the PostgreSQL engine runs. The results of this query are copied to an S3 bucket identified in the `s3_info` parameter.

`s3_info`

An `aws_commons._s3_uri_1` composite type containing the following information about the S3 object:

- `bucket` – The name of the Amazon S3 bucket to contain the file.
- `file_path` – The Amazon S3 file name and path.
- `region` – The AWS Region that the bucket is in. For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).

Currently, this value must be the same AWS Region as that of the exporting DB cluster. The default is the AWS Region of the exporting DB cluster.

To create an `aws_commons._s3_uri_1` composite structure, see the `aws_commons.create_s3_uri` (p. 1049) function.

`options`

An optional text string containing arguments for the PostgreSQL COPY command. These arguments specify how the data is to be copied when exported. For more details, see the PostgreSQL COPY documentation.

**Alternate input parameters**

To help with testing, you can use an expanded set of parameters instead of the `s3_info` parameter. Following are additional syntax variations for the `aws_s3.query_export_to_s3` function.
Instead of using the `s3_info` parameter to identify an Amazon S3 file, use the combination of the `bucket`, `file_path`, and `region` parameters.

```python
aws_s3.query_export_to_s3(
    query text,
    bucket text,
    file_path text,
    region text,
    options text
)
```

**query**

A required text string containing an SQL query that the PostgreSQL engine runs. The results of this query are copied to an S3 bucket identified in the `s3_info` parameter.

**bucket**

A required text string containing the name of the Amazon S3 bucket that contains the file.

**file_path**

A required text string containing the Amazon S3 file name including the path of the file.

**region**

An optional text string containing the AWS Region that the bucket is in. For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).

Currently, this value must be the same AWS Region as that of the exporting DB cluster. The default is the AWS Region of the exporting DB cluster.

**options**

An optional text string containing arguments for the PostgreSQL `COPY` command. These arguments specify how the data is to be copied when exported. For more details, see the PostgreSQL `COPY` documentation.

**Output parameters**

```python
aws_s3.query_export_to_s3(
    OUT rows_uploaded bigint,
    OUT files_uploaded bigint,
    OUT bytes_uploaded bigint
)
```

**rows_uploaded**

The number of table rows that were successfully uploaded to Amazon S3 for the given query.

**files_uploaded**

The number of files uploaded to Amazon S3. Files are created in sizes of approximately 6 GB. Each additional file created has `_partXX` appended to the name. The `XX` represents 2, then 3, and so on as needed.

**bytes_uploaded**

The total number of bytes uploaded to Amazon S3.
Examples

```sql
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-bucket', 'sample-filepath');
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-bucket', 'sample-filepath', 'us-west-2');
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-bucket', 'sample-filepath', 'us-west-2', 'format text');
```

/aws_commons.create_s3_uri

Creates an `aws_commons._s3_uri_1` structure to hold Amazon S3 file information. You use the results of the `aws_commons.create_s3_uri` function in the `s3_info` parameter of the `aws_s3.query_export_to_s3` (p. 1047) function. For an example of using the `aws_commons.create_s3_uri` function, see Specifying the Amazon S3 file path to export to (p. 1041).

Syntax

```
aws_commons.create_s3_uri(
    bucket text,
    file_path text,
    region text
)
```

Input parameters

- **bucket**
  
  A required text string containing the Amazon S3 bucket name for the file.

- **file_path**
  
  A required text string containing the Amazon S3 file name including the path of the file.

- **region**
  
  A required text string containing the AWS Region that the file is in. For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).

Managing query execution plans for Aurora PostgreSQL

With query plan management for Amazon Aurora with PostgreSQL compatibility, you can control how and when query execution plans change. Query plan management has two main objectives:

- Preventing plan regressions when the database system changes
- Controlling when the query optimizer can use new plans

The quality and consistency of query optimization have a major impact on the performance and stability of any relational database management system (RDBMS). Query optimizers create a query execution plan for a SQL statement at a specific point in time. As conditions change, the optimizer might pick a different plan that makes performance better or worse. In some cases, a number of changes can all cause the query optimizer to choose a different plan and lead to performance regression. These changes
include changes in statistics, constraints, environment settings, query parameter bindings, and software upgrades. Regression is a major concern for high-performance applications.

With query plan management, you can control execution plans for a set of statements that you want to manage. You can do the following:

- Improve plan stability by forcing the optimizer to choose from a small number of known, good plans.
- Optimize plans centrally and then distribute the best plans globally.
- Identify indexes that aren't used and assess the impact of creating or dropping an index.
- Automatically detect a new minimum-cost plan discovered by the optimizer.
- Try new optimizer features with less risk, because you can choose to approve only the plan changes that improve performance.

Topics
- Enabling query plan management for Aurora PostgreSQL (p. 1050)
- Upgrading query plan management (p. 1051)
- Basics of query plan management (p. 1051)
- Best practices for query plan management (p. 1054)
- Examining plans in the apg_plan_mgmt.dba_plans view (p. 1055)
- Capturing execution plans (p. 1058)
- Using managed plans (p. 1059)
- Maintaining execution plans (p. 1062)
- Parameter reference for query plan management (p. 1066)
- Function reference for query plan management (p. 1070)

**Enabling query plan management for Aurora PostgreSQL**

Query plan management is available with Amazon Aurora PostgreSQL version 2.1.0 (compatible with PostgreSQL 10.5) and greater versions.

**To enable query plan management**

1. Open the Amazon RDS console at [https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. Create a new instance-level parameter group to use for query plan management parameters. For more information, see Creating a DB parameter group (p. 301). Associate the new parameter group with the DB instances in which you want to use query plan management. For more information, see Modify a DB instance in a DB cluster (p. 328).
3. Create a new cluster-level parameter group to use for query plan management parameters. For more information, see Creating a DB cluster parameter group (p. 302). Associate the new cluster-level parameter group with the DB clusters in which you want to use query plan management. For more information, see Modifying the DB cluster by using the console, CLI, and API (p. 327).
4. Open your cluster-level parameter group and set the `rds.enable_plan_management` parameter to 1. For more information, see Modifying parameters in a DB cluster parameter group (p. 305).
5. Restart your DB instance to enable this new setting.
6. Connect to your DB instance with a SQL client such as psql.
7. Create the `apg_plan_mgmt` extension for your DB instance. The following shows an example.

```sql
psql my-database
```
CREATE EXTENSION apg_plan_mgmt;

If you create the `apg_plan_mgmt` extension in the `template1` default database, then the query plan management extension is available in each new database that you create.

**Note**

To create the `apg_plan_mgmt` extension, you need the `rds_superuser` role. When you create the `apg_plan_mgmt` extension, the `apg_plan_mgmt` role is created. Users must be granted the `apg_plan_mgmt` role to administer the `apg_plan_mgmt` extension.

---

**Upgrading query plan management**

The latest version of query plan management is 2.0. If you installed an earlier version of query plan management, we strongly recommend that you upgrade to version 2.0. For version details, see Extensions and modules for Amazon Aurora PostgreSQL (p. 1188).

To upgrade, run the following commands at the cluster or DB instance level.

```
ALTER EXTENSION apg_plan_mgmt UPDATE TO '2.0';
SELECT apg_plan_mgmt.validate_plans('update_plan_hash');
SELECT apg_plan_mgmt.reload();
```

---

**Basics of query plan management**

You can manage any SELECT, INSERT, UPDATE, or DELETE statement with query plan management, regardless of how complex the statement is. Prepared, dynamic, embedded, and immediate-mode SQL statements are all supported. All PostgreSQL language features can be used, including partitioned tables, inheritance, row-level security, and recursive common table expressions (CTEs).

**Topics**

- Performing a manual plan capture (p. 1051)
- Viewing captured plans (p. 1052)
- Working with managed statements and the SQL hash (p. 1052)
- Working with automatic plan capture (p. 1053)
- Validating plans (p. 1053)
- Approving new plans that improve performance (p. 1054)
- Deleting plans (p. 1054)

---

**Performing a manual plan capture**

To capture plans for specific statements, use the manual capture mode as in the following example.

```
/* Turn on manual capture */
SET apg_plan_mgmt.capture_plan_baselines = manual;
EXPLAIN SELECT COUNT(*) FROM pg_class; -- capture the plan baseline
SET apg_plan_mgmt.capture_plan_baselines = off; -- turn off capture
SET apg_plan_mgmt.use_plan_baselines = true; -- turn on plan usage
```

You can either execute SELECT, INSERT, UPDATE, or DELETE statements, or you can include the EXPLAIN statement as shown above. Use EXPLAIN to capture a plan without the overhead or potential side-effects of executing the statement. For more about manual capture, see Manually capturing plans for specific SQL statements (p. 1058).
Viewing captured plans

When EXPLAIN SELECT runs in the previous example, the optimizer saves the plan. To do so, it inserts a row into the `apg_plan_mgmt.dba_plans` view and commits the plan in an autonomous transaction. You can see the contents of the `apg_plan_mgmt.dba_plans` view if you've been granted the `apg_plan_mgmt` role. The following query displays some important columns of the `dba_plans` view.

```sql
SELECT sql_hash, plan_hash, status, enabled, plan_outline, sql_text::varchar(40)
FROM apg_plan_mgmt.dba_plans
ORDER BY sql_text, plan_created;
```

Each row displayed represents a managed plan. The preceding example displays the following information.

- `sql_hash` – The ID of the managed statement that the plan is for.
- `plan_hash` – The ID of the managed plan.
- `status` – The status of the plan. The optimizer can run an approved plan.
- `enabled` – A value that indicates whether the plan is enabled for use or disabled and not for use.
- `plan_outline` – Details of the managed plan.

For more about the `apg_plan_mgmt.dba_plans` view, see Examining plans in the `apg_plan_mgmt.dba_plans` view (p. 1055).

Working with managed statements and the SQL hash

A managed statement is a SQL statement captured by the optimizer under query plan management. You specify which SQL statements to capture as managed statements using either manual or automatic capture:

- For manual capture, you provide the specific statements to the optimizer as shown in the previous example.
- For automatic capture, the optimizer captures plans for statements that run multiple times. Automatic capture is shown in a later example.

In the `apg_plan_mgmt.dba_plans` view, you can identify a managed statement with a SQL hash value. The SQL hash is calculated on a normalized representation of the SQL statement that removes some differences such as the literal values. Using normalization means that when multiple SQL statements differ only in their literal or parameter values, they are represented by the same SQL hash in the `apg_plan_mgmt.dba_plans` view. Therefore, there can be multiple plans for the same SQL hash where each plan is optimal under different conditions.

When the optimizer processes any SQL statement, it uses the following rules to create the normalized SQL statement:

- Removes any leading block comment
- Removes the EXPLAIN keyword and EXPLAIN options, if present
- Removes trailing spaces
- Removes all literals
- Preserves space and case for readability

For example, take the following statement.

```sql
/*Leading comment*/ EXPLAIN SELECT /* Query 1 */ * FROM t WHERE x > 7 AND y = 1;
```
The optimizer normalizes this statement as the following.

```
SELECT /* Query 1 */ * FROM t WHERE x > CONST AND y = CONST;
```

## Working with automatic plan capture

Use automatic plan capture if you want to capture plans for all SQL statements in your application, or if you can’t use manual capture. With automatic plan capture, the optimizer captures plans for statements that run at least two times. To use automatic plan capture, do the following.

1. Create a custom DB parameter group based on the default DB parameter group for the version of Aurora PostgreSQL that you’re running.
2. Edit the custom DB parameter group, by changing the `apg_plan_mgmt.capture_plan_baselines` setting to `automatic`.
3. Save your customized DB parameter group.
4. Apply your custom DB parameter group to an Aurora DB instance that is already running as follows:
   - Choose your Aurora PostgreSQL DB instance from the list in the navigation pane, and then choose Modify.
   - In the Additional configuration section of the Modify DB instance page, for the DB parameter group, choose your custom DB parameter group.
   - Choose Continue. Confirm the Summary of modifications and choose Apply immediately.
   - Choose Modify DB instance to apply your custom DB parameter group.

You can also use your custom DB parameter group when you create a new Aurora PostgreSQL DB instance. For more information about parameter groups, see Modifying parameters in a DB parameter group (p. 303).

As your application runs, the optimizer captures plans for any statement that runs more than once. The optimizer always sets the status of a managed statement's first captured plan to approved. A managed statement's set of approved plans is known as its plan baseline.

As your application continues to run, the optimizer might find additional plans for the managed statements. The optimizer sets additional captured plans to a status of Unapproved.

The set of all captured plans for a managed statement is known as the plan history. Later, you can decide if the Unapproved plans perform well and change them to Approved, Rejected, or Preferred by using the `apg_plan_mgmt.evolve_plan_baselines` function or the `apg_plan_mgmt.set_plan_status` function.

To turn off automatic plan capture, set `apg_plan_mgmt.capture_plan_baselines` to off in the parameter group for the DB instance. Follow the same general process as outlined above, modifying your custom DB parameter group value for `apg_plan_mgmt.capture_plan_baselines` and then applying the custom DB parameter group to your Aurora DB instance.

For more about plan capture, see Capturing execution plans (p. 1058).

## Validating plans

Managed plans can become invalid (“stale”) when objects that they depend on are removed, such as an index. To find and delete all plans that are stale, use the `apg_plan_mgmt.validate_plans` function.

```
SELECT apg_plan_mgmt.validate_plans('delete');
```

For more information, see Validating plans (p. 1063).
Best practices for query plan management

Approving new plans that improve performance

While using your managed plans, you can verify whether newer, lower-cost plans discovered by the optimizer are faster than the minimum-cost plan already in the plan baseline. To do the performance comparison and optionally approve the faster plans, call the `apg_plan_mgmt.evolve_plan_baselines` function.

The following example automatically approves any unapproved plan that is enabled and faster by at least 10 percent than the minimum-cost plan in the plan baseline.

```sql
SELECT apg_plan_mgmt.evolve_plan_baselines(
    sql_hash,
    plan_hash,
    1.1,
    'approve'
) FROM apg_plan_mgmt.dba_plans
WHERE status = 'Unapproved' AND enabled = true;
```

When the `apg_plan_mgmt.evolve_plan_baselines` function runs, it collects performance statistics and saves them in the `apg_plan_mgmt.dba_plans` view in the columns `planning_time_ms`, `execution_time_ms`, `cardinality_error`, `total_time_benefit_ms`, and `execution_time_benefit_ms`. The `apg_plan_mgmt.evolve_plan_baselines` function also updates the columns `last_verified` or `last_validated` timestamps, in which you can see the most recent time the performance statistics were collected.

```sql
SELECT sql_hash, plan_hash, status, last_verified, sql_text::varchar(40)
FROM apg_plan_mgmt.dba_plans
ORDER BY last_verified DESC;  -- value updated by evolve_plan_baselines()
```

For more information about verifying plans, see Evaluating plan performance (p. 1062).

Deleting plans

The optimizer deletes plans automatically if they have not been executed or chosen as the minimum-cost plan for the plan retention period. By default, the plan retention period is 32 days. To change the plan retention period, set the `apg_plan_mgmt.plan_retention_period` parameter.

You can also review the contents of the `apg_plan_mgmt.dba_plans` view and delete any plans you don’t want by using the `apg_plan_mgmt.delete_plan` function. For more information, see Deleting plans (p. 1065).

Best practices for query plan management

Consider using a plan management style that is either proactive or reactive. These plan management styles contrast in how and when new plans get approved for use.

Proactive plan management to help prevent performance regression

With proactive plan management, you manually approve new plans after you have verified that they are faster. Do this to prevent plan performance regressions. Follow these steps for proactive plan management:

1. In a development environment, identify the SQL statements that have the greatest impact on performance or system throughput. Then capture the plans for these statements as described
Examining plans in the dba_plans view

1. Manually capturing plans for specific SQL statements (p. 1058) and Automatically capturing plans (p. 1059).
2. Export the captured plans from the development environment and import them into the production environment. For more information, see Exporting and importing plans (p. 1065).
3. In production, run your application and enforce the use of approved managed plans. For more information, see Using managed plans (p. 1059). While the application runs, also add new plans as the optimizer discovers them. For more information, see Automatically capturing plans (p. 1059).
4. Analyze the unapproved plans and approve those that perform well. For more information, see Evaluating plan performance (p. 1062).
5. While your application continues to run, the optimizer begins to use the new plans as appropriate.

Reactive plan management to detect and repair performance regression

With reactive plan management, you monitor your application as it runs to detect plans that cause performance regressions. When you detect regressions, you manually reject or fix the bad plans. Follow these steps for reactive plan management:

1. While your application runs, enforce the use of managed plans and automatically add newly discovered plans as unapproved. For more information, see Using managed plans (p. 1059) and Automatically capturing plans (p. 1059).
3. When you discover a plan regression, set the plan's status to rejected. The next time the optimizer runs the SQL statement, it automatically ignores the rejected plan and uses a different approved plan instead. For more information, see Rejecting or disabling slower plans (p. 1063).

In some cases, you might prefer to fix a bad plan rather than reject, disable, or delete it. Use the pg_hint_plan extension to experiment with improving a plan. With pg_hint_plan, you use special comments to tell the optimizer to override how it normally creates a plan. For more information, see Fixing plans using pg_hint_plan (p. 1063).

Examining plans in the apg_plan_mgmt.dba_plans view

Query plan management provides a new SQL view for database administrators (DBAs) to use called apg_plan_mgmt.dba_plans. This one view contains the plan history for all of the databases in the DB instance.

This view contains the plan history for all of your managed statements. Each managed plan is identified by the combination of a SQL hash value and a plan hash value. With these identifiers, you can use tools such as Amazon RDS Performance Insights to track individual plan performance. For more information on Performance Insights, see Using Amazon RDS performance insights.

Note
Access to the apg_plan_mgmt.dba_plans view is restricted to users that hold the apg_plan_mgmt role.

Listing managed plans

To list the managed plans, use a SELECT statement on the apg_plan_mgmt.dba_plans view. The following example displays some columns in the dba_plans view such as the status, which identifies the approved and unapproved plans.
SELECT sql_hash, plan_hash, status, enabled, stmt_name
FROM apg_plan_mgmt.dba_plans;

<table>
<thead>
<tr>
<th>sql_hash</th>
<th>plan_hash</th>
<th>status</th>
<th>enabled</th>
<th>stmt_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1984047223</td>
<td>512153379</td>
<td>Approved</td>
<td>t</td>
<td>rangequery</td>
</tr>
<tr>
<td>1984047223</td>
<td>512284451</td>
<td>Unapproved</td>
<td>t</td>
<td>rangequery</td>
</tr>
</tbody>
</table>

(2 rows)

Reference for the `apg_plan_mgmt.dba_plans` view

The columns of plan information in the `apg_plan_mgmt.dba_plans` view include the following.

<table>
<thead>
<tr>
<th>dba_plans column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cardinality_error</td>
<td>A measure of the error between the estimated cardinality versus the actual cardinality. Cardinality is the number of table rows that the plan is to process. If the cardinality error is large, then it increases the likelihood that the plan isn't optimal. This column is populated by the <code>apg_plan_mgmt.evolve_plan_baselines</code> function.</td>
</tr>
<tr>
<td>compatibility_level</td>
<td>The feature level of the Aurora PostgreSQL optimizer.</td>
</tr>
<tr>
<td>created_by</td>
<td>The authenticated user (<code>session_user</code>) who created the plan.</td>
</tr>
<tr>
<td>enabled</td>
<td>An indicator of whether the plan is enabled or disabled. All plans are enabled by default. You can disable plans to prevent them from being used by the optimizer. To modify this value, use the <code>apg_plan_mgmt.set_plan_enabled</code> function.</td>
</tr>
<tr>
<td>environment_variables</td>
<td>The PostgreSQL Grand Unified Configuration (GUC) parameters and values that the optimizer has overridden at the time the plan was captured.</td>
</tr>
<tr>
<td>estimated_startup_cost</td>
<td>The estimated optimizer setup cost before the optimizer delivers rows of a table.</td>
</tr>
<tr>
<td>estimated_total_cost</td>
<td>The estimated optimizer cost to deliver the final table row.</td>
</tr>
<tr>
<td>execution_time_benefit_ms</td>
<td>The execution time benefit in milliseconds of enabling the plan. This column is populated by the <code>apg_plan_mgmt.evolve_plan_baselines</code> function.</td>
</tr>
<tr>
<td>execution_time_ms</td>
<td>The estimated time in milliseconds that the plan would run. This column is populated by the <code>apg_plan_mgmt.evolve_plan_baselines</code> function.</td>
</tr>
<tr>
<td>has_side_effects</td>
<td>A value that indicates that the SQL statement is a data manipulation language (DML) statement or a SELECT statement that contains a VOLATILE function.</td>
</tr>
<tr>
<td>last_used</td>
<td>This value is updated to the current date whenever the plan is either executed or when the plan is the query optimizer's minimum-cost plan. This value is stored in shared memory and periodically flushed to disk. To get the most up-to-date value, read the date from shared memory by calling the function <code>apg_plan_mgmt.plan_last_used</code> instead of reading the <code>last_used</code> value. For additional information, see the <code>apg_plan_mgmt.plan_retention_period</code> parameter.</td>
</tr>
<tr>
<td>last_validated</td>
<td>The most recent date and time when it was verified that the plan could be recreated by either the <code>apg_plan_mgmt.validate_plans</code> function or the <code>apg_plan_mgmt.evolve_plan_baselines</code> function.</td>
</tr>
</tbody>
</table>
### dba_plans column

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>last_verified</td>
<td>The most recent date and time when a plan was verified to be the best-performing plan for the specified parameters by the <code>apg_plan_mgmt.evolve_plan_baselines</code> function.</td>
</tr>
<tr>
<td>origin</td>
<td>How the plan was captured with the <code>apg_plan_mgmt.capture_plan_baselines</code> parameter. Valid values include the following:</td>
</tr>
<tr>
<td></td>
<td>M – The plan was captured with manual plan capture.</td>
</tr>
<tr>
<td></td>
<td>A – The plan was captured with automatic plan capture.</td>
</tr>
<tr>
<td>param_list</td>
<td>The parameter values that were passed to the statement if this is a prepared statement.</td>
</tr>
<tr>
<td>plan_created</td>
<td>The date and time the plan that was created.</td>
</tr>
<tr>
<td>plan_hash</td>
<td>The plan identifier. The combination of <code>plan_hash</code> and <code>sql_hash</code> uniquely identifies a specific plan.</td>
</tr>
<tr>
<td>plan_outline</td>
<td>A representation of the plan that is used to recreate the actual execution plan, and that is database-independent. Operators in the tree correspond to operators that appear in the EXPLAIN output.</td>
</tr>
<tr>
<td>planning_time_ms</td>
<td>The actual time to run the planner, in milliseconds. This column is populated by the <code>apg_plan_mgmt.evolve_plan_baselines</code> function.</td>
</tr>
<tr>
<td>queryId</td>
<td>A statement hash, as calculated by the <code>pg_stat_statements</code> extension. This isn't a stable or database-independent identifier because it depends on object identifiers (OIDs).</td>
</tr>
<tr>
<td>sql_hash</td>
<td>A hash value of the SQL statement text, normalized with literals removed.</td>
</tr>
<tr>
<td>sql_text</td>
<td>The full text of the SQL statement.</td>
</tr>
<tr>
<td>status</td>
<td>A plan's status, which determines how the optimizer uses a plan. Valid values include the following.</td>
</tr>
<tr>
<td></td>
<td>• Approved – A usable plan that the optimizer can choose to run. The optimizer runs the least-cost plan from a managed statement's set of approved plans (baseline). To reset a plan to approved, use the <code>apg_plan_mgmt.evolve_plan_baselines</code> function.</td>
</tr>
<tr>
<td></td>
<td>• Unapproved – A captured plan that you have not verified for use. For more information, see Evaluating plan performance (p. 1062).</td>
</tr>
<tr>
<td></td>
<td>• Rejected – A plan that the optimizer won't use. For more information, see Rejecting or disabling slower plans (p. 1063).</td>
</tr>
<tr>
<td></td>
<td>• Preferred – A plan that you have determined is a preferred plan to use for a managed statement.</td>
</tr>
<tr>
<td></td>
<td>If the optimizer's minimum-cost plan isn't an approved or preferred plan, you can reduce plan enforcement overhead. To do so, make a subset of the approved plans Preferred. When the optimizer's minimum cost isn't an Approved plan, a Preferred plan is chosen before an Approved plan.</td>
</tr>
<tr>
<td></td>
<td>To reset a plan to Preferred, use the <code>apg_plan_mgmt.set_plan_status</code> function.</td>
</tr>
</tbody>
</table>
### Capturing execution plans

You can capture execution plans for specific SQL statements by using manual plan capture. Alternatively, you can capture all (or the slowest) plans that are executed two or more times as your application runs by using automatic plan capture.

When capturing plans, the optimizer sets the status of a managed statement's first captured plan to approved. The optimizer sets the status of any additional plans captured for a managed statement to unapproved. However, more than one plan might occasionally be saved with the approved status. This can happen when multiple plans are created for a statement in parallel and before the first plan for the statement is committed.

To control the maximum number of plans that can be captured and stored in the `dba_plans` view, set the `apg_plan_mgmt.max_plans` parameter in your DB instance-level parameter group. A change to the `apg_plan_mgmt.max_plans` parameter requires a DB instance restart for a new value to take effect. For more information, see the `apg_plan_mgmt.max_plans` (p. 1067) parameter.

#### Topics
- Manually capturing plans for specific SQL statements (p. 1058)
- Automatically capturing plans (p. 1059)

### Manually capturing plans for specific SQL statements

If you have a known set of SQL statements to manage, put the statements into a SQL script file and then manually capture plans. The following shows a `psql` example of how to capture query plans manually for a set of SQL statements.

```
psql> SET apg_plan_mgmt.capture_plan_baselines = manual;
pql> \i my-statements.sql
psql> SET apg_plan_mgmt.capture_plan_baselines = off;
```

After capturing a plan for each SQL statement, the optimizer adds a new row to the `apg_plan_mgmt.dba_plans` view.

We recommend that you use either EXPLAIN or EXPLAIN EXECUTE statements in the SQL script file. Make sure that you include enough variations in parameter values to capture all the plans of interest.

If you know of a better plan than the optimizer's minimum cost plan, you might be able to force the optimizer to use the better plan. To do so, specify one or more optimizer hints. For more information, see Fixing plans using `pg_hint_plan` (p. 1063). To compare the performance of the unapproved and approved plans and approve, reject, or delete them, see Evaluating plan performance (p. 1062).

---

<table>
<thead>
<tr>
<th><code>dba_plans</code> column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stmt_name</td>
<td>The name of the SQL statement within a PREPARE statement. This value is an empty string for an unnamed prepared statement. This value is NULL for a nonprepared statement.</td>
</tr>
<tr>
<td>total_time_benefit</td>
<td>The total time benefit in milliseconds of enabling this plan. This value considers both planning time and execution time. If this value is negative, there is a disadvantage to enabling this plan. This column is populated by the <code>apg_plan_mgmt.evolve_plan_baselines</code> (p. 1071) function.</td>
</tr>
</tbody>
</table>
Automatically capturing plans

Use automatic plan capture for situations such as the following:

- You don’t know the specific SQL statements that you want to manage.
- You have hundreds or thousands of SQL statements to manage.
- Your application uses a client API. For example, JDBC uses unnamed prepared statements or bulk-mode statements that can’t be expressed in psql.

To capture plans automatically

1. Turn on automatic plan capture by setting `apg_plan_mgmt.capture_plan_baselines` to `automatic` in the DB instance-level parameter group. For more information, see Modifying parameters in a DB parameter group (p. 303).
2. Restart your DB instance.
3. As the application runs, the optimizer captures plans for each SQL statement that runs at least twice.

   As the application runs with default query plan management parameter settings, the optimizer captures plans for each SQL statement that runs at least twice. Capturing all plans while using the defaults has very little run-time overhead and can be enabled in production.

   You can modify some parameters to capture plans for statements that have the greatest impact on throughput, run the longest, or have the most volatile performance. However, this extended mode of automatic plan capture has a noticeable performance overhead.

To turn off automatic plan capture

- Set the `apg_plan_mgmt.capture_plan_baselines` parameter to `off` from the DB instance-level parameter group.

To measure the performance of the unapproved plans and approve, reject, or delete them, see Evaluating plan performance (p. 1062).

Using managed plans

To get the optimizer to use captured plans for your managed statements, set the parameter `apg_plan_mgmt.use_plan_baselines` to `true`. The following is a local instance example.

```
SET apg_plan_mgmt.use_plan_baselines = true;
```

While the application runs, this setting causes the optimizer to use the minimum-cost, preferred, or approved plan that is valid and enabled, for each managed statement.

How the optimizer chooses which plan to run

The cost of an execution plan is an estimate that the optimizer makes to compare different plans. Optimizer cost is a function of several factors that include the CPU and I/O operations that the plan uses. For more information about PostgreSQL query planner costs, see the PostgreSQL documentation on query planning.

The following flowchart shows how the query plan management optimizer chooses which plan to run.
The flow is as follows:

1. When the optimizer processes every SQL statement, it generates a minimum-cost plan.
2. Without query plan management, the optimizer simply runs its generated plan. The optimizer uses query plan management if you set one or both of the following parameter settings:
• `apg_plan_mgmt.capture_plan_baselines` to `manual` or `automatic`
• `apg_plan_mgmt.use_plan_baselines` to `true`

3. The optimizer immediately runs the generated plan if the following are both true:
   • The optimizer's plan is already in the `apg_plan_mgmt.dba_plans` view for the SQL statement.
   • The plan's status is either approved or preferred.

4. The optimizer goes through the capture plan processing if the parameter `apg_plan_mgmt.capture_plan_baselines` is `manual` or `automatic`.

   For details on how the optimizer captures plans, see Capturing execution plans (p. 1058).

5. The optimizer runs the generated plan if `apg_plan_mgmt.use_plan_baselines` is `false`.

6. If the optimizer's plan isn't in the `apg_plan_mgmt.dba_plans` view, the optimizer captures the plan as a new unapproved plan.

7. The optimizer runs the generated plan if the following are both true:
   • The optimizer's plan isn't a rejected or disabled plan.
   • The plan's total cost is less than the unapproved execution plan threshold.

   The optimizer doesn't run disabled plans or any plans that have the rejected status. In most cases, the optimizer doesn't execute unapproved plans. However, the optimizer runs an unapproved plan if you set a value for the parameter `apg_plan_mgmt.unapproved_plan_execution_threshold` and the plan's total cost is less than the threshold. For more information, see the `apg_plan_mgmt.unapproved_plan_execution_threshold` (p. 1069) parameter.

8. If the managed statement has any enabled and valid preferred plans, the optimizer runs the minimum-cost one.

   A valid plan is one that the optimizer can run. Managed plans can become invalid for various reasons. For example, plans become invalid when objects that they depend on are removed, such as an index or a partition of a partitioned table.

9. The optimizer determines the minimum-cost plan from the managed statement's approved plans that are both enabled and valid. The optimizer then runs the minimum-cost approved plan.

**Analyzing which plan the optimizer will use**

When the `apg_plan_mgmt.use_plan_baselines` parameter is set to `true`, you can use EXPLAIN ANALYZE SQL statements to cause the optimizer to show the plan it would use if it were to run the statement. The following is an example.

```
EXPLAIN ANALYZE EXECUTE rangeQuery (1,10000);
```

```
<table>
<thead>
<tr>
<th>QUERY PLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Note: An Approved plan was used instead of the minimum cost plan.</td>
</tr>
<tr>
<td>SQL Hash: 1984047223, Plan Hash: 512153379</td>
</tr>
</tbody>
</table>
```

The optimizer indicates which plan it will run, but notice that in this example that it found a lower-cost plan. In this case, you capture this new minimum cost plan by turning on automatic plan capture as described in Automatically capturing plans (p. 1059).
Maintaining execution plans

Query plan management provides techniques and functions to add, maintain, and improve execution plans.

Topics

- Evaluating plan performance (p. 1062)
- Validating plans (p. 1063)
- Fixing plans using pg_hint_plan (p. 1063)
- Deleting plans (p. 1065)
- Exporting and importing plans (p. 1065)

Evaluating plan performance

After the optimizer captures plans as unapproved, use the `apg_plan_mgmt.evolve_plan_baselines` function to compare plans based on their actual performance. Depending on the outcome of your performance experiments, you can change a plan's status from unapproved to either approved or rejected. You can instead decide to use the `apg_plan_mgmt.evolve_plan_baselines` function to temporarily disable a plan if it does not meet your requirements.

Topics

- Approving better plans (p. 1062)
- Rejecting or disabling slower plans (p. 1063)

Approving better plans

The following example demonstrates how to change the status of managed plans to approved using the `apg_plan_mgmt.evolve_plan_baselines` function.

```
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)
```

The output shows a performance report for the `rangequery` statement with parameter bindings of 1 and 10,000. The new unapproved plan (`Baseline+1`) is better than the best previously approved plan (`Baseline`). To confirm that the new plan is now Approved, check the `apg_plan_mgmt.dba_plans` view.
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)

The managed plan now includes two approved plans that are the statement's plan baseline. You can also call the `apg_plan_mgmt.set_plan_status` function to directly set a plan's status field to 'Approved', 'Rejected', 'Unapproved', or 'Preferred'.

**Rejecting or disabling slower plans**

To reject or disable plans, pass 'reject' or 'disable' as the action parameter to the `apg_plan_mgmt.evolve_plan_baselines` function. This example disables any captured Unapproved plan that is slower by at least 10 percent than the best Approved plan for the statement.

```sql
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
```

You can also directly set a plan to rejected or disabled. To directly set a plan's enabled field to true or false, call the `apg_plan_mgmt.set_plan_enabled` function. To directly set a plan's status field to 'Approved', 'Rejected', 'Unapproved', or 'Preferred', call the `apg_plan_mgmt.set_plan_status` function.

**Validating plans**

Use the `apg_plan_mgmt.validate_plans` function to delete or disable plans that are invalid.

Plans can become invalid or stale when objects that they depend on are removed, such as an index or a table. However, a plan might be invalid only temporarily if the removed object gets recreated. If an invalid plan can become valid later, you might prefer to disable an invalid plan or do nothing rather than delete it.

To find and delete all plans that are invalid and haven't been used in the past week, use the `apg_plan_mgmt.validate_plans` function as follows.

```sql
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');
```

To enable or disabled a plan directly, use the `apg_plan_mgmt.set_plan_enabled` function.

**Fixing plans using pg_hint_plan**

The query optimizer is well-designed to find an optimal plan for all statements, and in most cases the optimizer finds a good plan. However, occasionally you might know that a much better plan exists than that generated by the optimizer. Two recommended ways to get the optimizer to generate a desired plan include using the `pg_hint_plan` extension or setting Grand Unified Configuration (GUC) variables in PostgreSQL:
• **pg_hint_plan extension** – Specify a "hint" to modify how the planner works by using PostgreSQL’s pg_hint_plan extension. To install and learn more about how to use the pg_hint_plan extension, see the pg_hint_plan documentation.

• **GUC variables** – Override one or more cost model parameters or other optimizer parameters, such as the \texttt{from\_collapse\_limit} or \texttt{GEQO\_threshold}.

When you use one of these techniques to force the query optimizer to use a plan, you can also use query plan management to capture and enforce use of the new plan.

You can use the pg_hint_plan extension to change the join order, the join methods, or the access paths for a SQL statement. You use a SQL comment with special pg_hint_plan syntax to modify how the optimizer creates a plan. For example, assume the problem SQL statement has a two-way join.

```sql
SELECT *
FROM t1, t2
WHERE t1.id = t2.id;
```

Then suppose that the optimizer chooses the join order (t1, t2), but we know that the join order (t2, t1) is faster. The following hint forces the optimizer to use the faster join order, (t2, t1). Include \texttt{EXPLAIN} so that the optimizer generates a plan for the SQL statement but does not run the statement. (Output not shown.)

```sql
/*+ Leading ((t2 t1)) */ EXPLAIN SELECT *
FROM t1, t2
WHERE t1.id = t2.id;
```

The following steps show how to use pg_hint_plan.

**To modify the optimizer's generated plan and capture the plan using pg_hint_plan**

1. Turn on the manual capture mode.

   ```sql
   SET apg_plan_mgmt.capture_plan_baselines = manual;
   ```

2. Specify a hint for the SQL statement of interest.

   ```sql
   /*+ Leading ((t2 t1)) */ */ EXPLAIN SELECT *
   FROM t1, t2
   WHERE t1.id = t2.id;
   ```

   After this runs, the optimizer captures the plan in the apg_plan_mgmt.dba_plans view. The captured plan doesn't include the special pg_hint_plan comment syntax because query plan management normalizes the statement by removing leading comments.

3. View the managed plans by using the apg_plan_mgmt.dba_plans view.

   ```sql
   SELECT sql_hash, plan_hash, status, sql_text, plan_outline
   FROM apg_plan_mgmt.dba_plans;
   ```

4. Set the status of the plan to Preferred. Doing so makes sure that the optimizer chooses to run it, instead of selecting from the set of approved plans, when the minimum-cost plan isn't already Approved or Preferred.

   ```sql
   SELECT apg_plan_mgmt.set_plan_status(<sql-hash>, <plan-hash>, 'preferred' );
   ```

5. Turn off manual plan capture and enforce the use of managed plans.
SET apg_plan_mgmt.capture_plan_baselines = false;
SET apg_plan_mgmt.use_plan_baselines = true;

Now, when the original SQL statement runs, the optimizer chooses either an Approved or Preferred plan. If the minimum-cost plan isn't Approved or Preferred, then the optimizer chooses the Preferred plan.

Deleting plans

Delete plans that have not been used for a long time or that are no longer relevant. Each plan has a last_used date that the optimizer updates each time it executes a plan or picks it as the minimum-cost plan for a statement. Use the last_used date to determine if a plan has been used recently and is still relevant.

For example, you can use the apg_plan_mgmt.delete_plan function as follows. Doing this deletes all plans that haven't been chosen as the minimum-cost plan or haven't run in at least 31 days. However, this example doesn't delete plans that have been explicitly rejected.

```
SELECT SUM(apg_plan_mgmt.delete_plan(sql_hash, plan_hash))
FROM apg_plan_mgmt.dba_plans
WHERE last_used < (current_date - interval '31 days')
AND status <> 'Rejected';
```

To delete any plan that is no longer valid and that you expect not to become valid again, use the apg_plan_mgmt.validate_plans function. For more information, see Validating plans (p. 1063).

You can implement your own policy for deleting plans. Plans are automatically deleted when the current date last_used is greater than the value of the apg_plan_mgmt.plan_retention_period parameter, which defaults to 32 days. You can specify a longer interval, or you can implement your own plan retention policy by calling the delete_plan function directly.

**Important**

If you don't clean up plans, you might eventually run out of shared memory that is set aside for query plan management. To control how much memory is available for managed plans, use the apg_plan_mgmt.max_plans parameter. Set this parameter in your DB instance-level parameter group and restart your DB instance for changes to take effect. For more information, see the apg_plan_mgmt.max_plans (p. 1067) parameter.

Exporting and importing plans

You can export your managed plans and import them into another DB instance.

**To export managed plans**

An authorized user can copy any subset of the apg_plan_mgmt.plans table to another table, and then save it using the pg_dump command. The following is an example.

```
CREATE TABLE plans_copy AS SELECT *
FROM apg_plan_mgmt.plans [ WHERE predicates ] ;
% pg_dump --table apg_plan_mgmt.plans_copy -Pt mysourcedatabase > plans_copy.tar
DROP TABLE apg_plan_mgmt.plans_copy;
```

**To import managed plans**

1. Copy the .tar file of the exported managed plans to the system where the plans are to be restored.
2. Use the `pg_restore` command to copy the tar file into a new table.

   ```
   % pg_restore --dbname mytargetdatabase -Ft plans_copy.tar
   ```

3. Merge the `plans_copy` table with the `apg_plan_mgmt.plans` table, as shown in the following example.

   **Note**
   In some cases, you might dump from one version of the `apg_plan_mgmt` extension and restore into a different version. In these cases, the columns in the plans table might be different. If so, name the columns explicitly instead of using `SELECT *`.

   ```
   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_timeBenefit_ms = EXCLUDED.total_timeBenefit_ms,
   execution_timeBenefit_ms = EXCLUDED.execution_timeBenefit_ms;
   ```

4. Reload the managed plans into shared memory and remove the temporary plans table.

   ```
   SELECT apg_plan_mgmt.reload(); -- refresh shared memory
   DROP TABLE plans_copy;
   ```

---

**Parameter reference for query plan management**

The `apg_plan_mgmt` extension provides the following parameters.

**Parameters**

- `apg_plan_mgmt.capture_plan_baselines` (p. 1067)
- `apg_plan_mgmt.max_databases` (p. 1067)
- `apg_plan_mgmt.max_plans` (p. 1067)
- `apg_plan_mgmt.pgss_min_calls` (p. 1067)
- `apg_plan_mgmt.pgss_min_mean_time_ms` (p. 1068)
- `apg_plan_mgmt.pgss_min_stddev_time_ms` (p. 1068)
- `apg_plan_mgmt.pgss_min_total_time_ms` (p. 1068)
- `apg_plan_mgmt.plan_retention_period` (p. 1069)
- `apg_plan_mgmt.unapproved_plan_execution_threshold` (p. 1069)
- `apg_plan_mgmt.use_plan_baselines` (p. 1069)

Set the query plan management parameters at the appropriate level:

- Set at the cluster-level to provide the same settings for all DB instances. For more information, see [Modifying parameters in a DB cluster parameter group](p. 305).
• Set at the DB instance level to isolate the settings to an individual DB instance. For more information, see Modifying parameters in a DB parameter group (p. 303).
• Set in a specific client session such as in psql, to isolate the values to only that session.

You must be set the parameters `apg_plan_mgmt.max_databases` and `apg_plan_mgmt.max_plans` at the cluster or DB instance level.

### `apg_plan_mgmt.capture_plan_baselines`

Enable execution plan capture for SQL statements.

```sql
SET apg_plan_mgmt.capture_plan_baselines = [off | automatic | manual]
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Disable plan capture. This is the default.</td>
</tr>
<tr>
<td>automatic</td>
<td>Enable plan capture for subsequent SQL statements that satisfy the eligibility criteria.</td>
</tr>
<tr>
<td>manual</td>
<td>Enable plan capture for subsequent SQL statements.</td>
</tr>
</tbody>
</table>

### `apg_plan_mgmt.max_databases`

Sets the maximum number of database objects that might use query plan management. A database object is what gets created with the `CREATE DATABASE` SQL statement.

**Important**

Set `apg_plan_mgmt.max_databases` at the cluster or DB instance level. It requires a DB instance restart for a new value to take effect.

<table>
<thead>
<tr>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive integer</td>
<td>10</td>
<td>A positive integer value.</td>
</tr>
</tbody>
</table>

### `apg_plan_mgmt.max_plans`

Sets the maximum number of plans that might be captured in the `apg_plan_mgmt.dba_plans` view.

**Important**

Set `apg_plan_mgmt.max_plans` at the cluster or DB instance level. It requires a DB instance restart for a new value to take effect.

<table>
<thead>
<tr>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>integer</td>
<td>1000</td>
<td>A positive integer value greater or equal to 10.</td>
</tr>
</tbody>
</table>

### `apg_plan_mgmt.pgss_min_calls`

This parameter has been deprecated.
Sets the minimum number of `pg_stat_statements` calls that are eligible for plan capture.

```
SET apg_plan_mgmt.pgss_min_calls = integer-value;
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive integer</td>
<td>2</td>
<td>A positive integer value greater or equal to 2.</td>
</tr>
</tbody>
</table>

**Usage notes**

Requires installation of the `pg_stat_statements` extension. For more information, see the PostgreSQL `pg_stats_statements` documentation.

**apg_plan_mgmt.pgss_min_mean_time_ms**

This parameter has been deprecated.

Minimum value of the `pg_stat_statements` `mean_time` to be eligible for plan capture.

```
SET apg_plan_mgmt.pgss_min_mean_time_ms = double-value;
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive number</td>
<td>0.0</td>
<td>A positive number value greater or equal to 0.0.</td>
</tr>
</tbody>
</table>

**Usage notes**

Requires installation of the `pg_stat_statements` extension. For more information, see the PostgreSQL `pg_stats_statements` documentation.

**apg_plan_mgmt.pgss_min_stddev_time_ms**

This parameter has been deprecated.

Minimum value of the `pg_stat_statements` `stddev_time` to be eligible for plan capture.

```
SET apg_plan_mgmt.pgss_min_stddev_time_ms = double-value;
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive number</td>
<td>0.0</td>
<td>A positive number value greater or equal to 0.0.</td>
</tr>
</tbody>
</table>

**Usage notes**

Requires installation of the `pg_stat_statements` extension. For more information, see the PostgreSQL `pg_stats_statements` documentation.

**apg_plan_mgmt.pgss_min_total_time_ms**

This parameter has been deprecated.
Minimum value of the `pg_stat_statements` `total_time` to be eligible for plan capture.

```
SET apg_plan_mgmt.pgss_min_total_time_ms = double-value;
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive number</td>
<td>0.0</td>
<td>A positive number value greater or equal to 0.0.</td>
</tr>
</tbody>
</table>

**Usage notes**

Requires installation of the `pg_stat_statements` extension. For more information, see the PostgreSQL `pg_stats_statements` documentation.

**apg_plan_mgmt.plan_retention_period**

The number of days plans are kept in the `apg_plan_mgmt.dba_plans` view before being automatically deleted. A plan is deleted when the current date is this many days since the plan's `last_used` date.

```
SET apg_plan_mgmt.plan_retention_period = integer-value;
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive integer</td>
<td>32</td>
<td>A positive integer value greater or equal to 32, representing days.</td>
</tr>
</tbody>
</table>

**apg_plan_mgmt.unapproved_plan_execution_threshold**

An estimated total plan cost threshold, below which the optimizer runs an unapproved plan. By default, the optimizer does not run unapproved plans. However, you can set an execution threshold for your fastest unapproved plans. With this setting, the optimizer bypasses the overhead of enforcing only approved plans.

```
SET apg_plan_mgmt.unapproved_plan_execution_threshold = integer-value;
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive integer</td>
<td>0</td>
<td>A positive integer value greater or equal to 0. A value of 0 means no unapproved plans run when <code>use_plan_baselines</code> is <code>true</code>.</td>
</tr>
</tbody>
</table>

With the following example, the optimizer runs an unapproved plan if the estimated cost is less than 550, even if `use_plan_baselines` is `true`.

```
SET apg_plan_mgmt.unapproved_plan_execution_threshold = 550;
```

**apg_plan_mgmt.use_plan_baselines**

Enforce the optimizer to use managed plans for managed statements.

```
SET apg_plan_mgmt.use_plan_baselines = [true | false];
```
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| true  | Enforce the use of managed plans. When a SQL statement runs and it is a managed statement in the `apg_plan_mgmt.dba_plans` view, the optimizer chooses a managed plan in the following order.  
1. The minimum-cost preferred plan that is valid and enabled.  
2. The minimum cost approved plan that is valid and enabled.  
3. The minimum cost unapproved plan that is valid, enabled, and that meets the threshold, if set with the `apg_plan_mgmt.unapproved_plan_execution_threshold` parameter.  
4. The optimizer's generated minimum-cost plan. |
| false | (Default) Do not use managed plans. The optimizer uses its generated minimum-cost plan. |

**Usage notes**

When `use_plan_baselines` is true, then the optimizer makes the following execution decisions:

1. If the estimated cost of the optimizer’s plan is below the `unapproved_plan_execution_threshold`, then execute it, else
2. If the plan is approved or preferred, then execute it, else
3. Execute a minimum-cost preferred plan, if possible, else
4. Execute a minimum-cost approved plan, if possible, else
5. Execute the optimizer's minimum-cost plan.

**Function reference for query plan management**

The `apg_plan_mgmt` extension provides the following functions.

**Functions**

- `apg_plan_mgmt.delete_plan (p. 1070)`
- `apg_plan_mgmt.evolve_plan_baselines (p. 1071)`
- `apg_plan_mgmt.plan_last_used (p. 1072)`
- `apg_plan_mgmt.reload (p. 1073)`
- `apg_plan_mgmt.set_plan_enabled (p. 1073)`
- `apg_plan_mgmt.set_plan_status (p. 1074)`
- `apg_plan_mgmt.validate_plans (p. 1074)`

**apg_plan_mgmt.delete_plan**

Delete a managed plan.

**Syntax**

```sql
apg_plan_mgmt.delete_plan(
    sql_hash,
    plan_hash
)
```
Return value

Returns 0 if the delete was successful or -1 if the delete failed.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_hash</td>
<td>The sql_hash ID of the plan's managed SQL statement.</td>
</tr>
<tr>
<td>plan_hash</td>
<td>The managed plan's plan_hash ID.</td>
</tr>
</tbody>
</table>

apg_plan_mgmt.evolve_plan_baselines

Verifies whether an already approved plan is faster or whether a plan identified by the query optimizer as a minimum cost plan is faster.

Syntax

```
apg_plan_mgmt.evolve_plan_baselines(
    sql_hash,
    plan_hash,
    min_speedup_factor,
    action
)
```

Return value

The number of plans that were not faster than the best approved plan.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_hash</td>
<td>The sql_hash ID of the plan's managed SQL statement.</td>
</tr>
<tr>
<td>plan_hash</td>
<td>The managed plan's plan_hash ID. Use NULL to mean all plans that have the same sql_hash ID value.</td>
</tr>
<tr>
<td>min_speedup_factor</td>
<td>The minimum speedup factor can be the number of times faster that a plan must be than the best of the already approved plans to approve it. Alternatively, this factor can be the number of times slower that a plan must be to reject or disable it. This is a positive float value.</td>
</tr>
<tr>
<td>action</td>
<td>The action the function is to perform. Valid values include the following. Case does not matter.</td>
</tr>
<tr>
<td></td>
<td>• 'disable' -- Disable each matching plan that does not meet the minimum speedup factor.</td>
</tr>
<tr>
<td></td>
<td>• 'approve' -- Enable each matching plan that meets the minimum speedup factor and set its status to approved.</td>
</tr>
<tr>
<td></td>
<td>• 'reject' -- For each matching plan that does not meet the minimum speedup factor, set its status to rejected.</td>
</tr>
</tbody>
</table>
### Parameter Description

- **NULL** – The function simply returns the number of plans that have no performance benefit because they do not meet the minimum speedup factor.

### Usage notes

Set specified plans to approved, rejected, or disabled based on whether the planning plus execution time is faster than the best approved plan by a factor that you can set. The action parameter might be set to 'approve' or 'reject' to automatically approve or reject a plan that meets the performance criteria. Alternatively, it might be set to '' (empty string) to do the performance experiment and produce a report, but take no action.

You can avoid pointlessly rerunning of the `apg_plan_mgmt.evolve_plan_baselines` function for a plan on which it was recently run. To do so, restrict the plans to just the recently created unapproved plans. Alternatively, you can avoid running the `apg_plan_mgmt.evolve_plan_baselines` function on any approved plan that has a recent `last_verified` timestamp.

Conduct a performance experiment to compare the planning plus execution time of each plan relative to the other plans in the baseline. In some cases, there is only one plan for a statement and the plan is approved. In such a case, compare the planning plus execution time of the plan to the planning plus execution time of using no plan.

The incremental benefit (or disadvantage) of each plan is recorded in the `apg_plan_mgmt.dba_plans` view in the `total_time_benefit_ms` column. When this value is positive, there is a measurable performance advantage to including this plan in the baseline.

In addition to collecting the planning and execution time of each candidate plan, the `last_verified` column of the `apg_plan_mgmt.dba_plans` view is updated with the `current_timestamp`. The `last_verified` timestamp might be used to avoid running this function again on a plan that recently had its performance verified.

### `apg_plan_mgmt.plan_last_used`

Returns the `last_used` date of the specified plan from shared memory.

#### Note

The value in shared memory is always current on the read/write node. The value is only periodically flushed to the `last_used` column of the `apg_plan_mgmt.dba_plans` view.

#### Syntax

```sql
apg_plan_mgmt.plan_last_used(
    sql_hash,
    plan_hash
)
```

#### Return value

Returns the `last_used` date.

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_hash</td>
<td>The <code>sql_hash</code> ID of the plan's managed SQL statement.</td>
</tr>
</tbody>
</table>
### apg_plan_mgmt.reload

Reload plans into shared memory from the `apg_plan_mgmt.dba_plans` view.

**Syntax**

```sql
apg_plan_mgmt.reload()
```

**Return value**

None.

**Parameters**

None.

**Usage notes**

Call `reload` for the following situations:

- Use it to refresh the shared memory of a read-only replica immediately, rather than wait for new plans to propagate to the replica.
- Use it after importing managed plans.

### apg_plan_mgmt.set_plan_enabled

Enable or disable a managed plan.

**Syntax**

```sql
apg_plan_mgmt.set_plan_enabled(
    sql_hash,
    plan_hash,
    [true | false]
)
```

**Return value**

Returns 0 if the setting was successful or -1 if the setting failed.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_hash</td>
<td>The <code>sql_hash</code> ID of the plan’s managed SQL statement.</td>
</tr>
<tr>
<td>plan_hash</td>
<td>The managed plan’s <code>plan_hash</code> ID.</td>
</tr>
<tr>
<td>enabled</td>
<td>Boolean value of true or false:</td>
</tr>
<tr>
<td></td>
<td>• A value of <code>true</code> enables the plan.</td>
</tr>
<tr>
<td></td>
<td>• A value of <code>false</code> disables the plan.</td>
</tr>
</tbody>
</table>
**apg_plan_mgmt.set_plan_status**

Set a managed plan's status to Approved, Unapproved, Rejected, or Preferred.

**Syntax**

```
apg_plan_mgmt.set_plan_status(
    sql_hash,  
    plan_hash,  
    status
)
```

**Return value**

Returns 0 if the setting was successful or -1 if the setting failed.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_hash</td>
<td>The sql_hash ID of the plan's managed SQL statement.</td>
</tr>
<tr>
<td>plan_hash</td>
<td>The managed plan's plan_hash ID.</td>
</tr>
</tbody>
</table>
| status    | A string with one of the following values:  
  • Approved  
  • Unapproved  
  • Rejected  
  • Preferred  

The case you use does not matter, however the status value is set to initial uppercase in the `apg_plan_mgmt.dba_plans` view. For more information about these values, see status in Reference for the `apg_plan_mgmt.dba_plans` view (p. 1056).

**apg_plan_mgmt.validate_plans**

Validate that the optimizer can still recreate plans. The optimizer validates Approved, Unapproved, and Preferred plans, whether the plan is enabled or disabled. Rejected plans are not validated. Optionally, you can use the `apg_plan_mgmt.validate_plans` function to delete or disable invalid plans.

**Syntax**

```
apg_plan_mgmt.validate_plans(
    sql_hash,  
    plan_hash,  
    action
)
```

```
apg_plan_mgmt.validate_plans(
    action
)
```

**Return value**
The number of invalid plans.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_hash</td>
<td>The sql_hash ID of the plan’s managed SQL statement.</td>
</tr>
<tr>
<td>plan_hash</td>
<td>The managed plan’s plan_hash ID. Use NULL to mean all plans for the same sql_hash ID value.</td>
</tr>
<tr>
<td>action</td>
<td>The action the function is to perform for invalid plans. Valid string values include the following. Case does not matter.</td>
</tr>
<tr>
<td></td>
<td>‘disable’ – Each invalid plan is disabled.</td>
</tr>
<tr>
<td></td>
<td>‘delete’ – Each invalid plan is deleted.</td>
</tr>
<tr>
<td></td>
<td>NULL – The function simply returns the number of invalid plans. No other action is performed.</td>
</tr>
<tr>
<td></td>
<td>‘’ – An empty string produces a message indicating the number of both valid and invalid plans.</td>
</tr>
<tr>
<td></td>
<td>Any other value is treated like the empty string.</td>
</tr>
</tbody>
</table>

**Usage notes**

Use the form `validate_plans(action)` to validate all the managed plans for all the managed statements in the entire `apg_plan_mgmt.dba_plans` view.

Use the form `validate_plans(sql_hash, plan_hash, action)` to validate a managed plan specified with plan_hash, for a managed statement specified with sql_hash.

Use the form `validate_plans(sql_hash, NULL, action)` to validate all the managed plans for the managed statement specified with sql_hash.

---

**Publishing Aurora PostgreSQL logs to Amazon CloudWatch Logs**

You can configure your Aurora PostgreSQL DB cluster to publish log data to a log group in Amazon CloudWatch Logs. With CloudWatch Logs, you can perform real-time analysis of the log data, and use CloudWatch to create alarms and view metrics. You can use CloudWatch Logs to store your log records in highly durable storage.

**Note**

Be aware of the following:

- Aurora PostgreSQL supports publishing logs to CloudWatch Logs for versions 9.6.12 (and later); versions 10.7 (and later); and versions 11.6 (and later).
- From Aurora PostgreSQL, only postgresql logs can be published. Publishing upgrade logs isn't supported.
- If exporting log data is disabled, Aurora doesn't delete existing log groups or log streams.
- If exporting log data is disabled, existing log data remains available in CloudWatch Logs, depending on log retention, and you still incur charges for stored audit log data. You can...
delete log streams and log groups using the CloudWatch Logs console, the AWS CLI, or the CloudWatch Logs API.

- If you don’t want to export audit logs to CloudWatch Logs, make sure that all methods of exporting audit logs are disabled. These methods are the AWS Management Console, the AWS CLI, and the RDS API.

**Console**

You can publish Aurora PostgreSQL logs to CloudWatch Logs with the console.

**To publish Aurora PostgreSQL logs from the console**

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. Choose the Aurora PostgreSQL DB cluster that you want to publish the log data for.
4. Choose **Modify**.
5. In the **Log exports** section, choose **Postgresql log**.
6. Choose **Continue**, and then choose **Modify cluster** on the summary page.

**AWS CLI**

You can publish Aurora PostgreSQL logs with the AWS CLI. You can run the `modify-db-cluster` AWS CLI command with the following options:

- `--db-cluster-identifier`—The DB cluster identifier.
- `--cloudwatch-logs-export-configuration`—The configuration setting for the log types to be enabled for export to CloudWatch Logs for the DB cluster.

You can also publish Aurora PostgreSQL logs by running one of the following AWS CLI commands:

- `create-db-cluster`
- `restore-db-cluster-from-s3`
- `restore-db-cluster-from-snapshot`
- `restore-db-cluster-to-point-in-time`

Run one of these AWS CLI commands with the following options:

- `--db-cluster-identifier`—The DB cluster identifier.
- `--engine`—The database engine.
- `--enable-cloudwatch-logs-exports`—The configuration setting for the log types to be enabled for export to CloudWatch Logs for the DB cluster.

Other options might be required depending on the AWS CLI command that you run.

**Example**

The following command creates an Aurora PostgreSQL DB cluster to publish log files to CloudWatch Logs.

For Linux, macOS, or Unix:
Publishing Aurora PostgreSQL logs to CloudWatch Logs

Example

The following command modifies an existing Aurora PostgreSQL DB cluster to publish log files to CloudWatch Logs. The `--cloudwatch-logs-export-configuration` value is a JSON object. The key for this object is `EnableLogTypes`, and its value is `postgresql`.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster \
   --db-cluster-identifier my-db-cluster \
   --cloudwatch-logs-export-configuration '{"EnableLogTypes": ["postgresql"]}'
```

For Windows:

```bash
aws rds modify-db-cluster ^
   --db-cluster-identifier my-db-cluster ^
   --cloudwatch-logs-export-configuration '{"EnableLogTypes": ["postgresql"]}'
```

Note

When using the Windows command prompt, you must escape double quotes ("" in JSON code by prefixing them with a backslash (\).

Example

The following example modifies an existing Aurora PostgreSQL DB cluster to disable publishing log files to CloudWatch Logs. The `--cloudwatch-logs-export-configuration` value is a JSON object. The key for this object is `DisableLogTypes`, and its value is `postgresql`.

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster \
   --db-cluster-identifier mydbinstance \
   --cloudwatch-logs-export-configuration '{"DisableLogTypes": ["postgresql"]}'
```

For Windows:

```bash
aws rds modify-db-cluster ^
   --db-cluster-identifier mydbinstance ^
   --cloudwatch-logs-export-configuration "{"DisableLogTypes": ["postgresql"]}"
```

Note

When using the Windows command prompt, you must escape double quotes ("" in JSON code by prefixing them with a backslash (\).
RDS API

You can publish Aurora PostgreSQL logs with the RDS API. You can run the ModifyDBCluster action with the following options:

- `DBClusterIdentifier`—The DB cluster identifier.
- `CloudwatchLogsExportConfiguration`—The configuration setting for the log types to be enabled for export to CloudWatch Logs for the DB cluster.

You can also publish Aurora PostgreSQL logs with the RDS API by running one of the following RDS API actions:

- `CreateDBCluster`
- `RestoreDBClusterFromS3`
- `RestoreDBClusterFromSnapshot`
- `RestoreDBClusterToPointInTime`

Run the RDS API action with the following parameters:

- `DBClusterIdentifier`—The DB cluster identifier.
- `Engine`—The database engine.
- `EnableCloudwatchLogsExports`—The configuration setting for the log types to be enabled for export to CloudWatch Logs for the DB cluster.

Other parameters might be required depending on the AWS CLI command that you run.

Monitoring log events in Amazon CloudWatch

After enabling Aurora PostgreSQL log events, you can monitor the events in Amazon CloudWatch Logs. For more information about monitoring, see View log data sent to CloudWatch Logs.

A new log group is automatically created for the Aurora DB cluster under the following prefix, in which `cluster-name` represents the DB cluster name, and `log_type` represents the log type.

```
/aws/rds/cluster/cluster-name/log_type
```

For example, if you configure the export function to include the postgresql log for a DB cluster named `my-db-cluster`, PostgreSQL log data is stored in the `/aws/rds/cluster/my-db-cluster/postgresql` log group.

All of the events from all of the DB instances in a DB cluster are pushed to a log group using different log streams.

If a log group with the specified name exists, Aurora uses that log group to export log data for the Aurora DB cluster. You can use automated configuration, such as AWS CloudFormation, to create log groups with predefined log retention periods, metric filters, and customer access. Otherwise, a new log group is automatically created using the default log retention period, **Never Expire**, in CloudWatch Logs. You can use the CloudWatch Logs console, the AWS CLI, or the CloudWatch Logs API to change the log retention period. For more information about changing log retention periods in CloudWatch Logs, see Change log data retention in CloudWatch Logs.

You can use the CloudWatch Logs console, the AWS CLI, or the CloudWatch Logs API to search for information within the log events for a DB cluster. For more information about searching and filtering log data, see Searching and filtering log data.
Using machine learning (ML) with Aurora PostgreSQL

Amazon Aurora machine learning enables you to add machine learning–based predictions to database applications using the SQL language. Aurora machine learning uses a highly optimized integration between the Aurora database and the AWS machine learning (ML) services SageMaker and Amazon Comprehend.

Benefits of Aurora machine learning include the following:

- You can add ML-based predictions to your existing database applications. You don't need to build custom integrations or learn separate tools. You can embed machine learning processing directly into your SQL query as calls to functions.
- The ML integration is a fast way to enable ML services to work with transactional data. You don't have to move the data out of the database to perform the machine learning operations. You don't have to convert or reimport the results of the machine learning operations to use them in your database application.
- You can use your existing governance policies to control who has access to the underlying data and to the generated insights.

AWS machine learning services are managed services that you set up and run in their own production environments. Currently, Aurora Machine Learning integrates with Amazon Comprehend for sentiment analysis and SageMaker for a wide variety of ML algorithms.

For general information about Amazon Comprehend, see Amazon Comprehend. For details about using Aurora and Amazon Comprehend together, see Using Amazon Comprehend for natural language processing (p. 1082).

For general information about SageMaker, see SageMaker. For details about using Aurora and SageMaker together, see Using SageMaker to run your own ML models (p. 1083).

Note
Aurora machine learning for PostgreSQL connects an Aurora cluster to SageMaker or Amazon Comprehend services only within the same AWS Region.

Topics
- Prerequisites for Aurora machine learning (p. 1079)
- Enabling Aurora Machine Learning (p. 1080)
- Using Amazon Comprehend for natural language processing (p. 1082)
- Exporting data to Amazon S3 for SageMaker model training (p. 1083)
- Using SageMaker to run your own ML models (p. 1083)
- Best practices with Aurora Machine Learning (p. 1086)
- Monitoring Aurora Machine Learning (p. 1090)
- PostgreSQL function reference for Aurora Machine Learning (p. 1091)
- Manually setting up IAM roles for SageMaker and Amazon Comprehend using the AWS CLI (p. 1093)

Prerequisites for Aurora machine learning

Aurora machine learning is available on any Aurora cluster running Aurora PostgreSQL 10.11, 11.6, and newer versions in AWS Regions that support Aurora machine learning. You can upgrade an Aurora cluster running to an older version of Aurora PostgreSQL to a newer version if you want to use Aurora machine...
Enabling Aurora Machine Learning

Enabling the ML capabilities involves the following steps.

Topics
- Setting up IAM access to AWS machine learning services (p. 1080)
- Installing the aws_ml extension for model inference (p. 1081)

Setting up IAM access to AWS machine learning services

Before you can access SageMaker and Amazon Comprehend services, you set up AWS Identity and Access Management (IAM) roles. You then add the IAM roles to the Aurora PostgreSQL cluster. These roles authorize the users of your Aurora PostgreSQL database to access AWS ML services.

You can do IAM setup automatically by using the AWS Management Console as shown here. To use the AWS CLI to set up IAM access, see Manually setting up IAM roles for SageMaker and Amazon Comprehend using the AWS CLI (p. 1093).

Automatically connecting an Aurora DB cluster to AWS services using the console

Aurora machine learning requires that your DB cluster use some combination of Amazon S3, SageMaker, and Amazon Comprehend. Amazon Comprehend is for sentiment analysis. SageMaker is for a wide variety of machine learning algorithms.

For Aurora machine learning, you use Amazon S3 only for training SageMaker models. You only need to use Amazon S3 with Aurora machine learning if you don't already have a trained model available and the training is your responsibility.

To connect a DB cluster to these services requires that you set up an AWS Identity and Access Management (IAM) role for each Amazon service. The IAM role enables users of your DB cluster to authenticate with the corresponding service.

To generate the IAM roles for SageMaker, Amazon Comprehend, or Amazon S3, repeat the following steps for each service that you need.

To connect a DB cluster to an Amazon service

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases, and then choose the Aurora PostgreSQL DB cluster that you want to use.
3. Choose the Connectivity & security tab.
4. Choose Select a service to connect to this cluster in the Manage IAM roles section.
5. Choose the service that you want to connect to from the list:
   - Amazon S3
   - Amazon Comprehend
   - SageMaker
6. Choose Connect service.
7. Enter the required information for the specific service on the Connect cluster window:
   - For SageMaker, enter the Amazon Resource Name (ARN) of a SageMaker endpoint. From the navigation pane of the SageMaker console, choose Endpoints and copy the ARN of the endpoint you want to use. For details about what the endpoint represents, see Deploy a model on Amazon SageMaker hosting services.
   - For Amazon Comprehend, you don’t specify any additional parameters.
   - For Amazon S3, enter the ARN of an Amazon S3 bucket to use.
     
     The format of an Amazon S3 bucket ARN is `arn:aws:s3:::bucket_name`. Ensure that the Amazon S3 bucket you use is set up with the requirements for training SageMaker models. When you train a model, your Aurora DB cluster requires permission to export data to the Amazon S3 bucket, and also to import data from the bucket.
     
     For more about an Amazon S3 bucket ARN, see Specifying resources in a policy in the Amazon Simple Storage Service Developer Guide. For more about using an Amazon S3 bucket with SageMaker, see Step 1: Create an Amazon S3 bucket in the Amazon SageMaker Developer Guide.

8. Choose Connect service.

9. Aurora creates a new IAM role and adds it to the DB cluster’s list of Current IAM roles for this cluster. The IAM role’s status is initially In progress. The IAM role name is autogenerated with the following pattern for each connected service:
   - The Amazon S3 IAM role name pattern is `rds-cluster_ID-S3-role-timestamp`.
   - The SageMaker IAM role name pattern is `rds-cluster_ID-SageMaker-role-timestamp`.
   - The Amazon Comprehend IAM role name pattern is `rds-cluster_ID-Comprehend-role-timestamp`.

   Aurora also creates a new IAM policy and attaches it to the role. The policy name follows a similar naming convention and also has a timestamp.

### Installing the aws_ml extension for model inference

After you create the required IAM roles and associate them with the Aurora PostgreSQL DB cluster, install the functions that use the SageMaker and Amazon Comprehend functionality. The `aws_ml` Aurora PostgreSQL extension provides the `aws_sagemaker.invoke_endpoint` function that communicates directly with SageMaker. The `aws_ml` extension also provides the `aws_comprehend.detect_sentiment` function that communicates directly with Amazon Comprehend.

To install these functions in a specific database, enter the following SQL command at a psql prompt.

```
psql> CREATE EXTENSION IF NOT EXISTS aws_ml CASCADE;
```

If you create the `aws_ml` extension in the `template1` default database, then the functions are available in each new database that you create.

To verify the installation, enter the following at a psql prompt.

```
psql> \dx
```

If you set up an IAM role for Amazon Comprehend, you can verify the setup as follows.

```
SELECT sentiment FROM aws_comprehend.detect_sentiment(null, 'I like it!', 'en');
```
When you install the `aws_ml` extension, the `aws_ml` administrative role is created and granted to the `rds_superuser` role. Separate schemas are also created for the `aws_sagemaker` service and for the `aws_comprehend` service. The `rds_superuser` role is made the OWNER of both of these schemas.

For users or roles to obtain access to the functions in the `aws_ml` extension, grant EXECUTE privilege on those functions. You can subsequently REVOKE the privileges, if needed. EXECUTE privileges are revoked from PUBLIC on the functions of these schemas by default. In a multi-tenant database configuration, to prevent tenants from accessing the functions use REVOKE USAGE on one or more of the ML service schemas.

For a reference to the installed functions of the `aws_ml` extension, see PostgreSQL function reference for Aurora Machine Learning (p. 1091).

## Using Amazon Comprehend for natural language processing

Amazon Comprehend uses machine learning to find insights and relationships in text. Amazon Comprehend uses natural language processing to extract insights about the content of documents. It develops insights by recognizing the entities, key phrases, language, sentiments, and other common elements in a document. You can use this Aurora machine learning service with very little machine learning experience.

Aurora machine learning uses Amazon Comprehend for sentiment analysis of text that is stored in your database. A sentiment is an opinion expressed in text. Sentiment analysis identifies and categorizes sentiments to determine if the attitude towards something (such as a topic or product) is positive, negative, or neutral.

**Note**  
Amazon Comprehend is currently available only in some AWS Regions. To check in which AWS Regions you can use Amazon Comprehend, see the AWS Region table page on the AWS site.

For example, using Amazon Comprehend you can analyze contact center call-in documents to detect caller sentiment and better understand caller-agent dynamics. You can find a further description in the post Analyzing contact center calls on the AWS Machine Learning blog.

You can also combine sentiment analysis with the analysis of other information in your database using a single query. For example, you can detect the average sentiment of call-in center documents for issues that combine the following:

- Open for more than 30 days.
- About a specific product or feature.
- Made by the customers who have the greatest social media influence.

Using Amazon Comprehend from Aurora Machine Learning is as easy as calling a SQL function. When you installed the `aws_ml` extension (Installing the `aws_ml` extension for model inference (p. 1081)), it provides the `aws_comprehend.detect_sentiment` (p. 1091) function to perform sentiment analysis through Amazon Comprehend.

For each text fragment that you analyze, this function helps you determine the sentiment and the confidence level. A typical Amazon Comprehend query looks for table rows where the sentiment has a certain value (POSITIVE or NEGATIVE), with a confidence level greater than a certain percent.

For example, the following query shows how to determine the average sentiment of documents in a database table, `myTable.document`. The query considers only documents where the confidence of the assessment is at least 80 percent. In the following example, English (en) is the language of the sentiment text.
To avoid your being charged for sentiment analysis more than once per table row, you can materialize the results of the analysis once per row. Do this on the rows of interest. In the following example, French (fr) is the language of the sentiment text.

```
-- *Example:* Update the sentiment and confidence of French text.
--
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;
```

For more information on optimizing your function calls, see Best practices with Aurora Machine Learning (p. 1086).

For information about parameters and return types for the sentiment detection function, see aws_comprehend.detect_sentiment (p. 1091).

### Exporting data to Amazon S3 for SageMaker model training

Depending on how your team divides the machine learning tasks, you might not perform model training. If someone else provides the SageMaker model for you, you can skip this section.

To train SageMaker models, you export data to an Amazon S3 bucket. The Amazon S3 bucket is used by SageMaker to train your model before it is deployed. You can query data from an Aurora PostgreSQL DB cluster and save it directly into text files stored in an Amazon S3 bucket. Then SageMaker consumes the data from the Amazon S3 bucket for training. For more about SageMaker model training, see Train a model with Amazon SageMaker.

**Note**

When you create an S3 bucket for SageMaker model training or batch scoring, always include the text sagemaker in the S3 bucket name. For more information about creating an S3 bucket for SageMaker, see Step 1: Create an Amazon S3 bucket.

For more information about exporting your data, see Exporting data from an Aurora PostgreSQL DB cluster to Amazon S3 (p. 1040).

### Using SageMaker to run your own ML models

SageMaker is a fully managed machine learning service. With SageMaker, data scientists and developers build and train machine learning models. Then they can directly deploy the models into a production-ready hosted environment.

SageMaker provides access to your data sources so that you can perform exploration and analysis without managing the hardware infrastructure for servers. SageMaker also provides common machine learning algorithms that are optimized to run efficiently against extremely large datasets in a distributed cloud environment.
environment. With native support for bring-your-own-algorithms and frameworks, SageMaker offers flexible distributed training options that adjust to your specific workflows.

**Note**
Currently, Aurora machine learning supports any SageMaker endpoint that can read and write the comma-separated value (CSV) format, through a `ContentType` value of `text/csv`. The built-in SageMaker algorithms that currently accept this format are Random Cut Forest, Linear Learner, and XGBoost.

Be sure to deploy the model you are using in the same AWS Region as your Aurora PostgreSQL cluster. Aurora machine learning always invokes SageMaker endpoints in the same AWS Region as your Aurora cluster.

When you install the `aws_ml` extension (as described in Installing the aws_ml extension for model inference (p. 1081)), it provides the `aws_sagemaker.invoke_endpoint` function. You use this function to invoke your SageMaker model and perform model inference directly from within your SQL database application.

**Topics**
- Creating a user-defined function to invoke a SageMaker model (p. 1084)
- Passing an array as input to a SageMaker model (p. 1085)
- Specifying batch size when invoking a SageMaker model (p. 1085)
- Invoking a SageMaker model that has multiple outputs (p. 1086)

### Creating a user-defined function to invoke a SageMaker model

Create a separate user-defined function to call `aws_sagemaker.invoke_endpoint` for each of your SageMaker models. Your user-defined function represents the SageMaker endpoint hosting the model. The `aws_sagemaker.invoke_endpoint` function runs within the user-defined function. User-defined functions provide many advantages:

- You can give your ML model its own name instead of only calling `aws_sagemaker.invoke_endpoint` for all of your ML models.
- You can specify the model endpoint URL in just one place in your SQL application code.
- You can control `EXECUTE` privileges to each ML function independently.
- You can declare the model input and output types using SQL types. SQL enforces the number and type of arguments passed to your ML model and performs type conversion if necessary. Using SQL types will also translate SQL `NULL` to the appropriate default value expected by your ML model.
- You can reduce the maximum batch size if you want to return the first few rows a little faster.

To specify a user-defined function, use the SQL data definition language (DDL) statement `CREATE FUNCTION`. When you define the function, you specify the following:

- The input parameters to the model.
- The specific SageMaker endpoint to invoke.
- The return type.

The user-defined function returns the inference computed by the SageMaker endpoint after running the model on the input parameters. The following example creates a user-defined function for an SageMaker model with two input parameters.

```sql
CREATE FUNCTION classify_event (IN arg1 INT, IN arg2 DATE, OUT category INT) AS $$
  SELECT aws_sagemaker.invoke_endpoint ()
$$;
```
Note the following:

- The `aws_sagemaker.invoke_endpoint` function input can be one or more parameters of any data type.

For more details about parameters, see the `aws_sagemaker.invoke_endpoint (p. 1092)` function reference.

- This example uses an INT output type. If you cast the output from a `varchar` type to a different type, then it must be cast to a PostgreSQL builtin scalar type such as `INTEGER`, `REAL`, `FLOAT`, or `NUMERIC`. For more information about these types, see Data types in the PostgreSQL documentation.

- Specify `PARALLEL SAFE` to enable parallel query processing. For more information, see Exploiting parallel query processing (p. 1089).

- Specify `COST 5000` to estimate the cost of running the function. Use a positive number giving the estimated run cost for the function, in units of `cpu_operator_cost`.

### Passing an array as input to a SageMaker model

The `aws_sagemaker.invoke_endpoint (p. 1092)` function can have up to 100 input parameters, which is the limit for PostgreSQL functions. If the SageMaker model requires more than 100 parameters of the same type, pass the model parameters as an array.

The following example creates a user-defined function that passes an array as input to the SageMaker regression model.

```sql
CREATE FUNCTION regression_model (params REAL[], OUT estimate REAL) AS $$
SELECT aws_sagemaker.invoke_endpoint ('sagemaker_model_endpoint_name', NULL,
params                            -- model input parameters as an array
)::REAL                           -- cast output to REAL
$$ LANGUAGE SQL PARALLEL SAFE COST 5000;
```

### Specifying batch size when invoking a SageMaker model

The following example creates a user-defined function for a SageMaker model that sets the batch size default to NULL. The function also allows you to provide a different batch size when you invoke it.

```sql
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 $$
SELECT aws_sagemaker.invoke_endpoint ('sagemaker_model_endpoint_name',
    event_type, event_day, COALESCE(amount, 0.0)
)::INT  -- casts output to type INT
$$ LANGUAGE SQL PARALLEL SAFE COST 5000;
```

Note the following:

- Use the optional `max_rows_per_batch` parameter to provide control of the number of rows for a batch-mode function invocation. If you use a value of `NULL`, then the query optimizer automatically
chooses the maximum batch size. For more information, see Optimizing batch-mode execution for Aurora Machine Learning function calls (p. 1087).

- By default, passing NULL as a parameter's value is translated to an empty string before passing to SageMaker. For this example, the inputs have different types.
- If you have a non-text input, or text input that needs to default to some value other than an empty string, use the COALESCE statement. Use COALESCE to translate NULL to the desired null replacement value in the call to aws_sagemaker.invoke_endpoint. For the amount parameter in this example, a NULL value is converted to 0.0.

Invoking a SageMaker model that has multiple outputs

The following example creates a user-defined function for a SageMaker model that returns multiple outputs. Your function needs to cast the output of the aws_sagemaker.invoke_endpoint function to a corresponding data type. For example, you could use the built-in PostgreSQL point type for (x,y) pairs or a user-defined composite type.

This user-defined function returns values from a model that returns multiple outputs by using a composite type for the outputs.

```sql
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;
```

For the composite type, use fields in the same order as they appear in the model output and cast the output of aws_sagemaker.invoke_endpoint to your composite type. The caller can extract the individual fields either by name or with PostgreSQL ".*" notation.

Best practices with Aurora Machine Learning

Most of the work in an aws_ml function call happens within the external Aurora Machine Learning service. This separation allows you to scale the resources for the machine learning service independent of your Aurora cluster. Within Aurora, you mostly focus on making the user-defined function calls themselves as efficient as possible. Some aspects that you can influence from your Aurora cluster include:

- The max_rows_per_batch setting for calls to the aws_ml functions.
- The number of virtual CPUs of the database instance, which determines the maximum degree of parallelism that the database might use when running your ML functions.
- the PostgreSQL parameters that control parallel query processing.

Topics

- Optimizing batch-mode execution for Aurora Machine Learning function calls (p. 1087)
- Exploiting parallel query processing (p. 1089)
Optimizing batch-mode execution for Aurora Machine Learning function calls

Typically PostgreSQL runs functions one row at a time. Aurora Machine Learning can minimize this overhead by combining the calls to the external Aurora Machine Learning service for many rows into batches with an approach called batch-mode execution. In batch mode, Aurora Machine Learning receives the responses for a batch of input rows, and then delivers the responses back to the running query one row at a time. This optimization improves the throughput of your Aurora queries without limiting the PostgreSQL query optimizer.

Aurora automatically uses batch mode if the function is referenced from the SELECT list, a WHERE clause, or a HAVING clause. Note that top-level simple CASE expressions are eligible for batch-mode execution. Top-level searched CASE expressions are also eligible for batch-mode execution provided that the first WHEN clause is a simple predicate with a batch-mode function call.

Your user-defined function must be a LANGUAGE SQL function and should specify PARALLEL SAFE and COST 5000.

Topics

- Function migration from the SELECT statement to the FROM clause (p. 1087)
- Using the max_rows_per_batch parameter (p. 1088)
- Verifying batch-mode execution (p. 1088)

Function migration from the SELECT statement to the FROM clause

Usually, an aws_ml function that is eligible for batch-mode execution is automatically migrated by Aurora to the FROM clause.

The migration of eligible batch-mode functions to the FROM clause can be examined manually on a per-query level. To do this, you use EXPLAIN statements (and ANALYZE and VERBOSE) and find the "Batch Processing" information below each batch-mode Function Scan. You can also use EXPLAIN (with VERBOSE) without running the query. You then observe whether the calls to the function appear as a Function Scan under a nested loop join that was not specified in the original statement.

In the following example, the presence of the nested loop join operator in the plan shows that Aurora migrated the anomaly_score function. It migrated this function from the SELECT list to the FROM clause, where it's eligible for batch-mode execution.

```
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)
```

To disable batch-mode execution, set the apg_enable_function_migration parameter to false. This prevents the migration of aws_ml functions from the SELECT to the FROM clause. The following shows how.
The `apg_enable_function_migration` parameter is a Grand Unified Configuration (GUC) parameter that is recognized by the Aurora PostgreSQL `apg_plan_mgmt` extension for query plan management. To disable function migration in a session, use query plan management to save the resulting plan as an approved plan. At runtime, query plan management enforces the approved plan with its `apg_enable_function_migration` setting. This enforcement occurs regardless of the `apg_enable_function_migration` GUC parameter setting. For more information, see Managing query execution plans for Aurora PostgreSQL (p. 1049).

Using the `max_rows_per_batch` parameter

The `max_rows_per_batch` parameter of the `aws_sagemaker.invoke_endpoint` (p. 1092) and `aws_comprehend.detect_sentiment` (p. 1091) functions influences how many rows are transferred to the Aurora Machine Learning service. The larger the dataset processed by the user-defined function, the larger you can make the batch size.

Batch-mode functions improve efficiency by building batches of rows that spread the cost of the Aurora Machine Learning function calls over a large number of rows. However, if a `SELECT` statement finishes early due to a `LIMIT` clause, then the batch can be constructed over more rows than the query uses. This approach can result in additional charges to your AWS account. To gain the benefits of batch-mode execution but avoid building batches that are too large, use a smaller value for the `max_rows_per_batch` parameter in your function calls.

If you do an `EXPLAIN (VERBOSE, ANALYZE)` of a query that uses batch-mode execution, you see a `FunctionScan` operator that is below a nested loop join. The number of loops reported by `EXPLAIN` tells you the number of times a row was fetched from the `FunctionScan` operator. If a statement uses a `LIMIT` clause, the number of fetches is consistent. To optimize the size of the batch, set the `max_rows_per_batch` parameter to this value. However, if the batch-mode function is referenced in a predicate in the `WHERE` clause or `HAVING` clause, then you probably can't know the number of fetches in advance. In this case, use the loops as a guideline and experiment with `max_rows_per_batch` to find a setting that optimizes performance.

Verifying batch-mode execution

To see if a function ran in batch mode, use `EXPLAIN ANALYZE`. If batch-mode execution was used, then the query plan will include the information in a "Batch Processing" section.

```
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 this example, there was 1 batch that contained 3,333 rows, which took 146.273 ms to process. The "Batch Processing" section shows the following:

- How many batches there were for this function scan operation
- The batch size average, minimum, and maximum
- The batch execution time average, minimum, and maximum

Typically the final batch is smaller than the rest, which often results in a minimum batch size that is much smaller than the average.

To return the first few rows more quickly, set the `max_rows_per_batch` parameter to a smaller value.

To reduce the number of batch mode calls to the ML service when you use a `LIMIT` in your user-defined function, set the `max_rows_per_batch` parameter to a smaller value.
Exploiting parallel query processing

To dramatically increase performance when processing a large number of rows, you can combine parallel query processing with batch mode processing. You can use parallel query processing for SELECT, CREATE TABLE AS SELECT, and CREATE MATERIALIZED VIEW statements.

Note
PostgreSQL doesn't yet support parallel query for data manipulation language (DML) statements.

Parallel query processing occurs both within the database and within the ML service. The number of cores in the instance class of the database limits the degree of parallelism that can be used when running a query. The database server can construct a parallel query execution plan that partitions the task among a set of parallel workers. Then each of these workers can build batched requests containing tens of thousands of rows (or as many as are allowed by each service).

The batched requests from all of the parallel workers are sent to the endpoint for the AWS service (SageMaker, for example). Thus, the number and type of instances behind the AWS service endpoint also limits the degree of parallelism that can be usefully exploited. Even a two-core instance class can benefit significantly from parallel query processing. However, to fully exploit parallelism at higher K degrees, you need a database instance class that has at least K cores. You also need to configure the AWS service so that it can process K batched requests in parallel. For SageMaker, you need to configure the SageMaker endpoint for your ML model to have K initial instances of a sufficiently high-performing instance class.

To exploit parallel query processing, you can set the parallel_workers storage parameter of the table that contains the data that you plan to pass. You set parallel_workers to a batch-mode function such as aws_comprehend.detect_sentiment. If the optimizer chooses a parallel query plan, the AWS ML services can be called both in batch and in parallel. You can use the following parameters with the aws_comprehend.detect_sentiment function to get a plan with four-way parallelism.

```
-- If you change either of the following two parameters, you must restart
-- the database instance for the changes to take effect.
--
-- 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 ML 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;
```

For more about controlling parallel query, see Parallel plans in the PostgreSQL documentation.

Using materialized views and materialized columns

When you invoke an AWS service such as SageMaker or Amazon Comprehend from your database, your account is charged according to the pricing policy of that service. To minimize charges to your account, you can materialize the result of calling the AWS service into a materialized column so that
the AWS service is not called more than once per input row. If desired, you can add a `materializedAt` timestamp column to record the time at which the columns were materialized.

The latency of an ordinary single-row `INSERT` statement is typically much less than the latency of calling a batch-mode function. Thus, you might not be able to meet the latency requirements of your application if you invoke the batch-mode function for every single-row `INSERT` that your application performs. To materialize the result of calling an AWS service into a materialized column, high-performance applications generally need to populate the materialized columns. To do this, they periodically issue an `UPDATE` statement that operates on a large batch of rows at the same time.

`UPDATE` takes a row-level lock that can impact a running application. So you might need to use `SELECT ... FOR UPDATE SKIP LOCKED`, or use `MATERIALIZED VIEW`.

Analytics queries that operate on a large number of rows in real time can combine batch-mode materialization with real-time processing. To do this, these queries assemble a `UNION ALL` of the pre-materialized results with a query over the rows that don't yet have materialized results. In some cases, such a `UNION ALL` is needed in multiple places, or the query is generated by a third-party application. If so, you can create a `VIEW` to encapsulate the `UNION ALL` operation so this detail isn't exposed to the rest of the SQL application.

You can use a materialized view to materialize the results of an arbitrary `SELECT` statement at a snapshot in time. You can also use it to refresh the materialized view at any time in the future. Currently PostgreSQL doesn't support incremental refresh, so each time the materialized view is refreshed the materialized view is fully recomputed.

You can refresh materialized views with the `CONCURRENTLY` option, which updates the contents of the materialized view without taking an exclusive lock. Doing this allows a SQL application to read from the materialized view while it's being refreshed.

### Monitoring Aurora Machine Learning

To monitor the functions in the `aws_ml` package, set the `track_functions` parameter and then query the PostgreSQL `pg_stat_user_functions` view.

For information about monitoring the performance of the SageMaker operations called from Aurora Machine Learning functions, see Monitor Amazon SageMaker.

To set `track_functions` at the session level, run the following.

```
SET track_functions = 'all';
```

Use one of the following values:

- `all` – Track C language functions and SQL language functions that aren't placed inline. To track the `aws_ml` functions, use `all` because these functions are implemented in C.
- `pl` – Track only procedural-language functions.
- `none` – Disable function statistics tracking.

After enabling `track_functions` and running your user-defined ML function, query the `pg_stat_user_functions` view to get information. The view includes the number of calls, `total_time` and `self_time` for each function. To view the statistics for the `aws_sagemaker.invoke_endpoint` and `aws_comprehend.detect_sentiment` functions, filter the results by schema names starting with `aws_`.

```
run your statement
SELECT * FROM pg_stat_user_functions WHERE schemaname LIKE 'aws_%';
SELECT pg_stat_reset();  -- To clear statistics
```
To find the names of your SQL functions that call the `aws_sagemaker.invoke_endpoint` function, query the source code of the functions in the PostgreSQL `pg_proc` catalog table.

```sql
SELECT proname FROM pg_proc WHERE prosrc LIKE '%invoke_endpoint%';
```

**Using query plan management to monitor ML functions**

If you captured plans using the `apg_plan_mgmt` extension of query plan management, you can then search through all the statements in your workload that refer to these function names. In your search, you can check `plan_outline` to see if batch-mode execution was used. You can also list statement statistics such as execution time and plan cost. Plans that use batch-mode function scans contain a FuncScan operator in the plan outline. Functions that aren't run as a join don't contain a FuncScan operator.

For more about query plan management, see Managing query execution plans for Aurora PostgreSQL (p. 1049).

To find calls to the `aws_sagemaker.invoke_endpoint` function that don't use batch mode, use the following statement.

```sql
\dx apg_plan_mgmt
SELECT sql_hash, plan_hash, status, environment_variables, sql_text::varchar(50), plan_outline FROM pg_proc, apg_plan_mgmt.dba_plans WHERE prosrc LIKE '%invoke_endpoint%' AND sql_text LIKE '%' || proname || '%' AND plan_outline NOT LIKE '%FuncScan%';
```

The example preceding searches all statements in your workload that call SQL functions that in turn call the `aws_sagemaker.invoke_endpoint` function.

To obtain detailed runtime statistics for each of these statements, call the `apg_plan_mgmt.get_explain_stmt` function.

```sql
SELECT apg_plan_mgmt.get_explain_stmt(sql_hash, plan_hash, 'analyze,verbose,buffers') FROM pg_proc, apg_plan_mgmt.dba_plans WHERE prosrc LIKE '%invoke_endpoint%' AND sql_text LIKE '%' || proname || '%' AND plan_outline NOT LIKE '%FuncScan%';
```

**PostgreSQL function reference for Aurora Machine Learning**

**Functions**
- `aws_comprehend.detect_sentiment` (p. 1091)
- `aws_sagemaker.invoke_endpoint` (p. 1092)

**aws_comprehend.detect_sentiment**

Performs sentiment analysis using Amazon Comprehend. For more about usage, see Using Amazon Comprehend for natural language processing (p. 1082).
Syntax

```sql
aws_comprehend.detect_sentiment (  
    IN input_text varchar,  
    IN language_code varchar,  
    IN max_rows_per_batch int,  
    OUT sentiment varchar,  
    OUT confidence real)  
)
```

**Input Parameters**

**input_text**

The text to detect sentiment on.

**language_code**

The language of the `input_text`. For valid values, see [Languages supported in Amazon Comprehend](#).

**max_rows_per_batch**

The maximum number of rows per batch for batch-mode processing. For more information, see [Optimizing batch-mode execution for Aurora Machine Learning function calls (p. 1087)](#).

**Output Parameters**

**sentiment**

The sentiment of the text. Valid values are POSITIVE, NEGATIVE, NEUTRAL, or MIXED.

**confidence**

The degree of confidence in the `sentiment` value. Values range between 1.0 for 100% to 0.0 for 0%.

**aws_sagemaker.invoke_endpoint**

After you train a model and deploy it into production using SageMaker services, your client applications use the `aws_sagemaker.invoke_endpoint` function to get inferences from the model. The model must be hosted at the specified endpoint and must be in the same AWS Region as the database instance. For more about usage, see [Using SageMaker to run your own ML models (p. 1083)](#).

Syntax

```sql
aws_sagemaker.invoke_endpoint(  
    IN endpoint_name varchar,  
    IN max_rows_per_batch int,  
    VARIADIC model_input "any",  
    OUT model_output varchar  
)
```

**Input Parameters**

**endpoint_name**

An endpoint URL that is AWS Region-independent.
max_rows_per_batch

The maximum number of rows per batch for batch-mode processing. For more information, see Optimizing batch-mode execution for Aurora Machine Learning function calls (p. 1087).

model_input

One or more input parameters for the ML model. These can be any data type.

PostgreSQL allows you to specify up to 100 input parameters for a function. Array data types must be one-dimensional, but can contain as many elements as are expected by the SageMaker model. The number of inputs to a SageMaker model is bounded only by the SageMaker 5 MB message size limit.

Output Parameters

model_output

The SageMaker model's output parameter, as text.

Usage Notes

The `aws_sagemaker.invoke_endpoint` function connects only to a model endpoint in the same AWS Region. If your database instance has replicas in multiple AWS Regions, always deploy each Amazon SageMaker model to all of those AWS Regions.

Calls to `aws_sagemaker.invoke_endpoint` are authenticated using the SageMaker IAM role for the database instance.

SageMaker model endpoints are scoped to an individual account and are not public. The `endpoint_name` URL doesn't contain the account ID. SageMaker determines the account ID from the authentication token that is supplied by the SageMaker IAM role of the database instance.

Manually setting up IAM roles for SageMaker and Amazon Comprehend using the AWS CLI

Note

If you use the AWS Management Console, AWS does the IAM setup for you automatically. In this case, you can skip the following information and follow the procedure in Automatically connecting an Aurora DB cluster to AWS services using the console (p. 1080).

Setting up the IAM roles for SageMaker or Amazon Comprehend using the AWS CLI or the RDS API consists of the following steps:

1. Create an IAM policy to specify which SageMaker endpoints can be invoked by your Aurora PostgreSQL cluster or to enable access to Amazon Comprehend.
2. Create an IAM role to permit your Aurora PostgreSQL database cluster to access AWS ML services. Also attach the IAM policy created preceding to the IAM role created here.
3. Associate the IAM role that you created preceding to the Aurora PostgreSQL database cluster to permit access to AWS ML services.

Topics

- Creating an IAM policy to access SageMaker using the AWS CLI (p. 1094)
- Creating an IAM policy to access Amazon Comprehend using the AWS CLI (p. 1094)
- Creating an IAM role to access SageMaker and Amazon Comprehend (p. 1095)
Creating an IAM policy to access SageMaker using the AWS CLI

**Note**
Aurora can create the IAM policy for you automatically. You can skip the following information and use the procedure in Automatically connecting an Aurora DB cluster to AWS services using the console (p. 1080).

The following policy adds the permissions required by Aurora PostgreSQL to invoke a SageMaker function on your behalf. You can specify all of your SageMaker endpoints that you need your database applications to access from your Aurora PostgreSQL cluster in a single policy.

**Note**
This policy enables you to specify the AWS Region for a SageMaker endpoint. However, an Aurora PostgreSQL cluster can only invoke SageMaker models deployed in the same AWS Region as the cluster.

```json
```

The following AWS CLI command creates an IAM policy with these options.

```
aws iam create-policy  --policy-name policy_name --policy-document '{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAuroraToInvokeRCFEndPoint",
      "Effect": "Allow",
      "Action": "sagemaker:InvokeEndpoint",
      "Resource": "arn:aws:sagemaker:region:123456789012:endpoint/endpointName"
    }
  ]
}
```

For the next step, see Creating an IAM role to access SageMaker and Amazon Comprehend (p. 1095).

Creating an IAM policy to access Amazon Comprehend using the AWS CLI

**Note**
Aurora can create the IAM policy for you automatically. You can skip the following information and use the procedure in Automatically connecting an Aurora DB cluster to AWS services using the console (p. 1080).

The following policy adds the permissions required by Aurora PostgreSQL to invoke AWS Amazon Comprehend on your behalf.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAuroraToInvokeComprehendDetectSentiment",
      "Effect": "Allow",
      "Action": [ "comprehend:DetectSentiment", "comprehend:BatchDetectSentiment" ]
    }
  ]
}
```
To create an IAM policy to grant access to Amazon Comprehend

1. Open the IAM management console.
2. In the navigation pane, choose Policies.
3. Choose Create policy.
4. On the Visual editor tab, choose Choose a service, and then choose Comprehend.
5. For Actions, choose Detect Sentiment and BatchDetectSentiment.
7. For Name, enter a name for your IAM policy. You use this name when you create an IAM role to associate with your Aurora DB cluster. You can also add an optional Description value.
8. Choose Create policy.

For the net step, see Creating an IAM role to access SageMaker and Amazon Comprehend (p. 1095).

Creating an IAM role to access SageMaker and Amazon Comprehend

Note
Aurora can create the IAM role for you automatically. You can skip the following information and use the procedure in Automatically connecting an Aurora DB cluster to AWS services using the console (p. 1080).

After you create the IAM policies, create an IAM role that the Aurora PostgreSQL DB cluster can assume for your database users to access ML services. To create an IAM role, follow the steps described in Creating a role to delegate permissions to an IAM user.

Attach the preceding policies to the IAM role you create. For more information, see Attaching an IAM policy to an IAM user or role (p. 1243).

For more information about IAM roles, see IAM roles in the AWS Identity and Access Management User Guide.

For the next step, see Associating an IAM role with an Aurora PostgreSQL DB cluster using the AWS CLI (p. 1095).

Associating an IAM role with an Aurora PostgreSQL DB cluster using the AWS CLI

Note
Aurora can associate an IAM role with your DB cluster for you automatically. You can skip the following information and use the procedure in Automatically connecting an Aurora DB cluster to AWS services using the console (p. 1080).

The last process in setting up IAM access is to associate the IAM role and its IAM policy with your Aurora PostgreSQL DB cluster. Do the following:

1. Add the role to the list of associated roles for a DB cluster.

   To associate the role with your DB cluster, use the AWS Management Console or the add-role-to-db-cluster AWS CLI command.
To add an IAM role for a PostgreSQL DB cluster using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. Choose the PostgreSQL DB cluster name to display its details.
3. On the Connectivity & security tab, in the Manage IAM roles section, choose the role to add under Add IAM roles to this cluster.
4. Under Feature, choose SageMaker or Comprehend.
5. Choose Add role.

To add an IAM role for a PostgreSQL DB cluster using the CLI

Use the following command to add the role to the PostgreSQL DB cluster named my-db-cluster. Replace your-role-arn with the role ARN that you noted in a previous step. For the value of the --feature-name option, use SageMaker, Comprehend, or s3Export depending on which service you want to use.

Example

For Linux, macOS, or Unix:

```
aws rds add-role-to-db-cluster \
    --db-cluster-identifier my-db-cluster \
    --feature-name external-service \
    --role-arn your-role-arn \
    --region your-region
```

For Windows:

```
aws rds add-role-to-db-cluster ^
    --db-cluster-identifier my-db-cluster ^
    --feature-name external-service ^
    --role-arn your-role-arn ^
    --region your-region
```

2. Set the cluster-level parameter for each AWS ML service to the ARN for the associated IAM role.

Use the electroencephalographic, miscomprehended, or both parameters depending on which AWS ML services you intend to use with your Aurora cluster.

Cluster-level parameters are grouped into DB cluster parameter groups. To set the preceding cluster parameters, use an existing custom DB cluster group or create a new one. To create a new DB cluster parameter group, call the create-db-cluster-parameter-group command from the AWS CLI, for example:

```
aws rds create-db-cluster-parameter-group --db-cluster-parameter-group-name AllowAWSAccessToExternalServices --db-parameter-group-family aurora-postgresql-group --description "Allow access to Amazon S3, Amazon SageMaker, and Amazon Comprehend"
```

Set the appropriate cluster-level parameter or parameters and the related IAM role ARN values in your DB cluster parameter group. Do the following.

```
aws rds modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name AllowAWSAccessToExternalServices \
    --parameters "ParameterName=aws_default_s3_role,ParameterValue=arn:aws:iam::123456789012:role/AllowAuroraS3Role,ApplyMethod=pending-reboot"
```
Modify the DB cluster to use the new DB cluster parameter group. Then, reboot the cluster. The following shows how.

```bash
aws rds modify-db-cluster --db-cluster-identifier your_cluster_id --db-cluster-parameter-group-name AllowAWSAccessToExternalServices
aws rds failover-db-cluster --db-cluster-identifier your_cluster_id
```

When the instance has rebooted, your IAM roles are associated with your DB cluster.

### Fast recovery after failover with cluster cache management for Aurora PostgreSQL

For fast recovery of the writer DB instance in your Aurora PostgreSQL clusters if there's a failover, use cluster cache management for Amazon Aurora PostgreSQL. Cluster cache management ensures that application performance is maintained if there's a failover.

In a typical failover situation, you might see a temporary but large performance degradation after failover. This degradation occurs because when the failover DB instance starts, the buffer cache is empty. An empty cache is also known as a **cold cache**. A cold cache degrades performance because the DB instance has to read from the slower disk, instead of taking advantage of values stored in the buffer cache.

With cluster cache management, you set a specific reader DB instance as the failover target. Cluster cache management ensures that the data in the designated reader's cache is kept synchronized with the data in the writer DB instance's cache. The designated reader's cache with prefilled values is known as a **warm cache**. If a failover occurs, the designated reader uses values in its warm cache immediately when it's promoted to the new writer DB instance. This approach provides your application much better recovery performance.

#### Topics
- Configuring cluster cache management (p. 1097)
- Monitoring the buffer cache (p. 1100)

### Configuring cluster cache management

**Note**

Cluster cache management is supported for Aurora PostgreSQL DB clusters of versions 9.6.11 and above, and versions 10.5 and above.

To configure cluster cache management, do the following processes in order.

#### Topics
- Enabling cluster cache management (p. 1098)
- Setting the promotion tier priority for the writer DB instance (p. 1098)
The DB cluster must use a parameter group other than the default, because you can't change values in a default parameter group.

4. For **Parameter group actions**, choose **Edit**.
5. Set the value of the `apg_ccm_enabled` cluster parameter to `1`.
6. Choose **Save changes**.

**AWS CLI**

To enable cluster cache management for an Aurora PostgreSQL DB cluster, use the AWS CLI `modify-db-cluster-parameter-group` command with the following required parameters:

- `--db-cluster-parameter-group-name`
- `--parameters`

**Example**

For Linux, macOS, or Unix:

```bash
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"
```

For Windows:

```bash
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"
```

**Setting the promotion tier priority for the writer DB instance**

For cluster cache management, make sure that the promotion priority is **tier-0** for the writer DB instance of the Aurora PostgreSQL DB cluster. The **promotion tier priority** is a value that specifies the order in which an Aurora reader is promoted to the writer DB instance after a failure. Valid values are 0–15, where...
0 is the first priority and 15 is the last priority. For more information about the promotion tier, see Fault tolerance for an Aurora DB cluster (p. 56).

**Console**

**To set the promotion priority for the writer DB instance to tier-0**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. Choose the **Writer** DB instance of the Aurora PostgreSQL DB cluster.
4. Choose **Modify**. The **Modify DB Instance** page appears.
5. On the **Additional configuration** panel, choose **tier-0** for the **Failover priority**.
6. Choose **Continue** and check the summary of modifications.
7. To apply the changes immediately after you save them, choose **Apply immediately**.
8. Choose **Modify DB Instance** to save your changes.

**AWS CLI**

To set the promotion tier priority to 0 for the writer DB instance using the AWS CLI, call the `modify-db-instance` command with the following required parameters:

- `--db-instance-identifier`
- `--promotion-tier`
- `--apply-immediately`

**Example**

For Linux, macOS, or Unix:

```bash/aws rds modify-db-instance \
  --db-instance-identifier writer-db-instance \ 
  --promotion-tier 0 \ 
  --apply-immediately```

For Windows:

```bash
aws rds modify-db-instance ^ 
  --db-instance-identifier writer-db-instance ^ 
  --promotion-tier 0 ^ 
  --apply-immediately```

**Setting the promotion tier priority for a reader DB instance**

You set one reader DB instance for cluster cache management. To do so, choose a reader from the Aurora PostgreSQL cluster that is the same instance class as the writer DB instance. Then set its promotion tier priority to 0.

The **promotion tier priority** is a value that specifies the order in which an Aurora reader is promoted to the writer DB instance after a failure. Valid values are 0–15, where 0 is the first priority and 15 is the last priority.
Console

To set the promotion priority of the reader DB instance to tier-0

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
3. Choose a Reader DB instance of the Aurora PostgreSQL DB cluster that is the same instance class as the writer DB instance.
5. On the Additional configuration panel, choose tier-0 for the Failover priority.
6. Choose Continue and check the summary of modifications.
7. To apply the changes immediately after you save them, choose Apply immediately.
8. Choose Modify DB Instance to save your changes.

AWS CLI

To set the promotion tier priority to 0 for the reader DB instance using the AWS CLI, call the modify-db-instance command with the following required parameters:

• --db-instance-identifier
• --promotion-tier
• --apply-immediately

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \  
 --db-instance-identifier reader-db-instance \  
 --promotion-tier 0 \  
 --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^  
 --db-instance-identifier reader-db-instance ^  
 --promotion-tier 0 ^  
 --apply-immediately
```

Monitoring the buffer cache

After setting up cluster cache management, you can monitor the state of synchronization between the writer DB instance's buffer cache and the designated reader's warm buffer cache. To examine the buffer cache contents on both the writer DB instance and the designated reader DB instance, use the PostgreSQL pg_buffercache module. For more information, see the PostgreSQL pg_buffercache documentation.

Using the aurora_ccm_status Function

Cluster cache management also provides the aurora_ccm_status function. Use the aurora_ccm_status function on the writer DB instance to get the following information about the progress of cache warming on the designated reader:
• `buffers_sent_last_minute` – How many buffers have been sent to the designated reader in the last minute.
• `buffers_sent_last_scan` – How many buffers have been sent to the designated reader during the last complete scan of the buffer cache.
• `buffers_found_last_scan` – How many buffers have been identified as frequently accessed and needed to be sent during the last complete scan of the buffer cache. Buffers already cached on the designated reader aren’t sent.
• `buffers_sent_current_scan` – How many buffers have been sent so far during the current scan.
• `buffers_found_current_scan` – How many buffers have been identified as frequently accessed in the current scan.
• `current_scan_progress` – How many buffers have been visited so far during the current scan.

The following example shows how to use the `aurora_ccm_status` function to convert some of its output into a warm rate and warm percentage.

```sql
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();
```

---

**Invoking an AWS Lambda function from an Aurora PostgreSQL DB cluster**

You can invoke AWS Lambda functions from an Aurora PostgreSQL DB cluster. To do this, use the `aws_lambda` PostgreSQL extension provided with Aurora PostgreSQL.

AWS Lambda is a compute service that you can use to run code. For example, you can use Lambda functions to process event notifications from a DB instance. For more information about Lambda, see [What is AWS Lambda?](#).

**Topics**

- Overview of using a Lambda function (p. 1101)
- Specifying the Lambda function to use (p. 1102)
- Giving Aurora access to Lambda (p. 1103)
- Invoking Lambda functions (p. 1104)
- Function reference (p. 1106)

**Overview of using a Lambda function**

You can invoke a Lambda function from an Aurora PostgreSQL database with the following procedure,

**To invoke a Lambda function from an Aurora PostgreSQL database**

1. Install the required PostgreSQL extensions. These include the `aws_lambda` and `aws_commons` extensions. To do so, start `psql` and run the following commands.

```sql
CREATE EXTENSION IF NOT EXISTS aws_lambda CASCADE;
```
Specifying the Lambda function to use

1. Identify the name or Amazon Resource Name (ARN) for the Lambda function to use. For details about this process, see Specifying the Lambda function to use (p. 1102).

2. Provide permission to access the Lambda function.

   To invoke a Lambda function, give the Aurora PostgreSQL DB cluster permission to access the Lambda invoke API operation. Doing this includes the following steps:
   
   1. Create an AWS Identity and Access Management (IAM) policy that provides access to a Lambda function that you want to invoke.
   2. Create an IAM role.
   3. Attach the IAM policy that you created to the role that you created.
   4. Add this IAM role to your DB cluster.

   For details about this process, see Giving Aurora access to Lambda (p. 1103).

3. Use the `aws_lambda.invoke` function to run the Lambda function. For details about this process, see Invoking Lambda functions (p. 1104).

Specifying the Lambda function to use

To identify the Lambda function to use, specify the following information:

- **Function name** – The name of the Lambda function, ARN, version, or alias. For a listing of possible formats, see Lambda function name formats.
- **AWS Region** – (Optional) The AWS Region where the Lambda function is located. If you don't specify an AWS Region value and it's not specified in the function ARN, then Aurora uses the same AWS Region as the DB cluster.

For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).

To hold the Lambda function name information, you can use the `aws_commons.create_lambda_function_arn` function. This function creates an `aws_commons._lambda_function_arn_1` composite structure to store the name information, as shown following.

```
psql=> SELECT aws_commons.create_lambda_function_arn('my-function',
   'us-west-2') AS aws_lambda_arn_1 \gset
psql=> SELECT aws_commons.create_lambda_function_arn('123456789012:function:my-function',
   'us-west-2') AS lambda_partial_arn_1 \gset
psql=> SELECT aws_commons.create_lambda_function_arn('arn:aws:lambda:us-west-2:123456789012:function:my-function'
   ) AS lambda_arn_1 \gset
```

You can later provide any of these values as a parameter in calls to the `aws_lambda.invoke` function. For examples, see Invoking Lambda functions (p. 1104).
Giving Aurora access to Lambda

To use a Lambda function, give your PostgreSQL DB cluster permission to access Lambda. To do this, use the following procedure.

**To give a PostgreSQL DB cluster access to Lambda**

1. Create an IAM policy.

   This policy provides the permissions that allow your PostgreSQL DB cluster to invoke Lambda functions.

   As part of creating this policy, take the following steps:

   a. Include in the policy the required action `lambda:InvokeFunction` to allow Lambda invocation from your Aurora PostgreSQL DB cluster.

   b. Include the Amazon Resource Name (ARN) that identifies the Lambda function. The ARN format for accessing Lambda is: `arn:aws:lambda::<region>:<123456789012>:function:example_function/*`

   For more information on creating an IAM policy for Aurora PostgreSQL, see [Creating and using an IAM policy for IAM database access](#) See also [IAM Tutorial: Create and attach your first customer managed policy](#) in the [IAM User Guide](#).

   The following AWS CLI command creates an IAM policy named `rds-lambda-policy` with these options. It grants access to a function named `example_function`.

   ```bash
   aws iam create-policy --policy-name rds-lambda-policy --policy-document '{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": "AllowAuroraToExampleFunction",
           "Effect": "Allow",
           "Action": "lambda:InvokeFunction",
           "Resource": "arn:aws:lambda::<region>:<123456789012>:function:example_function"
       }
   ]
   }'
   ```

   After you create the policy, note the ARN of the policy. You need the ARN for a subsequent step when you attach the policy to an IAM role.

2. Create an IAM role.

   You do this so Aurora PostgreSQL can assume this IAM role on your behalf to access your Lambda function. For more information, see [Creating a role to delegate permissions to an IAM user](#) in the [IAM User Guide](#).

   The following example shows using the AWS CLI command to create a role named `rds-lambda-role`.

   ```bash
   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. Attach the IAM policy that you created to the IAM role that you created.

The following AWS CLI command attaches the policy created earlier to the role named rds-lambda-role. Replace your-policy-arn with the policy ARN that you noted in an earlier step.

```bash
aws iam attach-role-policy --policy-arn your-policy-arn --role-name rds-lambda-role
```

4. Add the IAM role to the DB cluster. You do so by using the AWS CLI, as described following.

Use the following CLI command to add the IAM role to the Aurora PostgreSQL DB cluster named my-db-cluster. Replace your-role-arn with the role ARN that you noted in a previous step. Use Lambda for the value of the --feature-name option, as shown following.

```bash
aws rds add-role-to-db-cluster \
  --db-cluster-identifier my-db-cluster \
  --feature-name Lambda \
  --role-arn your-role-arn \
  --region your-region
```

**Invoking Lambda functions**

Following, you can find some examples of calling the `aws_lambda.invoke` function. Before you use the `aws_lambda.invoke` function, be sure to complete the following prerequisites:

- Install the required PostgreSQL extensions as described in Overview of using a Lambda function (p. 1101).
- Determine which Lambda function to invoke as described in Specifying the Lambda function to use (p. 1102).
- Make sure that the DB cluster has invoke access to Lambda as described in Giving Aurora access to Lambda (p. 1103).

You can invoke a Lambda function synchronously or asynchronously. You control this with the following values for the `aws_lambda.invoke` function's `invocation_type` parameter:

- The RequestResponse type of invocation for a Lambda function is synchronous and returns a response payload in the result of the `aws_lambda.invoke` function. Use the RequestResponse invocation type when your workflow depends on receiving the Lambda function result immediately. Most of the following examples use synchronous invocation.

  The RequestResponse type of invocation is the default.

- The Event type of invocation for a Lambda function is asynchronous and returns immediately without a returned payload. Use the Event type of invocation when you don’t need to know the result of the Lambda function before your workflow moves on. For an example of asynchronous invocation, see Asynchronous event invocation of Lambda functions (p. 1105).

The following `aws_lambda.invoke` examples use a `aws_lambda_arn_1` structure, which contains the identifying information for the Lambda function. To create the structure, use the `aws_commons.create_lambda_function_arn` function. For an example of using the `aws_commons.create_lambda_function_arn` function, see Specifying the Lambda function to use (p. 1102).
Invoking Lambda functions

Topics
- Synchronous RequestResponse invocation of Lambda functions (p. 1105)
- Asynchronous event invocation of Lambda functions (p. 1105)
- Requesting a Lambda execution log in a function response (p. 1105)
- Including client context in a Lambda function (p. 1105)
- Invoking a specific version of a Lambda function (p. 1106)
- Lambda function error handling (p. 1106)

Synchronous RequestResponse invocation of Lambda functions

Following is an example of a synchronous Lambda function invocation. The following two `aws_lambda.invoke` function call results are the same.

```sql
psql=> SELECT * FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"} '::json);
psql=> SELECT * FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"} '::json, 'RequestResponse');
```

The parameters are described as follows:
- `:'aws_lambda_arn_1'` – This parameter is a structure that identifies the Lambda function to call. This example uses a variable to identify the previously created structure. You can instead create the structure by including the `aws_commons.create_lambda_function_arn` function call inline within the `aws_lambda.invoke` function call as follows.

```sql
psql=> SELECT * FROM aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-function', 'us-west-2'),
    '{"body": "Hello from Postgres!"} '::json);
```

- `{"body": "Hello from Postgresql!"} '::json – The JSON payload to pass to the Lambda function.
- `'RequestResponse'` – The Lambda invocation type.

Asynchronous event invocation of Lambda functions

Following is an example of an asynchronous Lambda function invocation. The `Event` invocation type schedules the Lambda function invocation with the specified input payload and returns immediately. Use the `Event` invocation type in certain workflows that don't depend on the results of the Lambda function.

```sql
psql=> SELECT * FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"} '::json, 'Event');
```

Requesting a Lambda execution log in a function response

You can request to include the last 4 KB of the execution log in the function response, as shown following.

```sql
psql=> 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');
```
Set the `aws_lambda.invoke` function's `log_type` parameter to `Tail` to include the execution log in the response. The default value for the `log_type` parameter is `None`.

The `log_result` that's returned is a base64 encoded string. You can decode the contents using a combination of the `decode` and `convert_from` PostgreSQL functions.

**Including client context in a Lambda function**

You can pass in client context information that is separate from the payload, as shown following.

```sql
psql=> 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');
```

To include client context, use a JSON object for the `aws_lambda.invoke` function's `context` parameter.

**Invoking a specific version of a Lambda function**

For an example of invoking a specific version of a Lambda function, see the following.

```sql
psql=> SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from Postgres!":':json, 'RequestResponse', 'None', NULL, 'custom_version');
```

To identify a Lambda function's version, use the `aws_lambda.invoke` function's `qualifier` parameter. In this example, `custom_version` is an alias or version that identifies the version of the function to invoke.

You can instead supply a Lambda function qualifier with the function name information as follows.

```sql
psql=> SELECT * FROM aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-function:custom_version', 'us-west-2'), '{"body": "Hello from Postgres!":':json
```

**Lambda function error handling**

If a Lambda function throws an exception during request processing, `aws_lambda.invoke` fails with a PostgreSQL error such as the following.

```sql
psql=> SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from Postgres!":':json);
ERROR:  lambda invocation failed
```

**Function reference**

Following is the reference for the functions Aurora PostgreSQL uses to invoke Lambda functions.

**Functions**

- `aws_lambda.invoke` (p. 1107)
- `aws_commons.create_lambda_function_arn` (p. 1109)
**aws_lambda.invoke**

Runs a Lambda function for an Aurora PostgreSQL DB cluster.

For more details about invoking Lambda functions, see also `invoke` in the *AWS Lambda Developer Guide*.

**Syntax**

**JSON**

```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)
```

**JSONB**

```json
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)
```
**Input parameters**

*function_name*

The identifying name of the Lambda function. The value can be the function name, an ARN, or a partial ARN. For a listing of possible formats, see Lambda function name formats in the AWS Lambda Developer Guide.

*payload*

The input for the Lambda function. The format can be JSON or JSONB. For more information, see JSON Types in the PostgreSQL documentation.

*region*

(Optional) The Lambda Region for the function. By default Aurora resolves the Region from the full ARN in the function_name or it uses the Aurora PostgreSQL DB instance Region. If this Region value conflicts with the one provided in the function_name ARN, an error is raised.

*invocation_type*

The invocation type of the Lambda function. The value is case-sensitive. Possible values include the following:

- **RequestResponse** – The default. This type of invocation for a Lambda function is synchronous and returns a response payload in the result. Use the RequestResponse invocation type when your workflow depends on receiving the Lambda function result immediately.
- **Event** – This type of invocation for a Lambda function is asynchronous and returns immediately without a returned payload. Use the Event invocation type when you don't need results of the Lambda function before your workflow moves on.
- **DryRun** – This type of invocation tests access without running the Lambda function.

*log_type*

The type of Lambda log to return in the log_result output parameter. The value is case-sensitive. Possible values include the following:

- **Tail** – The returned log_result output parameter will include the last 4 KB of the execution log.
- **None** – No Lambda log information is returned.

*context*

Client context in JSON or JSONB format. Fields to use include than custom and env.

*qualifier*

A qualifier that identifies a Lambda function's version to be invoked. If this value conflicts with one provided in the function_name ARN, an error is raised.

**Output parameters**

*status_code*

An HTTP status response code. For more information, see Lambda Invoke response elements in the AWS Lambda Developer Guide.

*payload*

The information returned from the Lambda function that ran. The format is in JSON or JSONB.

*executed_version*

The version of the Lambda function that ran.
**log_result**

The execution log information returned if the `log_type` value is `Tail` when the Lambda function was invoked. The result contains the last 4 KB of the execution log encoded in Base64.

**aws_commons.create_lambda_function_arn**

Creates an `aws_commons._lambda_function_arn_1` structure to hold Lambda function name information. You can use the results of the `aws_commons.create_lambda_function_arn` function in the `function_name` parameter of the `aws_lambda.invoke` function.

**Syntax**

```sql
aws_commons.create_lambda_function_arn(
    function_name TEXT,
    region TEXT DEFAULT NULL
) 
RETURNS aws_commons._lambda_function_arn_1
```

**Input parameters**

**function_name**

A required text string containing the Lambda function name. The value can be a function name, a partial ARN, or a full ARN.

**region**

An optional text string containing the AWS Region that the Lambda function is in. For a listing of AWS Region names and associated values, see Regions and Availability Zones (p. 5).

---

**Upgrading the PostgreSQL DB engine for Aurora PostgreSQL**

When Aurora PostgreSQL supports a new version of a database engine, you can upgrade your DB clusters to the new version. There are two kinds of upgrades for PostgreSQL DB clusters: major version upgrades and minor version upgrades.

**Major version upgrades** can contain database changes that are not backward-compatible with existing applications. As a result, you must manually perform major version upgrades of your DB instances. You can initiate a major version upgrade by modifying your DB cluster. However, before you perform a major version upgrade, we recommend that you follow the steps described in How to perform a major version upgrade (p. 1111).

In contrast, **minor version upgrades** include only changes that are backward-compatible with existing applications. You can initiate a minor version upgrade manually by modifying your DB cluster. Or you can enable the **Auto minor version upgrade** option when creating or modifying a DB cluster. Doing so means that your DB cluster is automatically upgraded after Aurora PostgreSQL tests and approves the new version. For more details, see Automatic minor version upgrades for PostgreSQL (p. 1115). For information about manually performing a minor version upgrade, see Manually upgrading the Aurora PostgreSQL engine (p. 1114).

Aurora DB clusters that are configured as logical replication publishers or subscribers can't undergo a major version upgrade. For more information, see Using PostgreSQL logical replication with Aurora (p. 1035).
You can do the following Aurora PostgreSQL major version upgrades:

- Upgrade from version 9.6 minor versions 9.6.9 and greater, to version 10 minor versions 10.11 or greater.
- Upgrade from version 10 minor versions 10.7 and greater, to version 11 minor versions 11.7 or greater.

For how to determine valid upgrade targets, see Determining which engine version to upgrade to (p. 1111).

**Topics**

- Overview of upgrading Aurora PostgreSQL (p. 1110)
- PostgreSQL version numbers (p. 1110)
- Determining which engine version to upgrade to (p. 1111)
- How to perform a major version upgrade (p. 1111)
- Manually upgrading the Aurora PostgreSQL engine (p. 1114)
- Automatic minor version upgrades for PostgreSQL (p. 1115)
- Upgrading PostgreSQL extensions (p. 1115)

**Overview of upgrading Aurora PostgreSQL**

Major version upgrades can contain database changes that are not backward-compatible with previous versions of the database. This functionality can cause your existing applications to stop working correctly. As a result, Amazon Aurora doesn't apply major version upgrades automatically. To perform a major version upgrade, you modify your DB cluster manually.

To safely upgrade your DB instances, Aurora PostgreSQL uses the pg_upgrade utility described in the PostgreSQL documentation. After the writer upgrade completes, each reader instance experiences a brief outage while it's upgraded to the new major version automatically.

Aurora PostgreSQL takes a DB cluster snapshot before the upgrade begins. If you want to return to a previous version after an upgrade is complete, you can restore the DB cluster from this snapshot created before the upgrade, or you can restore the DB cluster to a specific point in time before the upgrade started. For more information, see Restoring from a DB cluster snapshot (p. 420) or Restoring a DB cluster to a specified time (p. 454).

During the major version upgrade process, a cloned volume is allocated. If the upgrade fails for some reason, such as due to a schema incompatibility, Aurora PostgreSQL uses this clone to roll back the upgrade. Note, when more than 15 clones of a source volume are allocated, subsequent clones become full copies and will take longer. This can cause the upgrade process to take longer as well. If Aurora PostgreSQL rolls back the upgrade, be aware of the following:

- You may see billing entries and metrics for both the original volume and the cloned volume allocated during the upgrade. Aurora PostgreSQL will clean up the extra volume after the cluster backup retention window is beyond the time of the upgrade.
- The next cross region snapshot copy from this cluster will be a full copy instead of an incremental copy.

**PostgreSQL version numbers**

To determine the current Aurora PostgreSQL version and PostgreSQL database engine version of a DB cluster, see Identifying your version of Amazon Aurora PostgreSQL (p. 1148).
The version numbering sequence for the PostgreSQL database engine is as follows:

- For PostgreSQL versions 10 and later, the engine version number is in the form `major.minor`. The major version number is the integer part of the version number. The minor version number is the fractional part of the version number.

  A major version upgrade increases the integer part of the version number, such as upgrading from `10.minor` to `11.minor`.

- For PostgreSQL versions earlier than 10, the engine version number is in the form `major.major.minor`. The major engine version number is both the integer and the first fractional part of the version number. For example, `9.6` is a major version. The minor version number is the third part of the version number. For example, for version `9.6.12`, the `12` is the minor version number.

  A major version upgrade increases the major part of the version number. For example, an upgrade from `9.6.12` to `10.7` is a major version upgrade, where `9.6` and `10` are the major version numbers.

**Determining which engine version to upgrade to**

To determine which major engine version that you can upgrade your database to, use the `describe-db-engine-versions` CLI command. In the output, a `ValidUpgradeTarget` array contains the target versions. If the `IsMajorVersionUpgrade` value is true, you can do a major version upgrade to the associated `EngineVersion`. If the array is empty, you can't do a major version upgrade. You first upgrade to a minor version that has a major version upgrade path.

For example, the following command displays the major engine versions available for upgrading a DB cluster currently running the Aurora PostgreSQL engine version `9.6.12`.

**Example**

For Linux, macOS, or Unix:

```bash
code
aws rds describe-db-engine-versions --engine aurora-postgresql --engine-version 9.6.12  
--query 'DBEngineVersions[].ValidUpgradeTarget[?IsMajorVersionUpgrade == `true`]'
```

For Windows:

```bash
code
aws rds describe-db-engine-versions --engine aurora-postgresql --engine-version 9.6.12  ^
--query "DBEngineVersions[].ValidUpgradeTarget[?IsMajorVersionUpgrade == `true`]"
```

**How to perform a major version upgrade**

Major version upgrades can contain database changes that are not backward-compatible with previous versions of the database. This functionality can cause your existing applications to stop working correctly. As a result, Amazon Aurora doesn't apply major version upgrades automatically. To perform a major version upgrade, you modify your DB cluster manually.

Before applying an upgrade to your production DB clusters, make sure that you thoroughly test any upgrade to verify that your applications work correctly.

We recommend the following process when upgrading an Aurora PostgreSQL DB cluster:

1. Have a version-compatible parameter group ready.

   If you are using a custom DB instance or DB cluster parameter group, you have two options:
• Specify the default DB instance, DB cluster parameter group, or both for the new DB engine version.
• Create your own custom parameter group for the new DB engine version.

If you associate a new DB instance or DB cluster parameter group as a part of the upgrade request, make sure to reboot the database after the upgrade completes to apply the parameters. If a DB instance needs to be rebooted to apply the parameter group changes, the instance's parameter group status shows `pending-reboot`. You can view an instance's parameter group status in the console or by using a CLI command such as `describe-db-instances` or `describe-db-clusters`.

2. Check for unsupported usage:
• Commit or roll back all open prepared transactions before attempting an upgrade. You can use the following query to verify that there are no open prepared transactions on your instance.

```sql
SELECT count(*) FROM pg_catalog.pg_prepared_xacts;
```

• Remove all uses of the `reg*` data types before attempting an upgrade. Except for `regtype` and `regclass`, you can't upgrade the `reg*` data types. The `pg_upgrade` utility can't persist this data type, which is used by Amazon Aurora to do the upgrade. For more information about the `pg_upgrade` utility, see the PostgreSQL documentation.

To verify that there are no uses of unsupported `reg*` data types, use the following query for each database.

```sql
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');
```

3. Perform a backup.

The upgrade process creates a DB cluster snapshot of your DB cluster during upgrading. If you also want to do a manual backup before the upgrade process, see Creating a DB cluster snapshot (p. 418) for more information.

4. Upgrade certain extensions to the latest available version before performing the major version upgrade. The extensions to update include the following:
• pgRouting
• postGIS

Run the following command for each extension that you are using.

```sql
ALTER EXTENSION PostgreSQL-extension UPDATE TO 'new-version'
```

For more information, see Upgrading PostgreSQL extensions (p. 1115).

5. If you're upgrading to version 11.x, drop the extensions that it doesn't support before performing the major version upgrade. The extensions to drop include:
• chkpass
• tsearch2
6. Drop unknown data types, depending on your target version.

PostgreSQL version 10 stopped supporting the unknown data type. If a version 9.6 database uses the unknown data type, an upgrade to a version 10 shows an error message such as the following.

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.

To find the unknown data type in your database so you can remove the offending column or change it to a supported data type, use the following SQL code.

```
SELECT DISTINCT data_type FROM information_schema.columns WHERE data_type ILIKE 'unknown';
```

7. Perform a dry run upgrade.

We highly recommend testing a major version upgrade on a duplicate of your production database before trying the upgrade on your production database. To create a duplicate test instance, you can either restore your database from a recent snapshot or clone your database. For more information, see Restoring from a snapshot (p. 421) or Cloning an Aurora DB cluster volume (p. 355).

For more information, see Manually upgrading the Aurora PostgreSQL engine (p. 1114).

8. Upgrade your production instance.

When your dry-run major version upgrade is successful, you should be able to upgrade your production database with confidence. For more information, see Manually upgrading the Aurora PostgreSQL engine (p. 1114).

Note
During the upgrade process, you can't do a point-in-time restore of your cluster. Aurora PostgreSQL takes a DB cluster snapshot during the upgrade process if your backup retention period is greater than 0. You can perform a point-in-time restore to times before the upgrade began and after the automatic snapshot of your instance has completed.

For information about an upgrade in progress, you can use Amazon RDS to view two logs that the pg_upgrade utility produces. These are pg_upgrade_internal.log and pg_upgrade_server.log. Amazon Aurora appends a timestamp to the file name for these logs. You can view these logs as you can any other log. For more information, see Amazon Aurora database log files (p. 618).

9. Upgrade PostgreSQL extensions. The PostgreSQL upgrade process doesn't upgrade any PostgreSQL extensions. For more information, see Upgrading PostgreSQL extensions (p. 1115).

After you complete a major version upgrade, we recommend the following:

- Run the ANALYZE operation to refresh the pg_statistic table.
- If you upgraded to PostgreSQL version 10, run REINDEX on any hash indexes you have. Hash indexes were changed in version 10 and must be rebuilt. To locate invalid hash indexes, run the following SQL for each database that contains hash indexes.

```
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;

- Consider testing your application on the upgraded database with a similar workload to verify that everything works as expected. After the upgrade is verified, you can delete this test instance.

Manually upgrading the Aurora PostgreSQL engine

To perform an upgrade of an Aurora PostgreSQL DB cluster, use the following instructions for the AWS Management Console, the AWS CLI, or the RDS API.

**Console**

**To upgrade the engine version of a DB cluster by using the console**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**, and then choose the DB cluster that you want to upgrade.
3. Choose **Modify**. The **Modify DB cluster** page appears.
4. For **DB engine version**, choose the new version.
5. Choose **Continue** and check the summary of modifications.
6. To apply the changes immediately, choose **Apply immediately**. Choosing this option can cause an outage in some cases. For more information, see Modifying an Amazon Aurora DB cluster (p. 327).
7. On the confirmation page, review your changes. If they are correct, choose **Modify Cluster** to save your changes.
   
   Or choose **Back** to edit your changes or **Cancel** to cancel your changes.

**AWS CLI**

To upgrade the engine version of a DB cluster, use the CLI modify-db-cluster command. Specify the following parameters:

- `--db-cluster-identifier` – the name of the DB cluster.
- `--engine-version` – the version number of the database engine to upgrade to. For information about valid engine versions, use the AWS CLI `describe-db-engine-versions` command.
- `--allow-major-version-upgrade` – a required flag when the `--engine-version` parameter is a different major version than the DB cluster's current major version.
- `--no-apply-immediately` – apply changes during the next maintenance window. To apply changes immediately, use `--apply-immediately`.

**Example**

For Linux, macOS, or Unix:

```bash
aws rds modify-db-cluster \  
   --db-cluster-identifier mydbcluster \  
   --engine-version new_version \  
   --allow-major-version-upgrade \  
   --no-apply-immediately
```

For Windows:

```bash
aws rds modify-db-cluster ^
   --db-cluster-identifier mydbcluster ^
```

1114
Amazon Aurora User Guide for Aurora
Automatic minor version upgrades
--engine-version new_version ^
--allow-major-version-upgrade ^
--no-apply-immediately

RDS API
To upgrade the engine version of a DB cluster, use the ModifyDBCluster operation. Specify the following
parameters:
• DBClusterIdentifier – the name of the DB cluster, for example mydbcluster.
• EngineVersion – the version number of the database engine to upgrade to. For information about
valid engine versions, use the DescribeDBEngineVersions operation.
• AllowMajorVersionUpgrade – a required ﬂag when the EngineVersion parameter is a diﬀerent
major version than the DB cluster's current major version.
• ApplyImmediately – whether to apply changes immediately or during the next maintenance
window. To apply changes immediately, set the value to true. To apply changes during the next
maintenance window, set the value to false.

Automatic minor version upgrades for PostgreSQL
If you enable the Auto minor version upgrade option when creating or modifying a DB cluster, you can
have your cluster automatically upgraded.
For each PostgreSQL major version, one minor version is designated by Amazon Aurora as the automatic
upgrade version. After a minor version has been tested and approved by Amazon Aurora, the minor
version upgrade occurs automatically during your maintenance window. Aurora doesn't automatically
set newer released minor versions as the automatic upgrade version. Before Aurora designates a newer
automatic upgrade version, several criteria are considered, such as the following:
• Known security issues
• Bugs in the PostgreSQL community version
• Overall ﬂeet stability since the minor version was released
You can use the following AWS CLI command and script to determine the current automatic upgrade
minor versions.
aws rds describe-db-engine-versions --engine aurora-postgresql | grep -A 1 AutoUpgrade|
grep -A 2 true |grep PostgreSQL | sort --unique | sed -e 's/"Description": "//g'

Note

If no results are returned, there is no automatic minor version upgrade available and scheduled.
A PostgreSQL DB instance is automatically upgraded during your maintenance window if the following
criteria are met:
• The DB cluster has the Auto minor version upgrade option enabled.
• The DB cluster is running a minor DB engine version that is less than the current automatic upgrade
minor version.

Upgrading PostgreSQL extensions
A PostgreSQL engine upgrade doesn't upgrade any PostgreSQL extensions. To update an extension after
an engine upgrade, use the ALTER EXTENSION UPDATE command.

1115


Note
If you are running the PostGIS extension in your Amazon RDS PostgreSQL DB instance, make sure that you follow the PostGIS upgrade instructions in the PostGIS documentation before you upgrade the extension.

To upgrade an extension, use the following command.

```
ALTER EXTENSION extension_name UPDATE TO 'new_version';
```

To list your currently installed extensions, use the PostgreSQL `pg_extension` catalog in the following command.

```
SELECT * FROM pg_extension;
```

To view a list of the specific extension versions that are available for your installation, use the PostgreSQL `pg_available_extension_versions` view in the following command.

```
SELECT * FROM pg_available_extension_versions;
```

Best practices with Amazon Aurora PostgreSQL

This topic includes information on best practices and options for using or migrating data to an Amazon Aurora PostgreSQL DB cluster.

Fast failover with Amazon Aurora PostgreSQL

There are several things you can do to make a failover perform faster with Aurora PostgreSQL. This section discusses each of the following ways:

- Aggressively set TCP keepalives to ensure that longer running queries that are waiting for a server response will be stopped before the read timeout expires in the event of a failure.
- Set the Java DNS caching timeouts aggressively to ensure the Aurora read-only endpoint can properly cycle through read-only nodes on subsequent connection attempts.
- Set the timeout variables used in the JDBC connection string as low as possible. Use separate connection objects for short and long running queries.
- Use the provided read and write Aurora endpoints to establish a connection to the cluster.
- Use RDS APIs to test application response on server side failures and use a packet dropping tool to test application response for client-side failures.

Topics
- Setting TCP keepalives parameters (p. 1116)
- Configuring your application for fast failover (p. 1117)
- Testing failover (p. 1121)
- Fast failover example (p. 1121)

Setting TCP keepalives parameters

The TCP keepalive process is simple: when you set up a TCP connection, you associate a set of timers. When the keepalive timer reaches zero, you send a keepalive probe packet. If you receive a reply to your keepalive probe, you can assume that the connection is still up and running.
Enabling TCP keepalive parameters and setting them aggressively ensures that if your client is no longer able to connect to the database, then any active connections are quickly closed. This action allows the application to react appropriately, such as by picking a new host to connect to.

You need to set the following TCP keepalive parameters:

- `tcp_keepalive_time` controls the time, in seconds, after which a keepalive packet is sent when no data has been sent by the socket (ACKs are not considered data). We recommend the following setting:
  
  `tcp_keepalive_time = 1`

- `tcp_keepalive_intvl` controls the time, in seconds, between sending subsequent keepalive packets after the initial packet is sent (set using the `tcp_keepalive_time` parameter). We recommend the following setting:
  
  `tcp_keepalive_intvl = 1`

- `tcp_keepalive_probes` is the number of unacknowledged keepalive probes that occur before the application is notified. We recommend the following setting:
  
  `tcp_keepalive_probes = 5`

These settings should notify the application within five seconds when the database stops responding. A higher `tcp_keepalive_probes` value can be set if keepalive packets are often dropped within the application’s network. This subsequently increases the time it takes to detect an actual failure, but allows for more buffer in less reliable networks.

**Setting TCP keepalive parameters on Linux**

1. When testing how to configure the TCP keepalive parameters, we recommend doing so via the command line with the following commands: This suggested configuration is system wide, meaning that it affects all other applications that create sockets with the SO_KEEPALIVE option on.

   ```bash
   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. After you’ve found a configuration that works for your application, persist these settings by adding the following lines to `/etc/sysctl.conf`, including any changes you made:

   ```conf
   tcp_keepalive_time = 1
   tcp_keepalive_intvl = 1
   tcp_keepalive_probes = 5
   ```

For information on setting TCP keepalive parameters on Windows, see [Things you May want to know about TCP keepalive](#).

**Configuring your application for fast failover**

This section discusses several Aurora PostgreSQL specific configuration changes you can make. Documentation for general setup and configuration of the JDBC driver is available from the [PostgreSQL JDBC site](#).

**Topics**

- [Reducing DNS cache timeouts](#)(p. 1118)
- [Setting an Aurora PostgreSQL connection string for fast failover](#)(p. 1118)
- [Other options for obtaining the host string](#)(p. 1119)
Reducing DNS cache timeouts

When your application tries to establish a connection after a failover, the new Aurora PostgreSQL writer will be a previous reader, which can be found using the Aurora read only endpoint before DNS updates have fully propagated. Setting the java DNS TTL to a low value helps cycle between reader nodes on subsequent connection attempts.

```java
// 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");
```

Setting an Aurora PostgreSQL connection string for fast failover

To make use of Aurora PostgreSQL fast failover, your application's connection string should have a list of hosts (highlighted in bold in the following example) instead of just a single host. Here is an example connection string you could use to connect to an Aurora PostgreSQL cluster:

```
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&loadBalanceHosts=true
```

For best availability and to avoid a dependency on the RDS API, the best option for connecting is to maintain a file with a host string that your application reads from when you establish a connection to the database. This host string would have all the Aurora endpoints available for the cluster. For more information about Aurora endpoints, see Amazon Aurora connection management (p. 24). For example, you could store the endpoints in a file locally like the following:

```
myauroracluster.cluster-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432,
myauroracluster.cluster-ro-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432
```

Your application would read from this file to populate the host section of the JDBC connection string. Renaming the DB Cluster causes these endpoints to change; ensure that your application handles that event should it occur.

Another option is to use a list of DB instance nodes:

```
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
```

The benefit of this approach is that the PostgreSQL JDBC connection driver will loop through all nodes on this list to find a valid connection, whereas when using the Aurora endpoints only two nodes will be tried per connection attempt. The downside of using DB instance nodes is that if you add or remove nodes from your cluster and the list of instance endpoints becomes stale, the connection driver may never find the correct host to connect to.

Set the following parameters aggressively to help ensure that your application doesn't wait too long to connect to any one host.

- **targetServerType** – Use this parameter to control whether the driver connects to a write or read node. To ensure your applications will reconnect only to a write node, set the targetServerType value to primary.
Values for the `targetServerType` parameter include primary, secondary, any, and `preferSecondary`. The `preferSecondary` value attempts to establish a connection to a reader first but connects to the writer if no reader connection can be established.

- **LoginTimeout** – Controls how long your application waits to login to the database after a socket connection has been established.
- **connectTimeout** – Controls how long the socket waits to establish a connection to the database.

You can modify other application parameters to speed up the connection process, depending on how aggressive you want your application to be.

- **cancelSignalTimeout** – In some applications, you may want to send a "best effort" cancel signal on a query that has timed out. If this cancel signal is in your failover path, you should consider setting it aggressively to avoid sending this signal to a dead host.
- **socketTimeout** – This parameter controls how long the socket waits for read operations. This parameter can be used as a global "query timeout" to ensure no query waits longer than this value. A good practice is to have one connection handler that runs short lived queries and sets this value lower, and to have another connection handler for long running queries with this value set much higher. Then, you can rely on TCP keepalive parameters to stop long running queries if the server goes down.
- **tcpKeepAlive** – Enable this parameter to ensure the TCP keepalive parameters that you set are respected.
- **loadBalanceHosts** – When set to true, this parameter has the application connect to a random host chosen from a list of candidate hosts.

### Other options for obtaining the host string

You can get the host string from several sources, including the `aurora_replica_status` function and by using the Amazon RDS API.

Your application can connect to any DB instance in the DB Cluster and query the `aurora_replica_status` function to determine who the writer of the cluster is, or to find any other reader nodes in the cluster. You can use this function to reduce the amount of time it takes to find a host to connect to, though in certain scenarios the `aurora_replica_status` function may show out of date or incomplete information in certain network failure scenarios.

A good way to ensure your application can find a node to connect to is to attempt to connect to the `clusterwriterendpoint` and then the `clusterreaderendpoint` until you can establish a readable connection. These endpoints do not change unless you rename your DB Cluster, and thus can generally be left as static members of your application or stored in a resource file that your application reads from.

Once you establish a connection using one of these endpoints, you can call the `aurora_replica_status` function to get information about the rest of the cluster. For example, the following command retrieves information with the `aurora_replica_status` function.

```sql
postgres=> SELECT server_id, session_id, highest_lsn_rcvd, cur_replay_latency_in_usec, now(), last_update_timestamp FROM aurora_replica_status();
```

<table>
<thead>
<tr>
<th>server_id</th>
<th>session_id</th>
<th>highest_lsn_rcvd</th>
<th>cur_replay_latency</th>
<th>now</th>
<th>last_update_timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>mynode-1</td>
<td>3e3c5044-02e2-11e7-b70d-95172646d6ca</td>
<td>594220999</td>
<td>19:50:24.695322+00</td>
<td>2017-03-07 19:50:23+00</td>
<td></td>
</tr>
<tr>
<td>mynode-2</td>
<td>1efdd188-02e4-11e7-becd-f12d7c88a28a</td>
<td>594221001</td>
<td>201421</td>
<td>2017-03-07</td>
<td></td>
</tr>
</tbody>
</table>
So for example, the hosts section of your connection string could start with both the writer and reader cluster endpoints:

```
myauroracircle.cluster-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432,
myauroracircle.cluster-ro-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432
```

In this scenario, your application would attempt to establish a connection to any node type, primary or secondary. Once connected, a good practice is to first examine the read/write status of the node by querying for the result of the command `SHOW transaction_read_only`.

If the return value of the query is `OFF`, then you've successfully connected to the primary node. If the return value is `ON`, and your application requires a read/write connection, you can then call the `aurora_replica_status` function to determine the `server_id` that has `session_id='MASTER_SESSION_ID'`. This function gives you the name of the primary node. You can use this in conjunction with the 'endpointPostfix' described below.

One thing to be aware of is when you connect to a replica that has stale data. When this happens, the `aurora_replica_status` function may show out-of-date information. A threshold for staleness can be set at the application level and examined by looking at the difference between the server time and the `last_update_time`. In general, your application should avoid flipping between two hosts due to conflicting information returned by the `aurora_replica_status` function. Your application should try all known hosts first instead of blindly following the data returned by the `aurora_replica_status` function.

**RDS API**

You can programmatically find the list of instances by using the AWS Java SDK, specifically the `DescribeDbClusters` API. Here's a small example of how you might do this in java 8:

```java
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(","));
```

The variable `endpointPostfix` can be a constant that your application sets, or can be obtained by querying the `DescribeDBInstances` API for a single instance in your cluster. This value remains
constant within a region and for an individual customer, so it would save an API call to simply keep this constant in a resource file that your application reads from. In the example above, it would be set to:

```
.cksc6x1mwcyw.us-east-1-beta.rds.amazonaws.com
```

For availability purposes, a good practice is to default to using the Aurora endpoints of your DB Cluster if the API is not responding, or is taking too long to respond. The endpoints are guaranteed to be up to date within the time it takes to update the DNS record. This is typically less than 30 seconds. You can store this in a resource file that your application consumes.

## Testing failover

In all cases you must have a DB cluster with two or more DB instances in it.

From the server side, certain APIs can cause an outage that can be used to test how your applications responds:

- **FailoverDBCluster** - Will attempt to promote a new DB Instance in your DB Cluster to writer

  ```java
  public void causeFailover() {
      /*
      * For more details about setting up an RDS client, see: http://docs.aws.amazon.com/
      * sdk-for-java/v1/developer-guide/basics.html
      */
      final AmazonRDS rdsClient = AmazonRDSClientBuilder.defaultClient();
      FailoverDBClusterRequest request = new FailoverDBClusterRequest();
      request.setDBClusterIdentifier("cluster-identifier");
      rdsClient.failoverDBCluster(request);
  }
  ```

- **RebootDBInstance** - Failover is not guaranteed in this API. It will shutdown the database on the writer, though, and can be used to test how your application responds to connections dropping (note that the **ForceFailover** parameter is not applicable for Aurora engines and instead should use the FailoverDBCluster API)

- **ModifyDBCluster** - Modifying the **Port** will cause an outage when the nodes in the cluster begin listening on a new port. In general your application can respond to this failure by ensuring that only your application controls port changes and can appropriately update the endpoints it depends on, by having someone manually update the port when they make modifications at the API level, or by querying the RDS API in your application to determine if the port has changed.

- **ModifyDBInstance** - Modifying the **DBInstanceClass** will cause an outage

- **DeleteDBInstance** - Deleting the primary/writer will cause a new DB Instance to be promoted to writer in your DB Cluster

From the application/client side, if using Linux, you can test how the application responds to sudden packet drops based on port, host, or if tcp keepalive packets are not sent or received by using iptables.

## Fast failover example

The following code sample shows how an application might set up an Aurora PostgreSQL driver manager. The application would call `getConnection()` when it needs a connection. A call to this function can fail to find a valid host, such as when no writer is found but the `targetServerType` parameter was set to `primary`. The calling application should simply retry calling the function. This can easily be wrapped into a connection pooler to avoid pushing the retry behavior onto the application.
Most connection poolers allow you to specify a JDBC connection string, so your application could call into `getJdbcConnectionString()` and pass that to the connection pooler to make use of faster failover on Aurora PostgreSQL.

```java
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();
        }

        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));

        Statement st = conn.createStatement();
        st.executeUpdate("set statement_timeout to " + queryTimeout.getMillis());
        st.close();

        return conn;
    }

    private static String urlFormat = "jdbc:postgresql://%s";

    private static String getJdbcConnectionString(String targetServerType, Duration queryTimeout) {
        return urlFormat + "//" + targetServerType + ":5432/postgres";
    }
}
```
Troubleshooting storage issues

If the amount of memory required by a sort or index creation operation exceeds the amount of memory available, Aurora PostgreSQL writes the excess data to storage. When it writes the data it uses the same storage space it uses for storing error and message logs. If your sorts or index creation functions exceed the memory available, you could develop a local storage shortage. If you experience issues with Aurora PostgreSQL running out of storage space, you can either reconfigure your data sorts to use more memory, or reduce the data retention period for your PostgreSQL log files. For more information about changing the log retention period see, PostgreSQL database log files (p. 627).

If your Aurora cluster is larger than 40 TB, don't use db.t2 or db.t3 instance classes.
Using Kerberos authentication with Aurora PostgreSQL

You can use Kerberos authentication to authenticate users when they connect to your DB cluster running PostgreSQL. In this case, your DB instance works with AWS Directory Service for Microsoft Active Directory to enable Kerberos authentication. AWS Directory Service for Microsoft Active Directory is also called AWS Managed Microsoft AD.

You create an AWS Managed Microsoft AD directory to store user credentials. You then provide to your PostgreSQL DB cluster the Active Directory's domain and other information. When users authenticate with the PostgreSQL DB cluster, authentication requests are forwarded to the AWS Managed Microsoft AD directory.

Keeping all of your credentials in the same directory can save you time and effort. You have a centralized place for storing and managing credentials for multiple DB clusters. Using a directory can also improve your overall security profile.

You can also access credentials from your own on-premises Microsoft Active Directory. To do so you create a trusting domain relationship so that the AWS Managed Microsoft AD directory trusts your on-premises Microsoft Active Directory. In this way, your users can access your PostgreSQL clusters with the same Windows single sign-on (SSO) experience as when they access workloads in your on-premises network.

Kerberos provides a different authentication method than AWS Identity and Access Management (IAM). A database can use either Kerberos or IAM authentication but not both. For more information about IAM authentication, see IAM database authentication (p. 1238).

Amazon Aurora supports Kerberos authentication for PostgreSQL DB clusters in the following AWS Regions:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Stockholm)
- South America (São Paulo)

Topics

- Overview of Kerberos authentication for PostgreSQL DB clusters (p. 1125)
- Setting up Kerberos authentication for PostgreSQL DB clusters (p. 1125)
- Managing a DB cluster in a Domain (p. 1135)
- Connecting to PostgreSQL with Kerberos authentication (p. 1136)
Overview of Kerberos authentication for PostgreSQL DB clusters

To set up Kerberos authentication for a PostgreSQL DB cluster, take the following steps, described in more detail later:

1. Use AWS Managed Microsoft AD to create an AWS Managed Microsoft AD directory. You can use the AWS Management Console, the AWS CLI, or the AWS Directory Service API to create the directory.

2. Create a role that provides Amazon Aurora access to make calls to your AWS Managed Microsoft AD directory. To do so, create an AWS Identity and Access Management (IAM) role that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`.

   For the IAM role to allow access, the AWS Security Token Service (AWS STS) endpoint must be activated in the correct AWS Region for your AWS account. AWS STS endpoints are active by default in all AWS Regions, and you can use them without any further actions. For more information, see Activating and deactivating AWS STS in an AWS Region in the IAM User Guide.

3. Create and configure users in the AWS Managed Microsoft AD directory using the Microsoft Active Directory tools. For more information about creating users in your Active Directory, see Manage users and groups in AWS Managed Microsoft AD in the AWS Directory Service Administration Guide.

4. If you plan to locate the directory and the DB instance in different AWS accounts or virtual private clouds (VPCs), configure VPC peering. For more information, see What is VPC peering? in the Amazon VPC Peering Guide.

5. Create or modify a PostgreSQL DB cluster either from the console, CLI, or RDS API using one of the following methods:
   - Creating a DB cluster and connecting to a database on an Aurora PostgreSQL DB cluster (p. 87)
   - Modifying an Amazon Aurora DB cluster (p. 327)
   - Restoring from a DB cluster snapshot (p. 420)
   - Restoring a DB cluster to a specified time (p. 454)

   When you create or modify the DB cluster, provide the domain identifier (`d-*` identifier) that was generated when you created your directory. Also provide the name of the IAM role that you created. You can locate the DB cluster in the same VPC as the directory or in a different AWS account or VPC.

6. Use the RDS master user credentials to connect to the PostgreSQL DB cluster. Create the user in PostgreSQL to be identified externally. Externally identified users can log in to the PostgreSQL DB cluster using Kerberos authentication.

Setting up Kerberos authentication for PostgreSQL DB clusters

You use AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) to set up Kerberos authentication for a PostgreSQL DB cluster. To set up Kerberos authentication, take the following steps.

Topics
- Step 1: Create a directory using AWS Managed Microsoft AD (p. 1126)
- Step 2: (Optional) create a trust for an on-premises Active Directory (p. 1129)
- Step 3: Create an IAM role for Amazon Aurora to access the AWS Directory Service (p. 1130)
- Step 4: Create and configure users (p. 1131)
- Step 5: Enable cross-VPC traffic between the directory and the DB instance (p. 1131)
- Step 6: Create or modify a PostgreSQL DB cluster (p. 1132)
• Step 7: Create Kerberos authentication PostgreSQL logins (p. 1134)
• Step 8: Configure a PostgreSQL client (p. 1134)

Step 1: Create a directory using AWS Managed Microsoft AD

AWS Directory Service creates a fully managed Active Directory in the AWS Cloud. When you create an AWS Managed Microsoft AD directory, AWS Directory Service creates two domain controllers and DNS servers for you. The directory servers are created in different subnets in a VPC. This redundancy helps make sure that your directory remains accessible even if a failure occurs.

When you create an AWS Managed Microsoft AD directory, AWS Directory Service performs the following tasks on your behalf:

• Sets up an Active Directory within your VPC.
• Creates a directory administrator account with the user name Admin and the specified password. You use this account to manage your directory.

  Important
  Make sure to save this password. AWS Directory Service doesn't store this password, and it can't be retrieved or reset.
• Creates a security group for the directory controllers.

When you launch AWS Directory Service for Microsoft Active Directory, AWS creates an Organizational Unit (OU) that contains all of your directory’s objects. This OU, which has the NetBIOS name that you entered when you created your directory, is located in the domain root. The domain root is owned and managed by AWS.

The Admin account that was created with your AWS Managed Microsoft AD directory has permissions for the most common administrative activities for your OU:

• Create, update, or delete users
• Add resources to your domain such as file or print servers, and then assign permissions for those resources to users in your OU
• Create additional OUs and containers
• Delegate authority
• Restore deleted objects from the Active Directory Recycle Bin
• Run Active Directory and Domain Name Service (DNS) modules for Windows PowerShell on the Active Directory Web Service

The Admin account also has rights to perform the following domain-wide activities:

• Manage DNS configurations (add, remove, or update records, zones, and forwarders)
• View DNS event logs
• View security event logs

To create a directory with AWS Managed Microsoft AD

1. In the AWS Directory Service console navigation pane, choose Directories, and then choose Set up directory.
2. Choose AWS Managed Microsoft AD. AWS Managed Microsoft AD is the only option currently supported for use with Amazon Aurora.
3. Choose Next.
4. On the **Enter directory information** page, provide the following information:

   **Edition**
   
   Choose the edition that meets your requirements.

   **Directory DNS name**
   
   The fully qualified name for the directory, such as `corp.example.com`.

   **Directory NetBIOS name**
   
   An optional short name for the directory, such as `CORP`.

   **Directory description**
   
   An optional description for the directory.

   **Admin password**
   
   The password for the directory administrator. The directory creation process creates an administrator account with the user name `Admin` and this password.

   The directory administrator password can't include the word "admin." The password is case-sensitive and must be 8–64 characters in length. It must also contain at least one character from three of the following four categories:
   - Lowercase letters (a–z)
   - Uppercase letters (A–Z)
   - Numbers (0–9)
   - Nonalphanumeric characters (~!@#$%^&*_-+=`\|(){}[]:;"'<,.?/)

   **Confirm password**
   
   Retype the administrator password.

   **Important**
   
   Make sure that you save this password. AWS Directory Service doesn't store this password, and it can't be retrieved or reset.

5. Choose **Next**.

6. On the **Choose VPC and subnets** page, provide the following information:

   **VPC**
   
   Choose the VPC for the directory. You can create the PostgreSQL DB cluster in this same VPC or in a different VPC.

   **Subnets**
   
   Choose the subnets for the directory servers. The two subnets must be in different Availability Zones.

7. Choose **Next**.

8. Review the directory information. If changes are needed, choose **Previous** and make the changes. When the information is correct, choose **Create directory**.
It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes to **Active**.

To see information about your directory, choose the directory ID in the directory listing. Make a note of the **Directory ID** value. You need this value when you create or modify your PostgreSQL DB instance.
Step 2: (Optional) create a trust for an on-premises Active Directory

If you don't plan to use your own on-premises Microsoft Active Directory, skip to Step 3: Create an IAM role for Amazon Aurora to access the AWS Directory Service (p. 1130).

To get Kerberos authentication using your on-premises Active Directory, you need to create a trusting domain relationship using a forest trust between your on-premises Microsoft Active Directory and the AWS Managed Microsoft AD directory (created in Step 1: Create a directory using AWS Managed Microsoft AD (p. 1126)). The trust can be one-way, where the AWS Managed Microsoft AD directory trusts the on-premises Microsoft Active Directory. The trust can also be two-way, where both Active Directories trust each other. For more information about setting up trusts using AWS Directory Service, see When to create a trust relationship in the AWS Directory Service Administration Guide.

Note
If you use an on-premises Microsoft Active Directory, DB cluster endpoints can't be used by Windows clients for global databases or custom endpoints. For more information, see Using Amazon Aurora global databases (p. 206) and Using custom endpoints (p. 28).
Make sure that your on-premises Microsoft Active Directory domain name includes a DNS suffix routing that corresponds to the newly created trust relationship. The following screenshot shows an example.

Step 3: Create an IAM role for Amazon Aurora to access the AWS Directory Service

For Amazon Aurora to call AWS Directory Service for you, an IAM role that uses the managed IAM policy AmazonRDSDirectoryServiceAccess is required. This role allows Amazon Aurora to make calls to AWS Directory Service.

When a DB instance is created using the AWS Management Console and the console user has the iam:CreateRole permission, the console creates this role automatically. In this case, the role name is rds-directoryservice-kerberos-access-role. Otherwise, create the IAM role manually. Choose RDS and then RDS - Directory Service. Attach the AWS managed policy AmazonRDSDirectoryServiceAccess to this role.

For more information about creating IAM roles for a service, see Creating a role to delegate permissions to an AWS service in the IAM User Guide.

Note
The IAM role used for Windows Authentication for RDS for Microsoft SQL Server can't be used for Amazon Aurora.

Optionally, you can create policies with the required permissions instead of using the managed IAM policy AmazonRDSDirectoryServiceAccess. In this case, the IAM role must have the following IAM trust policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "rds.amazonaws.com",
        "Resource": "*"
      }
    }]
}
```
The role must also have the following IAM role policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

**Step 4: Create and configure users**

You can create users by using the Active Directory Users and Computers tool, which is one of the Active Directory Domain Services and Active Directory Lightweight Directory Services tools. In this case, *users* are individual people or entities that have access to your directory.

To create users in an AWS Directory Service directory, you must be connected to a Windows-based Amazon EC2 instance. Also, this EC2 instance must be a member of the AWS Directory Service directory. At the same time, you must be logged in as a user that has privileges to create users. For more information, see *Create a user* in the *AWS Directory Service Administration Guide*.

**Step 5: Enable cross-VPC traffic between the directory and the DB instance**

If you plan to locate the directory and the DB cluster in the same VPC, skip this step and move on to **Step 6: Create or modify a PostgreSQL DB cluster** (p. 1132).

If you plan to locate the directory and the DB instance in different VPCs, configure cross-VPC traffic using VPC peering or AWS Transit Gateway.

The following procedure enables traffic between VPCs using VPC peering. Follow the instructions in *What is VPC peering?* in the *Amazon Virtual Private Cloud Peering Guide*.

**To enable cross-VPC traffic using VPC peering**

1. Set up appropriate VPC routing rules to ensure that network traffic can flow both ways.
2. Ensure that the DB instance's security group can receive inbound traffic from the directory's security group.
3. Ensure that there is no network access control list (ACL) rule to block traffic.
If a different AWS account owns the directory, you must share the directory.

**To share the directory between AWS accounts**

1. Start sharing the directory with the AWS account that the DB instance will be created in by following the instructions in Tutorial: Sharing your AWS Managed Microsoft AD directory for seamless EC2 Domain-join in the AWS Directory Service Administration Guide.
2. Sign in to the AWS Directory Service console using the account for the DB instance, and ensure that the domain has the **SHARED** status before proceeding.
3. While signed into the AWS Directory Service console using the account for the DB instance, note the **Directory ID** value. You use this directory ID to join the DB instance to the domain.

**Step 6: Create or modify a PostgreSQL DB cluster**

Create or modify a PostgreSQL DB cluster for use with your directory. You can use the console, CLI, or RDS API to associate a DB cluster with a directory. You can do this in one of the following ways:

- Create a new PostgreSQL DB cluster using the console, the `create-db-cluster` CLI command, or the `CreateDBCluster` RDS API operation. For instructions, see Creating a DB cluster and connecting to a database on an Aurora PostgreSQL DB cluster (p. 87).
- Modify an existing PostgreSQL DB cluster using the console, the `modify-db-cluster` CLI command, or the `ModifyDBCluster` RDS API operation. For instructions, see Modifying an Amazon Aurora DB cluster (p. 327).
- Restore a PostgreSQL DB cluster from a DB snapshot using the console, the `restore-db-cluster-from-db-snapshot` CLI command, or the `RestoreDBClusterFromDBSnapshot` RDS API operation. For instructions, see Restoring from a DB cluster snapshot (p. 420).
- Restore a PostgreSQL DB cluster to a point-in-time using the console, the `restore-db-instance-to-point-in-time` CLI command, or the `RestoreDBClusterToPointInTime` RDS API operation. For instructions, see Restoring a DB cluster to a specified time (p. 454).

Kerberos authentication is only supported for PostgreSQL DB clusters in a VPC. The DB cluster can be in the same VPC as the directory, or in a different VPC. The DB cluster must use a security group that allows egress within the directory's VPC so the DB cluster can communicate with the directory.

When you use the console to create a DB cluster, choose **Password and Kerberos authentication** in the **Database authentication** section. Choose **Browse Directory** and then select the directory, or choose **Create a new directory**.
When you use the console to modify or restore a DB cluster, choose the directory in the **Kerberos authentication** section, or choose **Create a new directory**.

When you use the AWS CLI, the following parameters are required for the DB cluster to be able to use the directory that you created:

- For the `--domain` parameter, use the domain identifier ("d-*" identifier) generated when you created the directory.
- For the `--domain-iam-role-name` parameter, use the role you created that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`.

For example, the following CLI command modifies a DB cluster to use a directory.

```
aws rds modify-db-cluster --db-cluster-identifier mydbinstance --domain d-Directory-ID --domain-iam-role-name role-name
```

**Important**

If you modify a DB cluster to enable Kerberos authentication, reboot the DB cluster after making the change.
Step 7: Create Kerberos authentication PostgreSQL logins

Next, use the RDS master user credentials to connect to the PostgreSQL DB cluster as you do with any other DB cluster. The DB instance is joined to the AWS Managed Microsoft AD domain. Thus, you can provision PostgreSQL logins and users from the Microsoft Active Directory users and groups in your domain. To manage database permissions, you grant and revoke standard PostgreSQL permissions to these logins.

To allow an Active Directory user to authenticate with PostgreSQL, use the RDS master user credentials. You use these credentials to connect to the PostgreSQL DB cluster as you do with any other DB cluster. After you're logged in, create an externally authenticated user in PostgreSQL and grant the rds_ad role to this user.

```
CREATE USER "username@CORP.EXAMPLE.COM" WITH LOGIN;
GRANT rds_ad TO "username@CORP.EXAMPLE.COM";
```

Replace `username` with the user name and include the domain name in uppercase. Users (both humans and applications) from your domain can now connect to the RDS PostgreSQL cluster from a domain-joined client machine using Kerberos authentication.

Step 8: Configure a PostgreSQL client

To configure a PostgreSQL client, take the following steps:

- Create a krb5.conf file (or equivalent) to point to the domain.
- Verify that traffic can flow between the client host and AWS Directory Service. Use a network utility such as Netcat for the following:
  - Verify traffic over DNS for port 53.
  - Verify traffic over TCP/UDP for port 53 and for Kerberos, which includes ports 88 and 464 for AWS Directory Service.
  - Verify that traffic can flow between the client host and the DB instance over the database port. For example, use psql to connect and access the database.

The following is sample krb5.conf content for 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
exemple.com = EXAMPLE.COM
```

The following is sample krb5.conf content for an on-premises Microsoft Active Directory.

```
[libdefaults]
default_realm = EXAMPLE.COM
[realms]
EXAMPLE.COM = {
kdc = example.com
admin_server = example.com
}
ONPREM.COM = {
```
Managing a DB cluster in a Domain

You can use the console, the CLI, or the RDS API to manage your DB cluster and its relationship with your Microsoft Active Directory. For example, you can associate an Active Directory to enable Kerberos authentication. You can also remove the association for an Active Directory to disable Kerberos authentication. You can also move a DB cluster to be externally authenticated by one Microsoft Active Directory to another.

For example, using the CLI, you can do the following:

- To reattempt enabling Kerberos authentication for a failed membership, use the `modify-db-cluster` CLI command. Specify the current membership's directory ID for the `--domain` option.
- To disable Kerberos authentication on a DB instance, use the `modify-db-cluster` CLI command. Specify `none` for the `--domain` option.
- To move a DB instance from one domain to another, use the `modify-db-cluster` CLI command. Specify the domain identifier of the new domain for the `--domain` option.

Understanding Domain membership

After you create or modify your DB cluster, the DB instances become members of the domain. You can view the status of the domain membership in the console or by running the `describe-db-instances` CLI command. The status of the DB instance can be one of the following:

- `kerberos-enabled` – The DB instance has Kerberos authentication enabled.
- `enabling-kerberos` – AWS is in the process of enabling Kerberos authentication on this DB instance.
- `pending-enable-kerberos` – Enabling Kerberos authentication is pending on this DB instance.
- `pending-maintenance-enable-kerberos` – AWS will attempt to enable Kerberos authentication on the DB instance during the next scheduled maintenance window.
- `pending-disable-kerberos` – Disabling Kerberos authentication is pending on this DB instance.
- `pending-maintenance-disable-kerberos` – AWS will attempt to disable Kerberos authentication on the DB instance during the next scheduled maintenance window.
- `enable-kerberos-failed` – A configuration problem prevented AWS from enabling Kerberos authentication on the DB instance. Correct the configuration problem before reissuing the command to modify the DB instance.
- `disabling-kerberos` – AWS is in the process of disabling Kerberos authentication on this DB instance.

A request to enable Kerberos authentication can fail because of a network connectivity issue or an incorrect IAM role. In some cases, the attempt to enable Kerberos authentication might fail when you create or modify a DB cluster. If so, make sure that you are using the correct IAM role, then modify the DB cluster to join the domain.
Connecting to PostgreSQL with Kerberos authentication

You can connect to PostgreSQL with Kerberos authentication with the pgAdmin interface or with a command line interface such as psql. For more information about connecting, see Connecting to an Amazon Aurora PostgreSQL DB cluster (p. 257).

pgAdmin

To use pgAdmin to connect to PostgreSQL with Kerberos authentication, take the following steps:

1. Launch the pgAdmin application on your client computer.
3. In the Create - Server dialog box, enter a name on the General tab to identify the server in pgAdmin.
4. On the Connection tab, enter the following information from your Aurora PostgreSQL database:
   - For Host, enter the endpoint. Use a format such as PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com.
     If you’re using an on-premises Microsoft Active Directory from a Windows client, then you need to connect using a special endpoint. Instead of using the Amazon domain rds.amazonaws.com in the host endpoint, use the domain name of the AWS Managed Active Directory.
     For example, suppose that the domain name for the AWS Managed Active Directory is corp.example.com. Then for Host, use the format PostgreSQL-endpoint.AWS-Region.corp.example.com.
   - For Port, enter the assigned port.
   - For Maintenance database, enter the name of the initial database to which the client will connect.
   - For Username, enter the user name that you entered for Kerberos authentication in Step 7: Create Kerberos authentication PostgreSQL logins (p. 1134).
5. Choose Save.

Psql

To use psql to connect to PostgreSQL with Kerberos authentication, take the following steps:

1. At a command prompt, run the following command.

   ```bash
   kinit username
   ```

   Replace username with the user name. At the prompt, enter the password stored in the Microsoft Active Directory for the user.

2. If the PostgreSQL DB cluster is using a publicly accessible VPC, put a private IP address for your DB cluster endpoint in your /etc/hosts file on the EC2 client. For example, the following commands obtain the private IP address and then put it in the /etc/hosts file.

   ```bash
   % 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
   ```
If you’re using an on-premises Microsoft Active Directory from a Windows client, then you need to connect using a special endpoint. Instead of using the Amazon domain rds.amazonaws.com in the host endpoint, use the domain name of the AWS Managed Active Directory.

For example, suppose that the domain name for your AWS Managed Active Directory is corp.example.com. Then use the format PostgreSQL-endpoint.AWS-Region.corp.example.com for the endpoint and put it in the /etc/hosts file.

```bash
% echo " 34.210.197.118 PostgreSQL-endpoint.AWS-Region.corp.example.com" >> /etc/hosts
```

3. Use the following psql command to log in to a PostgreSQL DB cluster that is integrated with Active Directory. Use a cluster or instance endpoint.

```bash
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com postgres
```

To log in to the PostgreSQL DB cluster from a Windows client using an on-premises Active Directory, use the following psql command with the domain name from the previous step (corp.example.com):

```bash
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-Region.corp.example.com postgres
```

## Amazon Aurora PostgreSQL reference

### Contents

- Amazon Aurora PostgreSQL parameters (p. 1137)
  - Aurora PostgreSQL cluster-level parameters (p. 1138)
  - Aurora PostgreSQL instance-level parameters (p. 1140)
- Amazon Aurora PostgreSQL events (p. 1146)

## Amazon Aurora PostgreSQL parameters

You manage your Amazon Aurora DB cluster in the same way that you manage other Amazon RDS DB instances, by using parameters in a DB parameter group. Amazon Aurora differs from other DB engines in that you have a DB cluster that contains multiple DB instances. As a result, some of the parameters that you use to manage your Amazon Aurora DB cluster apply to the entire cluster, while other parameters apply only to a particular DB instance in the DB cluster.

Cluster-level parameters are managed in DB cluster parameter groups. Instance-level parameters are managed in DB parameter groups. Although each DB instance in an Aurora PostgreSQL DB cluster is compatible with the PostgreSQL database engine, some of the PostgreSQL database engine parameters must be applied at the cluster level, and are managed using DB cluster parameter groups. Cluster-level parameters are not found in the DB parameter group for a DB instance in an Aurora PostgreSQL DB cluster and are listed later in this topic.

You can view both cluster-level and instance-level parameters in the Amazon RDS console, or by using the AWS CLI or Amazon RDS API. For example, to view cluster-level parameters in a DB cluster parameter group, use the `describe-db-cluster-parameters` AWS CLI command. To view instance-level parameters in a DB parameter group for a DB instance in a DB cluster, use the `describe-db-parameters` AWS CLI command.
You can manage both cluster-level and instance-level parameters using the Amazon RDS console, the AWS CLI, or the Amazon RDS API. There are separate commands for managing cluster-level parameters and instance-level parameters. For example:

- To manage cluster-level parameters in a DB cluster parameter group, use the `modify-db-cluster-parameter-group` AWS CLI command.
- To manage instance-level parameters in a DB parameter group for a DB instance in a DB cluster, use the `modify-db-parameter-group` AWS CLI command.

For more information about parameter groups, see Working with DB parameter groups and DB cluster parameter groups (p. 298).

### Aurora PostgreSQL cluster-level parameters

The following table shows all of the parameters that apply to the entire Aurora PostgreSQL DB cluster.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td>ansi_constraint_trigger_ordering</td>
<td>Yes</td>
</tr>
<tr>
<td>ansi_force_foreign_key_checks</td>
<td>Yes</td>
</tr>
<tr>
<td>ansi_qualified_update_set_target</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_ccm_enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>archive_command</td>
<td>No</td>
</tr>
<tr>
<td>archive_timeout</td>
<td>No</td>
</tr>
<tr>
<td>array_nulls</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_analyze_scale_factor</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_analyze_threshold</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_freeze_max_age</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_max_workers</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_multixact_freeze_max_age</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_naptime</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_vacuum_cost_delay</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_vacuum_cost_limit</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_vacuum_scale_factor</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_vacuum_threshold</td>
<td>Yes</td>
</tr>
<tr>
<td>autovacuum_work_mem</td>
<td>Yes</td>
</tr>
<tr>
<td>backslash_quote</td>
<td>Yes</td>
</tr>
<tr>
<td>client_encoding</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>data_directory</td>
<td>No</td>
</tr>
<tr>
<td>datestyle</td>
<td>Yes</td>
</tr>
<tr>
<td>default_tablespace</td>
<td>Yes</td>
</tr>
<tr>
<td>default_with_oids</td>
<td>Yes</td>
</tr>
<tr>
<td>extra_float_digits</td>
<td>Yes</td>
</tr>
<tr>
<td>huge_pages</td>
<td>No</td>
</tr>
<tr>
<td>intervalstyle</td>
<td>Yes</td>
</tr>
<tr>
<td>lc_monetary</td>
<td>Yes</td>
</tr>
<tr>
<td>lc_numeric</td>
<td>Yes</td>
</tr>
<tr>
<td>lc_time</td>
<td>Yes</td>
</tr>
<tr>
<td>log_autovacuum_min_duration</td>
<td>Yes</td>
</tr>
<tr>
<td>max_prepared_transactions</td>
<td>Yes</td>
</tr>
<tr>
<td>password_encryption</td>
<td>No</td>
</tr>
<tr>
<td>max_standby_streaming_delay</td>
<td>Yes for PostgreSQL 11, No for earlier PostgreSQL versions</td>
</tr>
<tr>
<td>port</td>
<td>No</td>
</tr>
<tr>
<td>rds.enable_plan_management</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.extensions</td>
<td>No</td>
</tr>
<tr>
<td>rds.force_autovacuum_logging_level</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.force_ssl</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.global_db_rpo</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.logical_replication</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.restrict_password_commands</td>
<td>Yes</td>
</tr>
<tr>
<td>server_encoding</td>
<td>No</td>
</tr>
<tr>
<td>ssl</td>
<td>Yes</td>
</tr>
<tr>
<td>ssl_max_protocol_version</td>
<td>Yes</td>
</tr>
<tr>
<td>ssl_min_protocol_version</td>
<td>Yes</td>
</tr>
<tr>
<td>synchronous_commit</td>
<td>Yes</td>
</tr>
<tr>
<td>timezone</td>
<td>Yes</td>
</tr>
<tr>
<td>track_commit_timestamp</td>
<td>Yes</td>
</tr>
<tr>
<td>vacuum_cost_delay</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Aurora PostgreSQL parameters

The following table shows all of the parameters that apply to a specific DB instance in an Aurora PostgreSQL DB cluster.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td>vacuum_cost_limit</td>
<td>Yes</td>
</tr>
<tr>
<td>vacuum_cost_page_hit</td>
<td>Yes</td>
</tr>
<tr>
<td>vacuum_cost_page_miss</td>
<td>Yes</td>
</tr>
<tr>
<td>vacuum_defer_cleanup_age</td>
<td>Yes</td>
</tr>
<tr>
<td>vacuum_freeze_min_age</td>
<td>Yes</td>
</tr>
<tr>
<td>vacuum_freeze_table_age</td>
<td>Yes</td>
</tr>
<tr>
<td>vacuum_multixact_freeze_min_age</td>
<td>Yes</td>
</tr>
<tr>
<td>vacuum_multixact_freeze_table_age</td>
<td>Yes</td>
</tr>
<tr>
<td>wal_buffers</td>
<td>Yes</td>
</tr>
<tr>
<td>wal_sender_timeout</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Aurora PostgreSQL instance-level parameters

The following table shows all of the parameters that apply to a specific DB instance in an Aurora PostgreSQL DB cluster.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td>apg_enable_not_in_transform</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_enable_remove_redundant_inner_joins</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_enable_semijoin_push_down</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.capture_plan_baselines</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.max_databases</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.max_plans</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.pgss_min_calls (deprecated)</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.pgss_min_mean_time_ms (deprecated)</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.pgss_min_stddev_time_ms (deprecated)</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.pgss_min_total_time_ms (deprecated)</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.plan_retention_period</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.unapproved_plan_execution_threshold</td>
<td>Yes</td>
</tr>
<tr>
<td>apg_plan_mgmt.use_plan_baselines</td>
<td>Yes</td>
</tr>
<tr>
<td>application_name</td>
<td>Yes</td>
</tr>
<tr>
<td>authentication_timeout</td>
<td>Yes</td>
</tr>
<tr>
<td>auto_explain.log_analyze</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>auto_explain.log_buffers</td>
<td>Yes</td>
</tr>
<tr>
<td>auto_explain.log_format</td>
<td>Yes</td>
</tr>
<tr>
<td>auto_explain.log_min_duration</td>
<td>Yes</td>
</tr>
<tr>
<td>auto_explain.log_nested_statements</td>
<td>Yes</td>
</tr>
<tr>
<td>auto_explain.log_timing</td>
<td>Yes</td>
</tr>
<tr>
<td>auto_explain.log_triggers</td>
<td>Yes</td>
</tr>
<tr>
<td>auto_explain.logVerbose</td>
<td>Yes</td>
</tr>
<tr>
<td>auto_explain.sample_rate</td>
<td>Yes</td>
</tr>
<tr>
<td>backend_flush_after</td>
<td>Yes</td>
</tr>
<tr>
<td>bgwriter_flush_after</td>
<td>Yes</td>
</tr>
<tr>
<td>bytea_output</td>
<td>Yes</td>
</tr>
<tr>
<td>check_function_bodies</td>
<td>Yes</td>
</tr>
<tr>
<td>checkpoint_flush_after</td>
<td>Yes</td>
</tr>
<tr>
<td>checkpoint_timeout</td>
<td>No</td>
</tr>
<tr>
<td>client_min_messages</td>
<td>Yes</td>
</tr>
<tr>
<td>config_file</td>
<td>No</td>
</tr>
<tr>
<td>constraint_exclusion</td>
<td>Yes</td>
</tr>
<tr>
<td>cpu_index_tuple_cost</td>
<td>Yes</td>
</tr>
<tr>
<td>cpu_operator_cost</td>
<td>Yes</td>
</tr>
<tr>
<td>cpu_tuple_cost</td>
<td>Yes</td>
</tr>
<tr>
<td>cursor_tuple_fraction</td>
<td>Yes</td>
</tr>
<tr>
<td>db_user_namespace</td>
<td>No</td>
</tr>
<tr>
<td>deadlock_timeout</td>
<td>Yes</td>
</tr>
<tr>
<td>debug.pretty_print</td>
<td>Yes</td>
</tr>
<tr>
<td>debug.print_parse</td>
<td>Yes</td>
</tr>
<tr>
<td>debug.print_plan</td>
<td>Yes</td>
</tr>
<tr>
<td>debug.print_rewritten</td>
<td>Yes</td>
</tr>
<tr>
<td>default_statistics_target</td>
<td>Yes</td>
</tr>
<tr>
<td>default_transaction_deferrable</td>
<td>Yes</td>
</tr>
<tr>
<td>default_transaction_isolation</td>
<td>Yes</td>
</tr>
<tr>
<td>default_transaction_read_only</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>effective_cache_size</td>
<td>Yes</td>
</tr>
<tr>
<td>effective_io_concurrency</td>
<td>No</td>
</tr>
<tr>
<td>enable_bitmapscan</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_hashagg</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_hashjoin</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_indexonlyscan</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_indexscan</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_material</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_mergejoin</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_nestloop</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_seqscan</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_sort</td>
<td>Yes</td>
</tr>
<tr>
<td>enable_tidscan</td>
<td>Yes</td>
</tr>
<tr>
<td>escape_string_warning</td>
<td>Yes</td>
</tr>
<tr>
<td>exit_on_error</td>
<td>No</td>
</tr>
<tr>
<td>force_parallel_mode</td>
<td>Yes</td>
</tr>
<tr>
<td>fromCollapse_limit</td>
<td>Yes</td>
</tr>
<tr>
<td>geqo</td>
<td>Yes</td>
</tr>
<tr>
<td>geqo_effort</td>
<td>Yes</td>
</tr>
<tr>
<td>geqo_generations</td>
<td>Yes</td>
</tr>
<tr>
<td>geqo_pool_size</td>
<td>Yes</td>
</tr>
<tr>
<td>geqo_seed</td>
<td>Yes</td>
</tr>
<tr>
<td>geqo_selection_bias</td>
<td>Yes</td>
</tr>
<tr>
<td>geqo_threshold</td>
<td>Yes</td>
</tr>
<tr>
<td>gin_fuzzy_search_limit</td>
<td>Yes</td>
</tr>
<tr>
<td>gin_pending_list_limit</td>
<td>Yes</td>
</tr>
<tr>
<td>hba_file</td>
<td>No</td>
</tr>
<tr>
<td>hot_standby_feedback</td>
<td>No</td>
</tr>
<tr>
<td>ident_file</td>
<td>No</td>
</tr>
<tr>
<td>idle_in_transaction_session_timeout</td>
<td>Yes</td>
</tr>
<tr>
<td>joinCollapse_limit</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Aurora PostgreSQL parameters

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Modifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td>lc_messages</td>
<td>Yes</td>
</tr>
<tr>
<td>listen_addresses</td>
<td>No</td>
</tr>
<tr>
<td>lo_compat_privileges</td>
<td>No</td>
</tr>
<tr>
<td>log_connections</td>
<td>Yes</td>
</tr>
<tr>
<td>log_destination</td>
<td>Yes</td>
</tr>
<tr>
<td>log_directory</td>
<td>No</td>
</tr>
<tr>
<td>log_disconnections</td>
<td>Yes</td>
</tr>
<tr>
<td>log_duration</td>
<td>Yes</td>
</tr>
<tr>
<td>log_error_verbosity</td>
<td>Yes</td>
</tr>
<tr>
<td>log_executor_stats</td>
<td>Yes</td>
</tr>
<tr>
<td>log_file_mode</td>
<td>No</td>
</tr>
<tr>
<td>log_filename</td>
<td>Yes</td>
</tr>
<tr>
<td>log_hostname</td>
<td>Yes</td>
</tr>
<tr>
<td>log_line_prefix</td>
<td>No</td>
</tr>
<tr>
<td>log_lock_waits</td>
<td>Yes</td>
</tr>
<tr>
<td>log_min_duration_statement</td>
<td>Yes</td>
</tr>
<tr>
<td>log_min_error_statement</td>
<td>Yes</td>
</tr>
<tr>
<td>log_min_messages</td>
<td>Yes</td>
</tr>
<tr>
<td>log_parser_stats</td>
<td>Yes</td>
</tr>
<tr>
<td>log_planner_stats</td>
<td>Yes</td>
</tr>
<tr>
<td>log_replication_commands</td>
<td>Yes</td>
</tr>
<tr>
<td>log_rotation_age</td>
<td>Yes</td>
</tr>
<tr>
<td>log_rotation_size</td>
<td>Yes</td>
</tr>
<tr>
<td>log_statement</td>
<td>Yes</td>
</tr>
<tr>
<td>log_statement_stats</td>
<td>Yes</td>
</tr>
<tr>
<td>log_temp_files</td>
<td>Yes</td>
</tr>
<tr>
<td>log_timezone</td>
<td>No</td>
</tr>
<tr>
<td>log_truncate_on_rotation</td>
<td>No</td>
</tr>
<tr>
<td>logging_collector</td>
<td>No</td>
</tr>
<tr>
<td>maintenance_work_mem</td>
<td>Yes</td>
</tr>
<tr>
<td>max_connections</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>max_files_per_process</td>
<td>Yes</td>
</tr>
<tr>
<td>max_locks_per_transaction</td>
<td>Yes</td>
</tr>
<tr>
<td>max_replication_slots</td>
<td>Yes</td>
</tr>
<tr>
<td>max_stack_depth</td>
<td>Yes</td>
</tr>
<tr>
<td>max_standby_archive_delay</td>
<td>No</td>
</tr>
<tr>
<td>max_standby_streaming_delay</td>
<td>Yes for PostgreSQL 11, No for earlier PostgreSQL versions</td>
</tr>
<tr>
<td>max_wal_senders</td>
<td>Yes</td>
</tr>
<tr>
<td>max_worker_processes</td>
<td>Yes</td>
</tr>
<tr>
<td>min_parallel_relation_size</td>
<td>Yes</td>
</tr>
<tr>
<td>old_snapshot_threshold</td>
<td>Yes</td>
</tr>
<tr>
<td>operator_precedence_warning</td>
<td>Yes</td>
</tr>
<tr>
<td>parallel_setup_cost</td>
<td>Yes</td>
</tr>
<tr>
<td>parallel_tuple_cost</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_hint_plan.debug_print</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_hint_plan.enable_hint</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_hint_plan.enable_hint_table</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_hint_plan.message_level</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_hint_plan.parse_messages</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_stat_statements.max</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_stat_statements.save</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_stat_statements.track</td>
<td>Yes</td>
</tr>
<tr>
<td>pg_stat_statements.track_utility</td>
<td>Yes</td>
</tr>
<tr>
<td>pgaudit.log</td>
<td>Yes</td>
</tr>
<tr>
<td>pgaudit.log_catalog</td>
<td>Yes</td>
</tr>
<tr>
<td>pgaudit.log_level</td>
<td>Yes</td>
</tr>
<tr>
<td>pgaudit.log_parameter</td>
<td>Yes</td>
</tr>
<tr>
<td>pgaudit.log_relation</td>
<td>Yes</td>
</tr>
<tr>
<td>pgaudit.log_statement_once</td>
<td>Yes</td>
</tr>
<tr>
<td>pgaudit.role</td>
<td>Yes</td>
</tr>
<tr>
<td>postgis.gdal_enabled_drivers</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>quote_all_identifiers</td>
<td>Yes</td>
</tr>
<tr>
<td>random_page_cost</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.force_admin_logging_level</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.log_retention_period</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.rds_superuser_reserved_connections</td>
<td>Yes</td>
</tr>
<tr>
<td>rds.superuser_variables</td>
<td>No</td>
</tr>
<tr>
<td>replacement_sort_tuples</td>
<td>Yes</td>
</tr>
<tr>
<td>restart_after_crash</td>
<td>No</td>
</tr>
<tr>
<td>row_security</td>
<td>Yes</td>
</tr>
<tr>
<td>search_path</td>
<td>Yes</td>
</tr>
<tr>
<td>seq_page_cost</td>
<td>Yes</td>
</tr>
<tr>
<td>session_replication_role</td>
<td>Yes</td>
</tr>
<tr>
<td>shared_buffers</td>
<td>Yes</td>
</tr>
<tr>
<td>shared_preload_libraries</td>
<td>Yes</td>
</tr>
<tr>
<td>sql_inheritance</td>
<td>Yes</td>
</tr>
<tr>
<td>ssl_ca_file</td>
<td>No</td>
</tr>
<tr>
<td>ssl_cert_file</td>
<td>No</td>
</tr>
<tr>
<td>ssl_ciphers</td>
<td>No</td>
</tr>
<tr>
<td>ssl_key_file</td>
<td>No</td>
</tr>
<tr>
<td>standard_conforming_strings</td>
<td>Yes</td>
</tr>
<tr>
<td>statement_timeout</td>
<td>Yes</td>
</tr>
<tr>
<td>stats_temp_directory</td>
<td>No</td>
</tr>
<tr>
<td>superuser_reserved_connections</td>
<td>No</td>
</tr>
<tr>
<td>synchronize_seqscans</td>
<td>Yes</td>
</tr>
<tr>
<td>syslog_facility</td>
<td>No</td>
</tr>
<tr>
<td>tcp_keepalives_count</td>
<td>Yes</td>
</tr>
<tr>
<td>tcp_keepalives_idle</td>
<td>Yes</td>
</tr>
<tr>
<td>tcp_keepalives_interval</td>
<td>Yes</td>
</tr>
<tr>
<td>temp_buffers</td>
<td>Yes</td>
</tr>
<tr>
<td>temp_tablespaces</td>
<td>Yes</td>
</tr>
<tr>
<td>track_activities</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Modifiable</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>track_activity_query_size</td>
<td>Yes</td>
</tr>
<tr>
<td>track_counts</td>
<td>Yes</td>
</tr>
<tr>
<td>track_functions</td>
<td>Yes</td>
</tr>
<tr>
<td>track_io_timing</td>
<td>Yes</td>
</tr>
<tr>
<td>transaction_deferrable</td>
<td>Yes</td>
</tr>
<tr>
<td>transaction_read_only</td>
<td>Yes</td>
</tr>
<tr>
<td>transform_null_equals</td>
<td>Yes</td>
</tr>
<tr>
<td>unix_socket_directories</td>
<td>No</td>
</tr>
<tr>
<td>unix_socket_group</td>
<td>No</td>
</tr>
<tr>
<td>unix_socket_permissions</td>
<td>No</td>
</tr>
<tr>
<td>update_process_title</td>
<td>Yes</td>
</tr>
<tr>
<td>wal_receiver_status_interval</td>
<td>Yes</td>
</tr>
<tr>
<td>wal_receiver_timeout</td>
<td>Yes</td>
</tr>
<tr>
<td>work_mem</td>
<td>Yes</td>
</tr>
<tr>
<td>xmlbinary</td>
<td>Yes</td>
</tr>
<tr>
<td>xmloption</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Amazon Aurora PostgreSQL events

The following are some common wait events for Aurora PostgreSQL.

**BufferPin:BufferPin**

In this wait event, a session is waiting to access a data buffer during a period when no other session can examine that buffer. Buffer pin waits can be protracted if another process holds an open cursor which last read data from the buffer in question.

**Client:ClientRead**

In this wait event, a session is receiving data from an application client. This wait might be prevalent during bulk data loads using the COPY statement, or for applications that pass data to Aurora using many round trips between the client and the database. A high number of client read waits per transaction may indicate excessive round trips, such as parameter passing. You should compare this against the expected number of statements per transaction.

**IO:DataFilePrefetch**

In this wait event, a session is waiting for an asynchronous prefetch from Aurora Storage.

**IO:DataFileRead**

In this wait event, a session is reading data from Aurora Storage. This may be a typical wait event for I/O intensive workloads. SQL statements showing a comparatively large proportion of this wait event compared to other SQL statements may be using an inefficient query plan that requires reading large amounts of data.
IO:XactSync

In this wait event, a session is issuing a COMMIT or ROLLBACK, requiring the current transaction's changes to be persisted. Aurora is waiting for Aurora storage to acknowledge persistence.

This wait most often arises when there is a very high rate of commit activity on the system. You can sometimes alleviate this wait by modifying applications to commit transactions in batches. You might see this wait at the same time as CPU waits in a case where the DB load exceeds the number of virtual CPUs (vCPUs) for the DB instance. In this case, the storage persistence might be competing for CPU with CPU-intensive database workloads. To alleviate this scenario, you can try reducing those workloads, or scaling up to a DB instance with more vCPUs.

Lock:transactionid

In this wait event, a session is trying to modify data that has been modified by another session, and is waiting for the other session's transaction to be committed or rolled back. You can investigate blocking and waiting sessions in the pg_locks view.

LWLock:buffer_content

In this wait event, a session is waiting to read or write a data page in memory while another session has that page locked for writing. Heavy write contention for a single page (hot page), due to frequent updates of the same piece of data by many sessions, could lead to prevalence of this wait event. Excessive use of foreign key constraints could increase lock duration, leading to increased contention. You should investigate workloads experiencing high buffer_content waits for usage of foreign key constraints to determine if the constraints are necessary. Alternatively, decreasing the fillfactor on the parent table will spread the keys across more of the block and can reduce contention on the page.

LWLock:SubtransControlLock

In this wait event, a session is looking up or manipulating the parent/child relationship between a transaction and a subtransaction. The two most common causes of subtransaction use are savepoints and PL/pgSQL exception blocks. The wait event might occur if there is heavy concurrent querying of data that's simultaneously being updated from within subtransactions. You should investigate whether it is possible to reduce the use of savepoints and exception blocks, or to decrease concurrent queries on the rows being updated.

For a complete list of PostgreSQL wait events, see PostgreSQL wait-event table.

Database engine updates for Amazon Aurora PostgreSQL

In the following topic, you can find version and update information specific to Amazon Aurora with PostgreSQL compatibility. For more information about updates that apply generally to Aurora, see Amazon Aurora updates (p. 413).

Note
For how to upgrade the Amazon Aurora PostgreSQL engine version, see Upgrading the PostgreSQL DB engine for Aurora PostgreSQL (p. 1109).

Topics
- Identifying your version of Amazon Aurora PostgreSQL (p. 1148)
- Engine versions for Amazon Aurora PostgreSQL (p. 1148)
Identifying your version of Amazon Aurora PostgreSQL

Amazon Aurora includes certain features that are general to Aurora and available to all Aurora DB clusters. Aurora includes other features that are specific to a particular database engine that Aurora supports. These features are available only to those Aurora DB clusters that use that database engine, such as Aurora PostgreSQL.

An Aurora database has two version numbers, the Aurora version number and the database engine version number:

Aurora version number

For how to get the Aurora version number, see Identifying your Amazon Aurora version (p. 413).

PostgreSQL engine version number

To get the database engine version number for an Aurora PostgreSQL DB instance, query for the `SERVER_VERSION` runtime parameter as shown following.

```
SHOW SERVER_VERSION;
```

To see which Aurora version number maps to which PostgreSQL engine version number, see Engine versions for Amazon Aurora PostgreSQL (p. 1148).

Engine versions for Amazon Aurora PostgreSQL

Following, you can find information about supported versions of the Aurora with PostgreSQL compatibility database engine. An Aurora database has two version numbers; the Aurora version number and the database engine version number. To determine the version numbers of your Aurora PostgreSQL database, see Identifying your version of Amazon Aurora PostgreSQL (p. 1148).

To determine which PostgreSQL engine versions are available in an AWS Region, use the `describe-db-engine-versions` AWS CLI command. For example:

```
aws rds describe-db-engine-versions --engine aurora-postgresql --query '[].[EngineVersion]' --output text --region your-AWS-Region
```

For a list of AWS Regions, see Aurora PostgreSQL Region availability (p. 8).

Topics

- Version 3.4, compatible with PostgreSQL 11.9 (p. 1149)
- Version 3.3, compatible with PostgreSQL 11.8 (p. 1150)
- Version 3.2, compatible with PostgreSQL 11.7 (p. 1152)
- Version 3.1, compatible with PostgreSQL 11.6 (p. 1155)
- Version 3.0, compatible with PostgreSQL 11.4 (p. 1159)
- Version 2.7, compatible with PostgreSQL 10.14 (p. 1160)
- Version 2.6, compatible with PostgreSQL 10.13 (p. 1161)
- Version 2.5, compatible with PostgreSQL 10.12 (p. 1163)
Version 2.4, compatible with PostgreSQL 10.11 (p. 1166)
Version 2.3, compatible with PostgreSQL 10.7 (p. 1170)
Version 2.2, compatible with PostgreSQL 10.6 (p. 1171)
Version 2.1, compatible with PostgreSQL 10.5 (p. 1172)
Version 2.0, compatible with PostgreSQL 10.4 (p. 1174)
Version 1.9, compatible with PostgreSQL 9.6.19 (p. 1175)
Version 1.8, compatible with PostgreSQL 9.6.18 (p. 1175)
Version 1.7, compatible with PostgreSQL 9.6.17 (p. 1176)
Version 1.6, compatible with PostgreSQL 9.6.16 (p. 1178)
Version 1.5, compatible with PostgreSQL 9.6.12 (p. 1181)
Version 1.4, compatible with PostgreSQL 9.6.11 (p. 1182)
Version 1.3, compatible with PostgreSQL 9.6.9 (p. 1183)
Version 1.2, compatible with PostgreSQL 9.6.8 (p. 1184)
Version 1.1, compatible with PostgreSQL 9.6.6 is deprecated (p. 1186)
Version 1.0, compatible with PostgreSQL 9.6.3 is deprecated (p. 1187)

For information on extensions and modules, see Extensions and modules for Amazon Aurora PostgreSQL (p. 1188).

The following Aurora PostgreSQL versions are supported.

**Version 3.4, compatible with PostgreSQL 11.9**

This version of Aurora PostgreSQL is compatible with PostgreSQL 11.9. For more information about the improvements in release 11.9, see PostgreSQL release 11.9.

**Version 3.4.0**

**New features**

1. Aurora PostgreSQL now supports invocation of AWS Lambda functions. This includes the new `aws_lambda` extension. For more information, see Invoking an AWS Lambda function from an Aurora PostgreSQL DB cluster (p. 1101).
2. The `db.r6g` instance classes are now available in preview for Aurora. For more information, see DB instance classes (p. 46).

**Critical stability enhancements**

- None

**High priority stability enhancements**

2. Fixed a bug in Aurora PostgreSQL replication that might result in the following error message: ERROR: MultiXactId nnnn has not been created yet -- apparent wraparound
3. Fixed a bug where in some cases, clusters with logical replication enabled might not remove truncated WAL segment files from storage. This could result in volume size growth.
4. Fixed a bug that caused excessive CPU consumption in the `pg_stat_statements` extension.
**Additional improvements and enhancements**

1. You can now use `ps_replication_slot_advance` to advance a logical replication slot for the roles `rds_replication` and `rds_superuser`.
2. Improved the asynchronous mode performance of database activity streams.
3. Reduced the delay of the `rpo_lag_in_msec` metric when publishing to CloudWatch in Aurora global database clusters.
4. Aurora PostgreSQL now avoids falling behind on a read node that occurred when the backend blocked writing to the database client.
5. Fixed a bug that in rare cases caused a brief period of unavailability on a read replica when the storage volume grew.
6. Fixed a bug when creating a database that could return the following: `ERROR: could not create directory on local disk`.
7. Updated data grid files to fix errors or incorrect transformation results from the `ST_Transform` method of the PostGIS extension.
8. Fixed a bug where in some cases replaying `XLOG_BTREE_REUSE_PAGE` records on Aurora reader instances caused unnecessary replay lag.
9. Fixed a small memory leak in the b-tree index that could lead to an out of memory condition.
10. Fixed a bug in the `GiST` index that could result in an out of memory condition after promoting an Aurora read replica.
11. Fixed an S3 export bug that reported the error `ERROR: HTTP 403. Permission denied when importing data from a file inside an S3 subfolder`.
12. Fixed a bug in the `aws_s3` extension for pre-signed URL handling that might result in the error message `S3 bucket names with a period (.) are not supported`.
13. Fixed a bug in the `aws_s3` extension where an import might be blocked indefinitely if an exclusive lock was taken on the relation prior to beginning the operation.
14. Fixed a bug related to replication when Aurora PostgreSQL is acting as a physical replica of an RDS PostgreSQL instance that uses `GiST` indexes. In rare cases, this bug caused a brief period of unavailability after promoting the Aurora cluster.
15. Fixed a bug in database activity streams where customers were not notified of the end of an outage.
16. Updated the `pg_audit` extension to version 1.3.1.

**Version 3.3, compatible with PostgreSQL 11.8**

This version of Aurora PostgreSQL is compatible with PostgreSQL 11.8. For more information about the improvements in release 11.8, see [PostgreSQL release 11.8](https://www.postgresql.org/docs/11/release-11.8.html).

**Patch versions**

- Version 3.3.1 (p. 1150)
- Version 3.3.0 (p. 1151)

**Version 3.3.1**

You can find the following improvements in this engine update.

**Critical stability enhancements**

1. Fixed a bug which materializes when the `NOT EXISTS` operator incorrectly returns TRUE which can only happen under the following unusual set of circumstances:
• A query is using the **NOT EXISTS** operator.
• The column or columns being evaluated against the outer query in the **NOT EXISTS** subquery contain a NULL value.
• There is not a another predicate in the subquery that removes the need for the evaluation of the NULL values.
• The filter used in the subquery does not use an index seek for its execution.
• The operator is not converted to a join by the query optimizer.

**Version 3.3.0**

**New features**

1. Added support for the RDKit extension version 3.8.

   The RDKit extension provides modeling functions for cheminformatics. Cheminformatics is storing, indexing, searching, retrieving, and applying information about chemical compounds. For example, with the RDKit extension you can construct models of molecules, search for molecular structures, and read or create molecules in various notations. You can also perform research on data loaded from the ChEMBL website or a SMILES file. The Simplified Molecular Input Line Entry System (SMILES) is a typographical notation for representing molecules and reactions. For more information, see The RDKit database cartridge in the RDKit documentation.

2. Added support for a minimum TLS version

   Support for a minimum Transport Layer Security (TLS) version is back ported from PostgreSQL 12. It allows the Aurora PostgreSQL server to constrain the TLS protocols with which a client is allowed to connect via two new PostgreSQL parameters. These parameters include `ssl_min_protocol_version` and `ssl_max_protocol_version`. For example, to limit client connections to the Aurora PostgreSQL server to at least TLS 1.2 protocol version, set the `ssl_min_protocol_version` to `TLSv1.2`.

3. Added support for the **pglogical** extension version 2.2.2.

   The **pglogical** extension is a logical streaming replication system that provides additional features beyond what’s available in PostgreSQL native logical replication. Features include conflict handling, row filtering, DDL/sequence replication and delayed apply. You can use the **pglogical** extension to set up replication between Aurora PostgreSQL clusters, between RDS PostgreSQL and Aurora PostgreSQL, and with PostgreSQL databases running outside of RDS.

4. Aurora dynamically resizes your cluster storage space. With dynamic resizing, the storage space for your Aurora DB cluster automatically decreases when you remove data from the DB cluster. For more information, see Storage scaling (p. 349).

   **Note**
   The dynamic resizing feature is being deployed in phases to the AWS Regions where Aurora is available. Depending on the Region where your cluster is, this feature might not be available yet. For more information, see the What’s New announcement.

**Critical stability enhancements**

1. Fixed a bug related to heap page extend that in rare cases resulted in longer recovery time and impacted availability.

**High priority stability enhancements**

1. Fixed a bug in Aurora Global Database that could cause delays in upgrading the database engine in a secondary AWS Region. For more information, see Using Amazon Aurora global databases (p. 206).
2. Fixed a bug that in rare cases caused delays in upgrading a database to engine version 11.8.
Additional improvements and enhancements

1. Fixed a bug where the Aurora replica crashed when workloads with heavy subtransactions are made on the writer instance.
2. Fixed a bug where the writer instance crashed due to a memory leak and the depletion of memory used to track active transactions.
3. Fixed a bug that lead to a crash due to improper initialization when there is no free memory available during PostgreSQL backend startup.
4. Fixed a bug where an Aurora PostgreSQL Serverless DB cluster might return the following error after a scaling event: ERROR: prepared statement "S_6" already exists.
5. Fixed an out-of-memory problem when issuing the `CREATE EXTENSION` command with PostGIS when Database Activity Streams enabled.
6. Fixed a bug where a `SELECT` query might incorrectly return the error Attempting to read past EOF of relation rrrr. blockno=bbb nblocks=nnn.
7. Fixed a bug where the database might be unavailable briefly due to error handling in database storage growth.
8. Fixed a bug in Aurora PostgreSQL Serverless where queries that executed on previously idle connections got delayed until the scale operation completed.
9. Fixed a bug where an Aurora PostgreSQL DB cluster with Database Activity Streams enabled might report the beginning of a potential loss window for activity records, but does not report the restoration of connectivity.

Version 3.2, compatible with PostgreSQL 11.7

This version of Aurora PostgreSQL is compatible with PostgreSQL 11.7. For more information about the improvements in release 11.7, see PostgreSQL release 11.7.

Patch versions
- Version 3.2.6 (p. 1152)
- Version 3.2.4 (p. 1153)
- Version 3.2.3 (p. 1153)
- Version 3.2.2 (p. 1154)
- Version 3.2.1 (p. 1154)

Version 3.2.6

You can find the following improvements in this engine update.

Critical stability enhancements
- None

High priority stability enhancements
1. Fixed a bug in Aurora PostgreSQL replication that might result in the error message, ERROR: MultiXactId nnnn has not been created yet -- apparent wraparound.

Additional improvements and enhancements
1. Fixed a bug that in rare cases caused brief read replica unavailability when storage volume grew.
2. Aurora PostgreSQL Serverless now supports execution of queries on all connections during a scale event.
3. Fixed a bug in Aurora PostgreSQL Serverless where a leaked lock resulted in a prolonged scale event.
4. Fixed a bug where the `aurora_replica_status` function showed truncated server identifiers.
5. Fixed a bug in Aurora PostgreSQL Serverless where connections being migrated during a scale event would disconnect with the message: "ERROR: could not open relation with OID ....
6. Fixed a small memory leak in a b-tree index that could lead to an out of memory condition.
7. Fixed a bug in a GiST index that might result in an out of memory condition after promoting an Aurora Read Replica.
8. Improved performance for Database Activity Streams.
9. Fixed a bug in Database Activity Streams where customers were not notified when an outage ended.
10. Fixed a bug in the `aws_s3` extension for pre-signed URL handling that might have resulted in the error message S3 bucket names with a period (.) are not supported.
11. Fixed a bug in the `aws_s3` extension where incorrect error handling could lead to failures during the import process.
12. Fixed a bug in the `aws_s3` extension where an import may be blocked indefinitely if an exclusive lock was taken on the relation prior to beginning the operation.

Version 3.2.4

You can find the following improvements in this engine update.

**Critical stability enhancements**

1. Fixed a bug which materializes when the NOT EXISTS operator incorrectly returns TRUE which can only happen under the following unusual set of circumstances:
   - A query is using the NOT EXISTS operator.
   - The column or columns being evaluated against the outer query in the NOT EXISTS subquery contain a NULL value.
   - There is not a another predicate in the subquery that removes the need for the evaluation of the NULL values.
   - The filter used in the subquery does not use an index seek for its execution.
   - The operator is not converted to a join by the query optimizer.

Version 3.2.3

You can find the following improvements in this engine update.

**Critical stability enhancements**

- None

**High priority stability enhancements**

- None

**Additional improvements and enhancements**

1. Fixed a bug in Aurora PostgreSQL Serverless where queries that ran on previously idle connections got delayed until the scale operation completed.
2. Fixed a bug that might cause brief unavailability for heavy subtransaction workloads when multiple reader instances restart or rejoin the cluster.

**Version 3.2.2**

You can find the following improvements in this engine update.

**Critical stability enhancements**

1. Fixed a bug related to heap page extend that in rare cases resulted in longer recovery time and impacted availability.

**High priority stability enhancements**

1. Fixed a bug in Aurora Global Database that could cause delays in upgrading the database engine in a secondary region. For more information, see Using Amazon Aurora global databases (p. 206).
2. Fixed a bug that in rare cases caused delays in upgrading a database to engine version 11.7.

**Additional improvements and enhancements**

1. Fixed a bug where the database might be unavailable briefly due to error handling in database storage growth.
2. Fixed a bug where a SELECT query might incorrectly return the error, Attempting to read past EOF of relation rrr. blockno=bbb nblocks=nnn.
3. Fixed a bug where an Aurora PostgreSQL Serverless DB cluster might return the following error after a scaling event: ERROR: prepared statement "S_6" already exists.

**Version 3.2.1**

**New features**

1. Added support for Amazon Aurora PostgreSQL Global Database. For more information, see Using Amazon Aurora global databases (p. 206).
2. Added the ability to configure the recovery point objective (RPO) of a global database for Aurora PostgreSQL. For more information, see Managing recovery for Aurora global databases (p. 245).

You can find the following improvements in this engine update.

**Critical stability enhancements**

None.

**High priority stability enhancements**

1. Improved performance and availability of read instances when applying DROP TABLE and TRUNCATE TABLE operations.
2. Fixed a small but continuous memory leak in a diagnostic module that could lead to an out-of-memory condition on smaller DB instance types.
3. Fixed a bug in the PostGIS extension which could lead to a database restart. This has been reported to the PostGIS community as https://trac.osgeo.org/postgis/ticket/4646.
4. Fixed a bug where read requests might stop responding due to incorrect error handling in the storage engine.
5. Fixed a bug that fails for some queries and results in the message `ERROR: found xmin xxxxxx from before relfrozenxid yyyyyyy`. This could occur following the promotion of a read instance to a write instance.

6. Fixed a bug where an Aurora serverless DB cluster might crash while rolling back a scale attempt.

**Additional improvements and enhancements**

1. Improved performance for queries that read many rows from storage.
2. Improved performance and availability of reader DB instances during heavy read workload.
3. Enabled correlated IN and NOT IN subqueries to be transformed to joins when possible.
4. Improved the filtering estimation for enhanced semi-join filter pushdown by using multi-column statistics or indexes when available.
5. Improved read performance of the `pg_prewarm` extension.
6. Fixed a bug where an Aurora serverless DB cluster might report the message `ERROR: incorrect binary data format in bind parameter ... following a scale event`.
7. Fixed a bug where a serverless DB cluster might report the message `ERROR: insufficient data left in message following a scale event`.
8. Fixed a bug where an Aurora serverless DB cluster can experience prolonged or failed scale attempts.
9. Fixed a bug that resulted in the message `ERROR: could not create file "base/xxxxxx/yyyyyy" as a previous version still exists on disk: Success. Please contact AWS customer support`. This can occur during object creation after PostgreSQL's 32-bit object identifier has wrapped around.

10. Fixed a bug where the write-ahead-log (WAL) segment files for PostgreSQL logical replication were not deleted when changing the `wal_level` value from `logical` to `replica`.

11. Fixed a bug in the `pg_hint_plan` extension where a multi-statement query could lead to a crash when `enable_hint_table` is enabled. This is tracked in the PostgreSQL community as `https://github.com/ossc-db/pg_hint_plan/issues/25`.

12. Fixed a bug where JDBC clients might report the message `java.io.IOException: Unexpected packet type: 75 following a scale event in an Aurora serverless DB cluster`.

13. Fixed a bug in PostgreSQL logical replication that resulted in the message `ERROR: snapshot reference is not owned by resource owner TopTransaction`.

14. Changed the following extensions:
   - Updated `orafce` to version 3.8
   - Updated `pgTAP` to version 1.1

15. Provided support for fault injection queries.

**Version 3.1, compatible with PostgreSQL 11.6**

This version of Aurora PostgreSQL is compatible with PostgreSQL 11.6. For more information about the improvements in release 11.6, see PostgreSQL release 11.6.

This release contains multiple critical stability enhancements. Amazon highly recommends upgrading your Aurora PostgreSQL clusters that use older PostgreSQL 11 engines to this release.

**Patch versions**

- Version 3.1.3 (p. 1156)
- Version 3.1.2 (p. 1156)
- Version 3.1.1 (p. 1156)
- Version 3.1.0 (p. 1157)
Version 3.1.3

New features
1. Aurora PostgreSQL now supports the PostgreSQL `vacuum_truncate` storage parameter to manage vacuum truncation for specific tables. Set this storage parameter to false for a table to prevent the `VACUUM` SQL command from truncating the table's trailing empty pages.

Critical stability enhancements
• None

High priority stability enhancements
1. Fixed a bug where reads from storage might stop responding due to incorrect error handling.

Additional improvements and enhancements
• None

Version 3.1.2

This release contains a critical stability enhancement. Amazon highly recommends updating your older Aurora PostgreSQL 11-compatible clusters to this release.

Critical stability enhancements
• Fixed a bug whereby a reader DB instance might temporarily use stale data. This could lead to wrong results such as too few or too many rows. This error is not persisted on storage, and will clear when the database page containing the row has been evicted from cache. This can happen when the primary DB instance enters a transaction snapshot overflow due to having more than 64 subtransactions in a single transaction. Applications susceptible to this bug include those that use SQL savepoints or PostgreSQL exception handlers with more than 64 subtransactions in the top transaction.

High priority stability enhancements
• Fixed a bug that might cause a reader DB instance to crash causing unavailability while attempting to join the DB cluster. This can happen in some cases when the primary DB instance has a transaction snapshot overflow due to a high number of subtransactions. In this situation the reader DB instance will be unable to join until the snapshot overflow has cleared.

Additional improvements and enhancements
• Fixed a bug that prevented Performance Insights from determining the query ID of a running statement.

Version 3.1.1

You can find the following improvements in this engine update.
Critical stability enhancements

1. Fixed a bug whereby the DB instance might be briefly unavailable due to the self-healing function of the underlying storage.

High priority stability enhancements

1. Fixed a bug whereby the database engine might crash causing unavailability. This occurred while scanning an included, non-key column of a B-Tree index. This only applies to PostgreSQL 11 "included column" indexes.
2. Fixed a bug that might cause the database engine to crash causing unavailability. This occurred if a newly established database connection encountered a resource exhaustion-related error during initialization after successful authentication.

Additional improvements and enhancements

1. Provided a fix for the pg_hint_plan extension that could lead the database engine to crash causing unavailability. The open source issue can be tracked at https://github.com/ossc-db/pg_hint_plan/pull/45.
2. Fixed a bug where SQL of the form ALTER FUNCTION ... OWNER TO ... would incorrectly report ERROR: improper qualified name (too many dotted names).
3. Improved the performance of GIN index vacuum via prefetching.
4. Fixed a bug in open source PostgreSQL that could lead to a database engine crash causing unavailability. This occurred during parallel B-Tree index scans. This issue has been reported to the PostgreSQL community.
5. Improved the performance of in-memory B-Tree index scans.

Version 3.1.0

You can find the following new features and improvements in this engine version.

New features

1. Support for exporting data to Amazon S3. For more information, see Exporting data from an Aurora PostgreSQL DB cluster to Amazon S3 (p. 1040).
2. Support for Amazon Aurora Machine Learning. For more information, see Using machine learning (ML) with Aurora PostgreSQL (p. 1079).
3. SQL processing enhancements include:
   - Optimizations for NOT IN with the apg_enable_not_in_transform parameter.
   - Semi-join filter pushdown enhancements for hash joins with the apg_enable_semi_join_push_down parameter.
   - Optimizations for redundant inner join removal with the apg_enable_remove_redundant_inner_joins parameter.
   - Improved ANSI compatibility options with the ansi_constraint_trigger_ordering, ansi_force_foreign_key_checks and ansi_qualified_update_set_target parameters.

For more information, see Amazon Aurora PostgreSQL parameters (p. 1137).
4. New and updated PostgreSQL extensions include:
   - The new aws_ml extension. For more information, see Using machine learning (ML) with Aurora PostgreSQL (p. 1079).
   - The new aws_s3 extension. For more information, see Exporting data from an Aurora PostgreSQL DB cluster to Amazon S3 (p. 1040).
• Updates to the `apg_plan_mgmt` extension. For more information, see Managing query execution plans for Aurora PostgreSQL (p. 1049)

**Critical stability enhancements**

1. Fixed a bug related to creating B-tree indexes on temporary tables that in rare cases might result in longer recovery time, and impact availability.
2. Fixed a bug related to replication when Aurora PostgreSQL is acting as a physical replica of an RDS PostgreSQL instance. In rare cases, this bug causes a log write failure that might result in longer recovery time, and impact availability.
3. Fixed a bug related to handling of reads with high I/O latency that in rare cases might result in longer recovery time, and impact availability.

**High priority stability enhancements**

1. Fixed a bug related to logical replication whereby `wal` segments are not properly removed from storage. This can result in storage bloat. To monitor this, view the `TransactionLogDiskUsage` parameter.
2. Fixed multiple bugs, which cause Aurora to crash during prefetch operations on Btree indexes.
3. Fixed a bug whereby an Aurora restart might time out when logical replication is used.
4. Enhanced the validation checks performed on data blocks in the buffer cache. This improves Aurora's detection of inconsistency.

**Additional improvements and enhancements**

1. The query plan management extension `apg_plan_mgmt` has an improved algorithm for managing plan generation for highly partitioned tables.
2. Reduced startup time on instances with large caches via improvements in the buffer cache recovery algorithm.
3. Improved the performance of the read-node-apply process under high transaction rate workloads by using changes to PostgreSQL LWLock prioritization. These changes prevent starvation of the read-node-apply process while the PostgreSQL ProcArray is under heavy contention.
4. Improved handling of batch reads during vacuum, table scans, and index scans. This results in greater throughput and lower CPU consumption.
5. Fixed a bug whereby a read node might crash during the replay of a PostgreSQL SLRU-truncate operation.
6. Fixed a bug where in rare cases, database writes might stall following an error returned by one of the six copies of an Aurora log record.
7. Fixed a bug related to logical replication where an individual transaction larger than 1 GB in size might result in an engine crash.
8. Fixed a memory leak on read nodes when cluster cache management is enabled.
9. Fixed a bug whereby importing an RDS PostgreSQL snapshot might stop responding if the source snapshot contains a large number of unlogged relations.
10. Fixed a bug whereby the Aurora storage daemon might crash under heavy I/O load.
11. Fixed a bug related to `hot_standby_feedback` for read nodes whereby the read node might report the wrong transaction id epoch to the write node. This can cause the write node to ignore the `hot_standby_feedback` and invalidate snapshots on the read node.
12. Fixed a bug whereby storage errors that occur during `CREATE DATABASE` statements are not properly handled. The bug would leave the resulting database inaccessible. The correct behavior is to fail the database creation and return the appropriate error to the user.
13. Improved handling of PostgreSQL snapshot overflow when a read node attempts to connect to a write node. Prior to this change, if the write node was in a snapshot overflow state, the read node would be unable to join. A message would appear in the PostgreSQL log file in the form, DEBUG: recovery snapshot waiting for non-overflowed snapshot or until oldest active xid on standby is at least xxxxxxx (now yyyyyyy). A snapshot overflow occurs when an individual transaction has created over 64 subtransactions.

14. Fixed a bug related to common table expressions whereby an error is incorrectly raised when a NOT IN class exists in a CTE. The error is CTE with NOT IN fails with ERROR: could not find CTE CTE-Name.

15. Fixed a bug related to an incorrect last_error_timestamp value in the aurora_replica_status table.

16. Fixed a bug to avoid populating shared buffers with blocks belonging to temporary objects. These blocks correctly reside in PostgreSQL backend local buffers.

17. Changed the following extensions:
   - Updated pg_hint_plan to version 1.3.4.
   - Added plprofiler version 4.1.
   - Added pgTAP version 1.0.0.

Version 3.0, compatible with PostgreSQL 11.4

This version of Aurora PostgreSQL is compatible with PostgreSQL 11.4. For more information about the improvements in release 11.4, see PostgreSQL release 11.4.

You can find the following improvements in this engine update.

Improvements

1. This release contains all fixes, features, and improvements present in Version 2.3.5 (p. 1170).
2. Partitioning – Partitioning improvements include support for hash partitioning, enabling creation of a default partition, and dynamic row movement to another partition based on the key column update.
3. Performance – Performance improvements include parallelism while creating indexes, materialized views, hash joins, and sequential scans to make the operations perform better.
4. Stored procedures – SQL stored procedures now added support for embedded transactions.
5. Autovacuum improvements – To provide valuable logging, the parameter rds.force_autovacuum_logging is ON by default in conjunction with the log_autovacuum_min_duration parameter set to 10 seconds. To increase autovacuum effectiveness, the values for the autovacuum_max_workers and autovacuum_vacuum_cost_limit parameters are computed based on host memory capacity to provide larger default values.
6. Improved transaction timeout – The parameter idle_in_transaction_session_timeout is set to 12 hours. Any session that has been idle more than 12 hours is terminated.
7. The tsearch2 module is no longer supported – If your application uses tsearch2 functions, update it to use the equivalent functions provided by the core PostgreSQL engine. For more information about the tsearch2 module, see PostgreSQL tsearch2.
8. The chkpass module is no longer supported – For more information about the chkpass module, see PostgreSQL chkpass.
9. Updated the following extensions:
   - address_standardizer to version 2.5.1
   - address_standardizer_data_us to version 2.5.1
   - btree_gin to version 1.3
   - citext to version 1.5
   - cube to version 1.4
• hstore to version 1.5
• ip4r to version 2.2
• isn to version 1.2
• orafce to version 3.7
• pg_hint_plan to version 1.3.4
• pg_prewarm to version 1.2
• pg_repack to version 1.4.4
• pg_trgm to version 1.4
• pgaudit to version 1.3
• pgRouting to version 2.6.1
• pgtap to version 1.0.0
• plcoffee to version 2.3.8
• plls to version 2.3.8
• plv8 to version 2.3.8
• postgis to version 2.5.1
• postgis_tiger_geocoder to version 2.5.1
• postgis_topology to version 2.5.1
• rds_activity_stream to version 1.3

Version 2.7, compatible with PostgreSQL 10.14

This version of Aurora PostgreSQL is compatible with PostgreSQL 10.14. For more information about the improvements in release 10.14, see PostgreSQL release 10.14.

Version 2.7.0

Critical stability enhancements

• None

High priority stability enhancements

2. Fixed a bug in Aurora PostgreSQL replication that might result in the following error message: ERROR: MultiXactId nnnn has not been created yet -- apparent wraparound
3. Fixed a bug where in some cases, clusters with logical replication enabled might not remove truncated WAL segment files from storage. This could result in volume size growth.
4. Fixed a bug that caused excessive CPU consumption in the pg_stat_statements extension.

Additional improvements and enhancements

1. Improved the asynchronous mode performance of database activity streams.
2. Aurora Serverless v1 for PostgreSQL now supports query execution on all connections during a scale event.
3. Reduced the delay of the rpo_lag_in_msec metric when publishing to CloudWatch for Aurora global database clusters.
4. Fixed a bug in Serverless clusters where transaction processing was unnecessarily suspended for long periods when creating a scale point.
5. Fixed a bug in Aurora Serverless v1 for PostgreSQL where a leaked lock resulted in a prolonged scale event.

6. Fixed a bug in Aurora Serverless v1 for PostgreSQL where connections being migrated during a scale event would be disconnected with the following message: ERROR: could not open relation with OID ...

7. Aurora PostgreSQL now avoids falling behind on a read node that occurred when the backend blocked writing to the database client.

8. Fixed a bug that in rare cases caused a brief period of unavailability on a read replica when the storage volume grew.

9. Fixed a bug when creating a database that could return the following error: ERROR: could not create directory on local disk

10. Fixed a bug where in some cases replaying XLOG_BTREE_REUSE_PAGE records on Aurora reader instances caused unnecessary replay lag.

11. Fixed a bug in the GiST index that could result in an out of memory condition after promoting an Aurora read replica.

12. Fixed a bug where the aurora_replica_status function showed truncated server identifiers.

13. Fixed an S3 export bug that reported the error ERROR: HTTP 403. Permission denied when importing data from a file inside an S3 subfolder.

14. Fixed a bug in the aws_s3 extension for pre-signed URL handling that might result in the error message S3 bucket names with a period (.) are not supported.

15. Fixed a bug in the aws_s3 extension where an import might be blocked indefinitely if an exclusive lock was taken on the relation prior to beginning the operation.

16. Fixed a bug related to replication when Aurora PostgreSQL is acting as a physical replica of an RDS PostgreSQL instance that uses GiST indexes. In rare cases, this bug caused a brief period of unavailability after promoting the Aurora cluster.

17. Fixed a bug in database activity streams where customers were not notified of the end of an outage.

Version 2.6, compatible with PostgreSQL 10.13

This version of Aurora PostgreSQL is compatible with PostgreSQL 10.13. For more information about the improvements in release 10.13, see PostgreSQL release 10.13.

Patch versions

- Version 2.6.1 (p. 1161)
- Version 2.6.0 (p. 1162)

Version 2.6.1

You can find the following improvements in this engine update.

Critical stability enhancements

1. Fixed a bug which materializes when the NOT EXISTS operator incorrectly returns TRUE which can only happen under the following unusual set of circumstances:
   - A query is using the NOT EXISTS operator.
   - The column or columns being evaluated against the outer query in the NOT EXISTS subquery contain a NULL value.
   - There is not another predicate in the subquery that removes the need for the evaluation of the NULL values.
   - The filter used in the subquery does not use an index seek for its execution.
   - The operator is not converted to a join by the query optimizer.
Version 2.6.0

You can find the following improvements in this engine update.

**New features**

1. Added support for the RDKit extension version 3.8.

   The RDKit extension provides modeling functions for cheminformatics. Cheminformatics is storing, indexing, searching, retrieving, and applying information about chemical compounds. For example, with the RDKit extension you can construct models of molecules, search for molecular structures, and read or create molecules in various notations. You can also perform research on data loaded from the ChEMBL website or a SMILES file. The Simplified Molecular Input Line Entry System (SMILES) is a typographical notation for representing molecules and reactions. For more information, see The RDKit database cartridge in the RDKit documentation.

2. Added support for the pglogical extension version 2.2.2.

   The pglogical extension is a logical streaming replication system that provides additional features beyond what's available in PostgreSQL native logical replication. Features include conflict handling, row filtering, DDL/sequence replication and delayed apply. You can use the pglogical extension to set up replication between Aurora PostgreSQL clusters, between RDS PostgreSQL and Aurora PostgreSQL, and with PostgreSQL databases running outside of RDS.

3. Aurora dynamically resizes your cluster storage space. With dynamic resizing, the storage space for your Aurora DB cluster automatically decreases when you remove data from the DB cluster. For more information, see Storage scaling (p. 349).

   **Note**
   The dynamic resizing feature is being deployed in phases to the AWS Regions where Aurora is available. Depending on the Region where your cluster is, this feature might not be available yet. For more information, see the What's New announcement.

**Critical stability enhancements**

1. Fixed a bug related to heap page extend that in rare cases resulted in longer recovery time and impacted availability.

**High priority stability enhancements**

1. Fixed a bug when upgrading Aurora Global Database clusters from 10.11.
2. Fixed a bug in Aurora Global Database that could cause delays in upgrading the database engine in a secondary AWS Region. For more information, see Using Amazon Aurora global databases (p. 206).
3. Fixed a bug that in rare cases caused delays in upgrading a database to engine version 10.13.

**Additional improvements and enhancements**

1. Fixed a bug where the Aurora replica crashed when workloads with heavy subtransactions are made on the writer instance.
2. Fixed a bug where the writer instance crashed due to a memory leak and the depletion of memory used to track active transactions.
3. Fixed a bug that lead to a crash due to improper initialization when there is no free memory available during PostgreSQL backend startup.
4. Fixed a bug where an Aurora PostgreSQL Serverless DB cluster might return the following error after a scaling event: ERROR: prepared statement "S_6" already exists.
5. Fixed an out-of-memory problem when issuing the `CREATE EXTENSION` command with PostGIS when Database Activity Streams enabled.
6. Fixed a bug where a `SELECT` query might incorrectly return the error Attempting to read past EOF of relation rrrr. blockno=bbb nblocks=nnn.
7. Fixed a bug where the database might be unavailable briefly due to error handling in database storage growth.
8. Fixed a bug in Aurora PostgreSQL Serverless where queries that executed on previously idle connections got delayed until the scale operation completed.
9. Fixed a bug where an Aurora PostgreSQL DB cluster with Database Activity Streams enabled might report the beginning of a potential loss window for activity records, but does not report the restoration of connectivity.

Version 2.5, compatible with PostgreSQL 10.12

This version of Aurora PostgreSQL is compatible with PostgreSQL 10.12. For more information about the improvements in release 10.12, see PostgreSQL release 10.12.

Patch versions

- Version 2.5.6 (p. 1163)
- Version 2.5.4 (p. 1164)
- Version 2.5.3 (p. 1164)
- Version 2.5.2 (p. 1164)
- Version 2.5.1 (p. 1165)

Version 2.5.6

You can find the following improvements in this engine update.

Critical stability enhancements

- None

High priority stability enhancements

1. Fixed a bug in Aurora PostgreSQL replication that might result in the error message, ERROR: MultiXactId nnnn has not been created yet -- apparent wraparound.

Additional improvements and enhancements

1. Fixed a bug that in rare cases caused brief read replica unavailability when storage volume grew.
2. Aurora PostgreSQL Serverless now supports execution of queries on all connections during a scale event.
3. Fixed a bug in Aurora PostgreSQL Serverless where a leaked lock resulted in a prolonged scale event.
4. Fixed a bug where the `aurora_replica_status` function showed truncated server identifiers.
5. Fixed a bug in Aurora PostgreSQL Serverless where connections being migrated during a scale event would disconnect with the message: "ERROR: could not open relation with OID ....
6. Fixed a bug in a GiST index that might result in an out of memory condition after promoting an Aurora Read Replica.
8. Fixed a bug in Database Activity Streams where customers were not notified when an outage ended.
9. Fixed a bug in the `aws_s3` extension for pre-signed URL handling that might have resulted in the error message S3 bucket names with a period (.) are not supported.

10. Fixed a bug in the `aws_s3` extension where incorrect error handling could lead to failures during the import process.

11. Fixed a bug in the `aws_s3` extension where an import may be blocked indefinitely if an exclusive lock was taken on the relation prior to beginning the operation.

**Version 2.5.4**

You can find the following improvements in this engine update.

**Critical stability enhancements**

1. Fixed a bug which materializes when the `NOT EXISTS` operator incorrectly returns TRUE which can only happen under the following unusual set of circumstances:
   - A query is using the `NOT EXISTS` operator.
   - The column or columns being evaluated against the outer query in the `NOT EXISTS` subquery contain a NULL value.
   - There is not another predicate in the subquery that removes the need for the evaluation of the NULL values.
   - The filter used in the subquery does not use an index seek for its execution.
   - The operator is not converted to a join by the query optimizer.

**Version 2.5.3**

You can find the following improvements in this engine update.

**Critical stability enhancements**

- None

**High priority stability enhancements**

- None

**Additional improvements and enhancements**

1. Fixed a bug in Aurora PostgreSQL Serverless where queries that ran on previously idle connections got delayed until the scale operation completed.
2. Fixed a bug that might cause brief unavailability for heavy subtransaction workloads when multiple reader instances restart or rejoin the cluster.
3. Fixed a bug in Aurora PostgreSQL Global Database where upgrading a secondary cluster might result in failure due to incorrect checksum versioning. This might have required re-creating the secondary clusters.

**Version 2.5.2**

You can find the following improvements in this engine update.

**Critical stability enhancements**

1. Fixed a bug related to heap page extend that in rare cases resulted in longer recovery time and impacted availability.
High priority stability enhancements

1. Fixed a bug in Aurora Global Database that could cause delays in upgrading the database engine in a secondary region. For more information, see Using Amazon Aurora global databases (p. 206).
2. Fixed a bug that in rare cases caused delays in upgrading a database to engine version 10.12.

Additional improvements and enhancements

1. Fixed a bug where the database might be unavailable briefly due to error handling in database storage growth.
2. Fixed a bug where a SELECT query might incorrectly return the error, Attempting to read past EOF of relation rrrr. blockno=bbb nblocks=nnn.
3. Fixed a bug where an Aurora PostgreSQL Serverless DB cluster might return the following error after a scaling event: ERROR: prepared statement "S_6" already exists.

Version 2.5.1

New features

1. Added support for Amazon Aurora PostgreSQL Global Database. For more information, see Using Amazon Aurora global databases (p. 206).
2. Added the ability to configure the recovery point objective (RPO) of a global database for Aurora PostgreSQL. For more information, see Managing recovery for Aurora global databases (p. 245).

You can find the following improvements in this engine update.

Critical stability enhancements

None.

High priority stability enhancements

1. Improved performance and availability of read instances when applying DROP TABLE and TRUNCATE TABLE operations.
2. Fixed a small but continuous memory leak in a diagnostic module that could lead to an out-of-memory condition on smaller DB instance types.
3. Fixed a bug in the PostGIS extension which could lead to a database restart. This has been reported to the PostGIS community as https://trac.osgeo.org/postgis/ticket/4646.
4. Fixed a bug where read requests might stop responding due to incorrect error handling in the storage engine.
5. Fixed a bug that fails for some queries and results in the message ERROR: found xmin xxxxxxx from before relfrozenxid yyyyyyy. This could occur following the promotion of a read instance to a write instance.
6. Fixed a bug where an Aurora serverless DB cluster might crash while rolling back a scale attempt.

Additional improvements and enhancements

1. Improved performance for queries that read many rows from storage.
2. Improved performance and availability of reader DB instances during heavy read workload.
3. Enabled correlated IN and NOT IN subqueries to be transformed to joins when possible.
4. Improved read performance of the pg_prewarm extension.
5. Fixed a bug where an Aurora serverless DB cluster might report the message ERROR: incorrect binary data format in bind parameter ... following a scale event.

6. Fixed a bug where a serverless DB cluster might report the message ERROR: insufficient data left in message following a scale event.

7. Fixed a bug where an Aurora serverless DB cluster may experience prolonged or failed scale attempts.

8. Fixed a bug that resulted in the message ERROR: could not create file "base/xxxxx/yyyyyyy" as a previous version still exists on disk: Success. Please contact AWS customer support. This can occur during object creation after PostgreSQL's 32-bit object identifier has wrapped around.

9. Fixed a bug where the write-ahead-log (WAL) segment files for PostgreSQL logical replication were not deleted when changing the wal_level value from logical to replica.

10. Fixed a bug in the pg_hint_plan extension where a multi-statement query could lead to a crash when enable_hint_table is enabled. This is tracked in the PostgreSQL community as https://github.com/ossc-db/pg_hint_plan/issues/25.

11. Fixed a bug where JDBC clients might report the message java.io.IOException: Unexpected packet type: 75 following a scale event in an Aurora serverless DB cluster.

12. Fixed a bug in PostgreSQL logical replication that resulted in the message ERROR: snapshot reference is not owned by resource owner TopTransaction.

13. Changed the following extensions:
   • Updated orafce to version 3.8

Version 2.4, compatible with PostgreSQL 10.11

This version of Aurora PostgreSQL is compatible with PostgreSQL 10.11. For more information about the improvements in release 10.11, see PostgreSQL release 10.11.

This release contains multiple critical stability enhancements. Amazon highly recommends upgrading your Aurora PostgreSQL clusters that use older PostgreSQL 10 engines to this release.

Patch versions
   • Version 2.4.3 (p. 1166)
   • Version 2.4.2 (p. 1167)
   • Version 2.4.1 (p. 1167)
   • Version 2.4.0 (p. 1168)

Version 2.4.3

New features

1. Aurora PostgreSQL now supports the PostgreSQL vacuum_truncate storage parameter to manage vacuum truncation for specific tables. Set this storage parameter to false for a table to prevent the VACUUM SQL command from truncating the table’s trailing empty pages.

Critical stability enhancements
   • None

High priority stability enhancements

1. Fixed a bug where reads from storage might stop responding due to incorrect error handling.
Additional improvements and enhancements

- None

Version 2.4.2

You can find the following improvements in this engine update.

Critical stability enhancements

1. Fixed a bug whereby a reader DB instance might temporarily use stale data. This could lead to wrong results such as too few or too many rows. This error is not persisted on storage, and will clear when the database page containing the row has been evicted from cache. This can happen when the primary DB instance enters a transaction snapshot overflow due to having more than 64 subtransactions in a single transaction. Applications susceptible to this bug include those that use SQL savepoints or PostgreSQL exception handlers with more than 64 subtransactions in the top transaction.

High priority stability enhancements

1. Fixed a bug that may cause a reader DB instance to crash causing unavailability while attempting to join the DB cluster. This can happen in some cases when the primary DB instance has a transaction snapshot overflow due to a high number of subtransactions. In this situation the reader DB instance will be unable to join until the snapshot overflow has cleared.

Additional improvements and enhancements

1. Fixed a bug that prevented Performance Insights from determining the query ID of a running statement.

Version 2.4.1

You can find the following improvements in this engine update.

Critical stability enhancements

1. Fixed a bug whereby the DB instance might be briefly unavailable due to the self-healing function of the underlying storage.

High priority stability enhancements

1. Fixed a bug that might cause the database engine to crash causing unavailability. This occurred if a newly established database connection encountered a resource exhaustion-related error during initialization after successful authentication.

Additional improvements and enhancements

1. Provided a fix for the pg_hint_plan extension that could lead the database engine to crash causing unavailability. The open source issue can be tracked at https://github.com/ossc-db/pg_hint_plan/pull/45.
2. Fixed a bug where SQL of the form ALTER FUNCTION ... OWNER TO ... would incorrectly report ERROR: improper qualified name (too many dotted names).
3. Improved the performance of GIN index vacuum via prefetching.
4. Fixed a bug in open source PostgreSQL that could lead to a database engine crash causing unavailability. This occurred during parallel B-Tree index scans. This issue has been reported to the PostgreSQL community.

5. Improved the performance of in-memory B-Tree index scans.

6. Additional general improvements to the stability and availability of Aurora PostgreSQL.

Version 2.4.0

You can find the following new features and improvements in this engine version.

New features

1. Support for exporting data to Amazon S3. For more information, see Exporting data from an Aurora PostgreSQL DB cluster to Amazon S3 (p. 1040).

2. Support for Amazon Aurora Machine Learning. For more information, see Using machine learning (ML) with Aurora PostgreSQL (p. 1079).

3. SQL processing enhancements include:
   - Optimizations for NOT IN with the apg_enable_not_in_transform parameter.
   - Semi-join filter pushdown enhancements for hash joins with the apg_enable-semi-join-push_down parameter.
   - Optimizations for redundant inner join removal with the apg_enable_remove-redundant-inner-joins parameter.
   - Improved ANSI compatibility options with the ansi_constraint_trigger_ordering, ansi_force-foreign_key_checks and ansi_qualified_update_set_target parameters.

   For more information, see Amazon Aurora PostgreSQL parameters (p. 1137).

4. New and updated PostgreSQL extensions include:
   - The new aws_ml extension. For more information, see Using machine learning (ML) with Aurora PostgreSQL (p. 1079).
   - The new aws_s3 extension. For more information, see Exporting data from an Aurora PostgreSQL DB cluster to Amazon S3 (p. 1040).
   - Updates to the apg_plan_mgmt extension. For more information, see Managing query execution plans for Aurora PostgreSQL (p. 1049)

Critical stability enhancements

1. Fixed a bug related to creating B-tree indexes on temporary tables that in rare cases may result in longer recovery time, and impact availability.

2. Fixed a bug related to replication when Aurora PostgreSQL is acting as a physical replica of an RDS PostgreSQL instance. In rare cases, this bug causes a log write failure that may result in longer recovery time, and impact availability.

3. Fixed a bug related to handling of reads with high I/O latency that in rare cases may result in longer recovery time, and impact availability.

High priority stability enhancements

1. Fixed a bug related to logical replication whereby wal segments are not properly removed from storage. This can result in storage bloat. To monitor this, view the TransactionLogDiskUsage parameter.

2. Fixed multiple bugs, which cause Aurora to crash during prefetch operations on Btree indexes.

3. Fixed a bug whereby an Aurora restart may timeout when logical replication is used.
4. Enhanced the validation checks performed on data blocks in the buffer cache. This improves Aurora's detection of inconsistency.

**Additional improvements and enhancements**

1. The query plan management extension `apg_plan_mgmt` has an improved algorithm for managing plan generation for highly partitioned tables.
2. Reduced startup time on instances with large caches via improvements in the buffer cache recovery algorithm.
3. Improved the performance of the read-node-apply process under high transaction rate workloads by using changes to PostgreSQL `LWLock` prioritization. These changes prevent starvation of the read-node-apply process while the PostgreSQL `ProcArray` is under heavy contention.
4. Improved handling of batch reads during vacuum, table scans, and index scans. This results in greater throughput and lower CPU consumption.
5. Fixed a bug whereby a read node may crash during the replay of a PostgreSQL `SLRU-truncate` operation.
6. Fixed a bug where in rare cases, database writes may stall following an error returned by one of the six copies of an Aurora log record.
7. Fixed a bug related to logical replication where an individual transaction larger than 1 Gb in size may result in an engine crash.
8. Fixed a memory leak on read nodes when cluster cache management is enabled.
9. Fixed a bug whereby importing an RDS PostgreSQL snapshot might stop responding if the source snapshot contains a large number of unlogged relations.
10. Fixed a bug whereby the Aurora storage daemon may crash under heavy I/O load.
11. Fixed a bug related to `hot_standby_feedback` for read nodes whereby the read node may report the wrong transaction id epoch to the write node. This can cause the write node to ignore the `hot_standby_feedback` and invalidate snapshots on the read node.
12. Fixed a bug whereby storage errors that occur during `CREATE DATABASE` statements are not properly handled. The bug would leave the resulting database inaccessible. The correct behavior is to fail the database creation and return the appropriate error to the user.
13. Improved handling of PostgreSQL snapshot overflow when a read node attempts to connect to a write node. Prior to this change, if the write node was in a snapshot overflow state, the read node would be unable to join. A message would appear in the PostgreSQL log file in the form, `DEBUG: recovery snapshot waiting for non-overflowed snapshot or until oldest active xid on standby is at least xxxxxxx (now yyyyyyy)`. A snapshot overflow occurs when an individual transaction has created over 64 subtransactions.
14. Fixed a bug related to common table expressions whereby an error is incorrectly raised when a NOT IN class exists in a CTE. The error is `CTE with NOT IN fails with ERROR: could not find CTE CTE-Name`.
15. Fixed a bug related to an incorrect last_error_timestamp value in the `aurora_replica_status` table.
16. Fixed a bug to avoid populating shared buffers with blocks belonging to temporary objects. These blocks correctly reside in PostgreSQL backend local buffers.
17. Improved the performance of vacuum cleanup on GIN indexes.
18. Fixed a bug where in rare cases Aurora may exhibit 100% CPU utilization while acting as a replica of an RDS PostgreSQL instance even when the replication stream is idle.
19. Backported a change from PostgreSQL 11 which improves the cleanup of orphaned temporary tables. Without this change, it is possible that in rare cases orphaned temporary tables can lead to transaction ID wraparound. For more information, see this PostgreSQL community commit.
20. Fixed a bug where a Writer instance may accept replication registration requests from Reader instances while having an uninitialized startup process.
21.Changed the following extensions:
   • Updated `pg_hint_plan` to version 1.3.3.
   • Added `plprofiler` version 4.1.

Version 2.3, compatible with PostgreSQL 10.7

This version of Aurora PostgreSQL is compatible with PostgreSQL 10.7. For more information about the improvements in release 10.7, see PostgreSQL release 10.7.

Patch versions
   • Version 2.3.5 (p. 1170)
   • Version 2.3.3 (p. 1170)
   • Version 2.3.1 (p. 1171)
   • Version 2.3.0 (p. 1171)

Version 2.3.5

You can find the following improvements in this engine update.

Improvements

1. Fixed a bug that could cause DB instance restarts.
2. Fixed a bug that could cause a crash when the PostgreSQL backend exits while using logical replication.
3. Fixed a bug that could cause a restart when reads occurred during failovers.
4. Fixed a bug with the `wal2json` module for logical replication.
5. Fixed a bug that could result in inconsistent metadata.

Version 2.3.3

You can find the following improvements in this engine update.

Improvements

3. Fixed a bug whereby data activity streaming could consume excessive CPU time.
4. Fixed a bug whereby parallel threads scanning a B-tree index might stop responding following a disk read.
5. Fixed a bug where use of the `not in` predicate against a common table expression (CTE) could return the following error: "ERROR: bad levelsup for CTE".
6. Fixed a bug whereby the read node replay process might stop responding while applying a modification to a generalized search tree (GiST) index.
7. Fixed a bug whereby visibility map pages could contain incorrect freeze bits following a failover to a read node.
8. Optimized log traffic between the write node and read nodes during index maintenance.
9. Fixed a bug whereby queries on read nodes may crash while performing a B-tree index scan.
10. Fixed a bug whereby a query that has been optimized for redundant inner join removal could crash.
11. The function `aurora_stat_memctx_usage` now reports the number of instances of a given context name.
12 Fixed a bug whereby the function `aurora_stat_memctx_usage` reported incorrect results.
13 Fixed a bug whereby the read node replay process could wait to stop conflicting queries beyond the configured `max_standby_streaming_delay` value.
14 Additional information is now logged on read nodes when active connections conflict with the relay process.
15 Provided a backport fix for the PostgreSQL community bug #15677, where a crash could occur while deleting from a partitioned table.

**Version 2.3.1**

You can find the following improvements in this engine update.

**Improvements**

1. Fixed multiple bugs related to I/O prefetching that caused engine crashes.

**Version 2.3.0**

You can find the following improvements in this engine update.

**New features**

1. Aurora PostgreSQL now performs I/O prefetching while scanning B-tree indexes. This results in significantly improved performance for B-tree scans over uncached data.

**Improvements**

1. Fixed a bug whereby read nodes may fail with the error "too many LWLocks taken".
2. Addressed numerous issues that caused read nodes to fail to startup while the cluster is under heavy write workload.
3. Fixed a bug whereby usage of the `aurora_stat_memctx_usage()` function could lead to a crash.
4. Improved the cache replacement strategy used by table scans to minimize thrashing of the buffer cache.

**Version 2.2, compatible with PostgreSQL 10.6**

This version of Aurora PostgreSQL is compatible with PostgreSQL 10.6. For more information about the improvements in release 10.6, see [PostgreSQL release 10.6](#).

**Patch versions**

- Version 2.2.1 (p. 1171)
- Version 2.2.0 (p. 1172)

**Version 2.2.1**

You can find the following improvements in this engine update.

**Improvements**

1. Improved stability of logical replication.
2. Fixed a bug which could cause an error running queries. The message reported would be of the form "CLOG segment 123 does not exist: No such file or directory".
3. Increased the supported size of IAM passwords to 8KB.
4. Improved consistency of performance under high throughput write workloads.
5. Fixed a bug which could cause a read replica to crash during a restart.
6. Fixed a bug which could cause an error running queries. The message reported would be of the form "SQL ERROR: Attempting to read past EOF of relation".
7. Fixed a bug which could cause an increase in memory usage after a restart.
8. Fixed a bug which could cause a transaction with a large number of subtransactions to fail.
9. Merged a patch from community PostgreSQL which addresses potential failures when using GIN indexes. For more information see https://git.postgresql.org/gitweb/?p=postgresql.git;a=commit;h=f9e66f2fbb49a493045c8d8086a9b15d95b8f18.
10. Fixed a bug which could cause a snapshot import from RDS for PostgreSQL to fail.

Version 2.2.0

You can find the following improvements in this engine update.

New features

1. Added the restricted password management feature. Restricted password management enables you to restrict who can manage user passwords and password expiration changes by using the parameter rds.restrict_password_commands and the role rds_password. For more information, see Restricting password management (p. 998).

Version 2.1, compatible with PostgreSQL 10.5

This version of Aurora PostgreSQL is compatible with PostgreSQL 10.5. For more information about the improvements in release 10.5, see PostgreSQL release 10.5.

Patch versions

• Version 2.1.1 (p. 1172)
• Version 2.1.0 (p. 1173)

Version 2.1.1

You can find the following improvements in this engine update.

Improvements

1. Fixed a bug which could cause an error running queries. The message reported would be of the form "CLOG segment 123 does not exist: No such file or directory".
2. Increased the supported size of IAM passwords to 8KB.
3. Improved consistency of performance under high throughput write workloads.
4. Fixed a bug which could cause a read replica to crash during a restart.
5. Fixed a bug which could cause an error running queries. The message reported would be of the form "SQL ERROR: Attempting to read past EOF of relation".
6. Fixed a bug which could cause an increase in memory usage after a restart.
7. Fixed a bug which could cause a transaction with a large number of subtransactions to fail.
8. Merged a patch from community PostgreSQL which addresses potential failures when using GIN indexes. For more information see https://git.postgresql.org/gitweb/?p=postgresql.git;a=commit;h=f9e66f2fbb49a493045c8d8086a9b15d95b8f18.
9. Fixed a bug which could cause a snapshot import from RDS for PostgreSQL to fail.
Version 2.1.0

You can find the following improvements in this engine update.

New features

1. General availability of Aurora Query Plan Management, which enables customers to track and manage any or all query plans used by their applications, to control query optimizer plan selection, and to ensure high and stable application performance. For more information, see Managing query execution plans for Aurora PostgreSQL (p. 1049).
2. Updated the libprotobuf extension to version 1.3.0. This is used by the PostGIS extension.
3. Updated the pg_similarity extension to version 1.0.
4. Updated the log_fdw extension to version 1.1.
5. Updated the pg_hint_plan extension to version 1.3.1.

Improvements

1. Network traffic between the writer and reader nodes is now compressed to reduce network utilization. This reduces the chance of read node unavailability due to network saturation.
2. Implemented a high performance, scalable subsystem for PostgreSQL subtransactions. This improves the performance of applications which make extensive use of savepoints and PL/pgSQL exception handlers.
3. The rds_superuser role can now set the following parameters on a per-session, database, or role level:
   - log_duration
   - log_error_verbosity
   - log_executor_stats
   - log_lock_waits
   - log_min_duration_statement
   - log_min_error_statement
   - log_min_messages
   - log_parser_stats
   - log_planner_stats
   - log_replication_commands
   - log_statement_stats
   - log_temp_files
4. Fixed a bug whereby the SQL command "ALTER FUNCTION ... OWNER TO ..." might fail with error "improper qualified name (too many dotted names)".
5. Fixed a bug whereby a crash could occur while committing a transaction with more than two million subtransactions.
6. Fixed a bug in community PostgreSQL code related to GIN indexes which can cause the Aurora Storage volume to become unavailable.
7. Fixed a bug whereby an Aurora PostgreSQL replica of an RDS for PostgreSQL instance might fail to start, reporting error: "PANIC: could not locate a valid checkpoint record".
8. Fixed a bug whereby passing an invalid parameter to the aurora_stat_backend_waits function could cause a crash.

Known issues

1. The pageinspect extension is not supported in Aurora PostgreSQL.
Version 2.0, compatible with PostgreSQL 10.4

This version of Aurora PostgreSQL is compatible with PostgreSQL 10.4. For more information about the improvements in release 10.4, see PostgreSQL release 10.4.

Patch versions

- Version 2.0.1 (p. 1174)
- Version 2.0.0 (p. 1174)

Version 2.0.1

You can find the following improvements in this engine update.

Improvements

1. Fixed a bug which could cause an error running queries. The message reported would be of the form "CLOG segment 123 does not exist: No such file or directory".
2. Increased the supported size of IAM passwords to 8KB.
3. Improved consistency of performance under high throughput write workloads.
4. Fixed a bug which could cause a read replica to crash during a restart.
5. Fixed a bug which could cause an error running queries. The message reported would be of the form "SQL ERROR: Attempting to read past EOF of relation".
6. Fixed a bug which could cause an increase in memory usage after a restart.
7. Fixed a bug which could cause a transaction with a large number of subtransactions to fail.
8. Merged a patch from community PostgreSQL which addresses potential failures when using GIN indexes. For more information see https://git.postgresql.org/gitweb/?p=postgresql.git;a=commit;h=f9e66f2fbb49a493045c8d8086a9b15d95b8f18.
9. Fixed a bug which could cause a snapshot import from RDS for PostgreSQL to fail.

Version 2.0.0

You can find the following improvements in this engine update.

Improvements

1. This release contains all fixes, features, and improvements present in Version 1.3, compatible with PostgreSQL 9.6.9 (p. 1183).
2. The temporary file size limitation is user-configurable. You require the rds_superuser role to modify the temp_file_limit parameter.
3. Updated the GDAL library, which is used by the PostGIS extension.
4. Updated the ip4r extension to version 2.1.1.
5. Updated the pg_repack extension to version 1.4.3.
6. Updated the plv8 extension to version 2.1.2.
7. Parallel queries – When you create a new Aurora PostgreSQL version 2.0 instance, parallel queries are enabled for the default.postgres10 parameter group. The parameter max_parallel_workers_per_gather is set to 2 by default, but you can modify it to support your specific workload requirements.
8. Fixed a bug whereby read nodes may crash following a specific type of free space change from the write node.
Version 1.9, compatible with PostgreSQL 9.6.19

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.19. For more information about the improvements in release 9.6.19, see PostgreSQL release 9.6.19.

Version 1.9.0

Critical stability enhancements

- None

High priority stability enhancements

2. Fixed a bug in Aurora PostgreSQL replication that might result in the following error message: ERROR: MultiXactId nnnn has not been created yet -- apparent wraparound

Additional improvements and enhancements

1. Aurora PostgreSQL now avoids falling behind on a read node that occurred when the backend blocked writing to the database client.
2. Fixed a bug that in rare cases caused a brief period of unavailability on a read replica when the storage volume grew.
3. Fixed a bug when creating a database that could return the following error: ERROR: could not create directory on local disk
4. Fixed a bug in the GiST index that could result in an out of memory condition after promoting an Aurora read replica.
5. Fixed a bug related to replication when Aurora PostgreSQL is acting as a physical replica of an RDS PostgreSQL instance that uses GiST indexes. In rare cases, this bug caused a brief period of unavailability after promoting the Aurora cluster.

Version 1.8, compatible with PostgreSQL 9.6.18

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.18. For more information about the improvements in release 9.6.18, see PostgreSQL release 9.6.18.

Patch versions

- Version 1.8.0 (p. 1175)

Version 1.8.0

You can find the following improvements in this engine update.

Critical stability enhancements

1. Fixed a bug related to heap page extend that in rare cases resulted in longer recovery time and impacted availability.

Additional improvements and enhancements

1. Fixed a bug where the Aurora replica crashed when workloads with heavy subtransactions are made on the writer instance.
2. Fixed a bug where the writer instance crashed due to a memory leak and the depletion of memory used to track active transactions.

3. Fixed a bug that lead to a crash due to improper initialization when there is no free memory available during PostgreSQL backend startup.

4. Fixed a crash during a BTree prefetch that occurred under certain conditions that depended on the shape and data contained in the index.

5. Fixed a bug where a SELECT query might incorrectly return the error Attempting to read past EOF of relation rrr, blockno=bbb nblocks=nnn.

6. Fixed a bug where the database might be unavailable briefly due to error handling in database storage growth.

Version 1.7, compatible with PostgreSQL 9.6.17

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.17. For more information about the improvements in release 9.6.17, see PostgreSQL release 9.6.17.

Patch versions

• Version 1.7.6 (p. 1176)
• Version 1.7.3 (p. 1176)
• Version 1.7.2 (p. 1177)
• Version 1.7.1 (p. 1177)

Version 1.7.6

You can find the following improvements in this engine update.

Critical stability enhancements

• None

High priority stability enhancements

1. Fixed a bug in Aurora PostgreSQL replication that might result in the error message, ERROR: MultiXactId nnnn has not been created yet -- apparent wraparound.

Additional improvements and enhancements

1. Fixed a bug that in rare cases caused brief read replica unavailability when storage volume grew.
2. Fixed a bug in a b-tree index read optimization that might have caused a brief period of unavailability.
3. Fixed a bug in a GiST index that might result in an out of memory condition after promoting an Aurora Read Replica.

Version 1.7.3

You can find the following improvements in this engine update.

Critical stability enhancements

• None
High priority stability enhancements

- None

Additional improvements and enhancements

1. Fixed a bug that might cause brief unavailability for heavy subtransaction workloads when multiple reader instances restart or rejoin the cluster.

Version 1.7.2

You can find the following improvements in this engine update.

Critical stability enhancements

1. Fixed a bug related to heap page extend that in rare cases resulted in longer recovery time and impacted availability.

High Priority Stability Enhancements

None

Additional improvements and enhancements

1. Fixed a bug where the database might be unavailable briefly due to error handling in database storage growth.
2. Fixed a bug where a SELECT query might incorrectly return the error, Attempting to read past EOF of relation rrr. blockno=bbb nblocks=nnn.
3. Fixed an issue with the internal metrics collector that could result in erratic CPU spikes on database instances.

Version 1.7.1

You can find the following improvements in this engine update.

Critical stability enhancements

None.

High priority stability enhancements

1. Improved performance and availability of read instances when applying DROP TABLE and TRUNCATE TABLE operations.
2. Fixed a small but continuous memory leak in a diagnostic module that could lead to an out-of-memory condition on smaller DB instance types.
3. Fixed a bug in the PostGIS extension which could lead to a database restart. This has been reported to the PostGIS community as https://trac.osgeo.org/postgis/ticket/4646.
4. Fixed a bug where read requests might stop responding due to incorrect error handling in the storage engine.
5. Fixed a bug that fails for some queries and results in the message ERROR: found xmin xxxxxx from before refrozenxid yyyyyyy. This could occur following the promotion of a read instance to a write instance.
Additional improvements and enhancements

1. Improved performance for queries that read many rows from storage.
2. Improved performance and availability of reader DB instances during heavy read workload.
3. Fixed a bug that resulted in the message ERROR: could not create file "base/xxxxxx/yyyyyyy" as a previous version still exists on disk: Success. Please contact AWS customer support. This can occur during object creation after PostgreSQL's 32-bit object identifier has wrapped around.
4. Fixed a bug in the `pg_hint_plan` extension where a multi-statement query could lead to a crash when `enable_hint_table` is enabled. This is tracked in the PostgreSQL community as https://github.com/ossc-db/pg_hint_plan/issues/25.
5. Changed the following extensions:
   - Updated `orafce` to version 3.8

Version 1.6, compatible with PostgreSQL 9.6.16

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.16. For more information about the improvements in release 9.6.16, see PostgreSQL release 9.6.16.

This release contains multiple critical stability enhancements. Amazon highly recommends upgrading your Aurora PostgreSQL clusters that use older PostgreSQL 9.6 engines to this release.

Patch versions

- Version 1.6.3 (p. 1178)
- Version 1.6.2 (p. 1178)
- Version 1.6.1 (p. 1179)
- Version 1.6.0 (p. 1179)

Version 1.6.3

New features

1. Aurora PostgreSQL now supports the PostgreSQL `vacuum_truncate` storage parameter to manage vacuum truncation for specific tables. Set this `storage parameter` to false when creating or altering a table to prevent the `VACUUM` SQL command from truncating the table's trailing empty pages.

Critical stability enhancements

- None

High priority stability enhancements

1. Fixed a bug where reads from storage might stop responding due to incorrect error handling.

Additional improvements and enhancements

- None

Version 1.6.2

You can find the following improvements in this engine update.
Critical stability enhancements

1. Fixed a bug whereby a reader DB instance might temporarily use stale data. This could lead to wrong results such as too few or too many rows. This error is not persisted on storage, and will clear when the database page containing the row has been evicted from cache. This can happen when the primary DB instance enters a transaction snapshot overflow due to having more than 64 subtransactions in a single transaction. Applications susceptible to this bug include those that use SQL savepoints or PostgreSQL exception handlers with more than 64 subtransactions in the top transaction.

High priority stability enhancements

1. Fixed a bug that may cause a reader DB instance to crash causing unavailability while attempting to join the DB cluster. This can happen in some cases when the primary DB instance has a transaction snapshot overflow due to a high number of subtransactions. In this situation the reader DB instance will be unable to join until the snapshot overflow has cleared.

Additional improvements and enhancements

1. Fixed a bug that prevented Performance Insights from determining the query ID of a running statement.

Version 1.6.1

You can find the following improvements in this engine update.

Critical stability enhancements

1. None

High priority stability enhancements

1. Fixed a bug that might cause the database engine to crash causing unavailability. This occurred if a newly established database connection encountered a resource exhaustion-related error during initialization after successful authentication.

Additional improvements and enhancements

1. Provided general improvements to the stability and availability of Aurora PostgreSQL.

Version 1.6.0

You can find the following new features and improvements in this engine version.

New features

1. Updates to the apg_plan_mgmt extension. For more information, see Managing query execution plans for Aurora PostgreSQL (p. 1049)

Critical stability enhancements

1. Fixed a bug related to creating B-tree indexes on temporary tables that in rare cases may result in longer recovery time, and impact availability.
2. Fixed a bug related to replication when Aurora PostgreSQL is acting as a physical replica of an RDS PostgreSQL instance. In rare cases, this bug causes a log write failure that may result in longer recovery time, and impact availability.

3. Fixed a bug related to handling of reads with high I/O latency that in rare cases may result in longer recovery time, and impact availability.

**High priority stability enhancements**

1. Fixed multiple bugs, which cause Aurora to crash during prefetch operations on Btree indexes.

2. Enhanced the validation checks performed on data blocks in the buffer cache. This improves Aurora's detection of inconsistency.

**Additional improvements and enhancements**

1. The query plan management extension `apg_plan_mgmt` has an improved algorithm for managing plan generation for highly partitioned tables.

2. Reduced startup time on instances with large caches via improvements in the buffer cache recovery algorithm.

3. Improved the performance of the read-node-apply process under high transaction rate workloads by using changes to PostgreSQL LWLock prioritization. These changes prevent starvation of the read-node-apply process while the PostgreSQL ProcArray is under heavy contention.

4. Fixed a bug whereby a read node may crash during the replay of a PostgreSQL SLRU-truncate operation.

5. Fixed a bug where in rare cases, database writes might stall following an error returned by one of the six copies of an Aurora log record.

6. Fixed a memory leak on read nodes when cluster cache management is enabled.

7. Fixed a bug whereby importing an RDS PostgreSQL snapshot might stop responding if the source snapshot contains a large number of unlogged relations.

8. Fixed a bug related to `hot_standby_feedback` for read nodes whereby the read node may report the wrong transaction id epoch to the write node. This can cause the write node to ignore the `hot_standby_feedback` and invalidate snapshots on the read node.

9. Fixed a bug whereby storage errors that occur during `CREATE DATABASE` statements are not properly handled. The bug would leave the resulting database inaccessible. The correct behavior is to fail the database creation and return the appropriate error to the user.

10. Improved handling of PostgreSQL snapshot overflow when a read node attempts to connect to a write node. Prior to this change, if the write node was in a snapshot overflow state, the read node would be unable to join. A message would appear in the PostgreSQL log file in the form, `DEBUG: recovery snapshot waiting for non-overflowed snapshot or until oldest active xid on standby is at least `xxxxxxx` (now `yyyyyyy`). A snapshot overflow occurs when an individual transaction has created over 64 subtransactions.

11. Fixed a bug related to common table expressions whereby an error is incorrectly raised when a NOT IN class exists in a CTE. The error is `CTE with NOT IN fails with ERROR: could not find CTE CTE-Name`.

12. Fixed a bug related to an incorrect `last_error_timestamp` value in the `aurora_replica_status` table.

13. Fixed a bug to avoid populating shared buffers with blocks belonging to temporary objects. These blocks correctly reside in PostgreSQL backend local buffers.

14. Fixed a bug where in rare cases Aurora may exhibit 100% CPU utilization while acting as a replica of an RDS PostgreSQL instance even when the replication stream is idle.

15. Backported a change from PostgreSQL 11 which improves the cleanup of orphaned temporary tables. Without this change, it is possible that in rare cases orphaned temporary tables can lead to transaction ID wraparound. For more information, see this PostgreSQL community commit.
16 Fixed a bug where a Writer instance may accept replication registration requests from Reader instances while having an uninitialized startup process.

17 Changed the following extensions:
   • Updated `pg_hint_plan` to version 1.2.5.

**Version 1.5, compatible with PostgreSQL 9.6.12**

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.12. For more information about the improvements in release 9.6.12, see [PostgreSQL release 9.6.12](https://www.postgresql.org/docs/9.6/).

**Patch versions**

- Version 1.5.3 (p. 1181)
- Version 1.5.2 (p. 1181)
- Version 1.5.1 (p. 1181)
- Version 1.5.0 (p. 1182)

**Version 1.5.3**

You can find the following improvements in this engine update.

**Improvements**

1. Fixed a bug that could cause DB instance restarts.
2. Fixed a bug that could cause a restart when reads occurred during failovers.
3. Fixed a bug that could result in inconsistent metadata.

**Version 1.5.2**

You can find the following improvements in this engine update.

**Improvements**

2. Fixed a bug whereby the read node replay process might stop responding while applying a modification to a generalized search tree (GiST) index.
3. Fixed a bug whereby visibility map pages may contain incorrect freeze bits following a failover to a read node.
4. Fixed a bug whereby the error "relation relation-name does not exist" is incorrectly reported.
5. Optimized log traffic between the write node and read nodes during index maintenance.
6. Fixed a bug whereby queries on read nodes may crash while performing a B-tree index scan.
7. The function `aurora_stat_memctx_usage` now reports the number of instances of a given context name.
8. Fixed a bug whereby the function `aurora_stat_memctx_usage` reported incorrect results.
9. Fixed a bug whereby the read node replay process may wait to stop conflicting queries beyond the configured `max_standby_streaming_delay`.
10. Additional information is now logged on read nodes when active connections conflict with the relay process.

**Version 1.5.1**

You can find the following improvements in this engine update.
Improvements

1. Fixed multiple bugs related to I/O prefetching, which caused engine crashes.

Version 1.5.0

You can find the following improvements in this engine update.

New features

1. Aurora PostgreSQL now performs I/O prefetching while scanning B-tree indexes. This results in significantly improved performance for B-tree scans over uncached data.

Improvements

1. Addressed numerous issues that caused read nodes to fail to startup while the cluster is under heavy write workload.
2. Fixed a bug whereby usage of the `aurora_stat_memctx_usage()` function could lead to a crash.
3. Improved the cache replacement strategy used by table scans to minimize thrashing of the buffer cache.

Version 1.4, compatible with PostgreSQL 9.6.11

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.11. For more information about the improvements in release 9.6.11, see PostgreSQL release 9.6.11.

You can find the following improvements in this engine update.

New features

1. Support is added for the `pg_similarity` extension version 1.0.

Improvements

1. This release contains all fixes, features, and improvements present in Version 1.3, compatible with PostgreSQL 9.6.9 (p. 1183).
2. Network traffic between the writer and reader nodes is now compressed to reduce network utilization. This reduces the chance of read node unavailability due to network saturation.
3. Performance of subtransactions has improved under high concurrency workloads.
4. An update for the `pg_hint_plan` extension to version 1.2.3.
5. Fixed an issue where on a busy system, a commit with millions of subtransactions (and sometimes with commit timestamps enabled) can cause Aurora to crash.
6. Fixed an issue where an INSERT statement with VALUES could fail with the message "Attempting to read past EOF of relation".
7. An upgrade of the `apg_plan_mgmt` extension to version 1.0.1. For details, see The Aurora PostgreSQL `apg_plan_mgmt` extension version 1.0.1 (p. 1189).

The `apg_plan_mgmt` extension is used with query plan management. For more about how to install, upgrade, and use the `apg_plan_mgmt` extension, see Managing query execution plans for Aurora PostgreSQL (p. 1049).
Version 1.3, compatible with PostgreSQL 9.6.9

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.9. For more information about the improvements in version 9.6.9, see PostgreSQL release 9.6.9.

Patch versions

- Version 1.3.2 (p. 1183)
- Version 1.3.0 (p. 1183)

Version 1.3.2

You can find the following improvements in this engine update.

New features

1. Added the `ProcArrayGroupUpdate` wait event.

Improvements

1. Fixed a bug which could cause an error running queries. The message reported would be of the form "CLOG segment 123 does not exist: No such file or directory".
2. Increased the supported size of IAM passwords to 8KB.
3. Improved consistency of performance under high throughpout write workloads.
4. Fixed a bug which could cause a read replica to crash during a restart.
5. Fixed a bug which could cause an error running queries. The message reported would be of the form "SQL ERROR: Attempting to read past EOF of relation".
6. Fixed a bug which could cause an increase in memory usage after a restart.
7. Fixed a bug which could cause a transaction with a large number of subtransactions to fail.
8. Merged a patch from community PostgreSQL which addresses potential failures when using GIN indexes. For more information see https://git.postgresql.org/gitweb/?p=postgresql.git;a=commit;h=f9e66f2fbb49a493045c8d8086a9b15d95b8f18.
9. Fixed a bug which could cause a snapshot import from RDS for PostgreSQL to fail.

Version 1.3.0

You can find the following improvements in this engine update.

Improvements

1. This release contains all fixes, features, and improvements present in Version 1.2, compatible with PostgreSQL 9.6.8 (p. 1184).
2. Updated the GDAL library, which is used by the PostGIS extension.
3. Updated the following PostgreSQL extensions:
   - `ip4r` updated to version 2.1.1.
   - `pgaudit` updated to version 1.1.1.
   - `pg_repack` updated to version 1.4.3.
   - `plv8` updated to version 2.1.2.
4. Fixed an issue in the monitoring system that could incorrectly cause a failover when local disk usage is high.
5. Fixed a bug whereby Aurora PostgreSQL can repeatedly crash, reporting:
PANIC: new_record_total_len (8201) must be less than BLCKSZ (8192), rmid (6), info (32)

6. Fixed a bug whereby an Aurora PostgreSQL read node might be unable to rejoin a cluster due to
recovery of a large buffer cache. This issue is unlikely to occur on instances other than r4.16xlarge.

7. Fixed a bug whereby inserting into an empty GIN index leaf page imported from pre-9.4 engine
versions can cause the Aurora storage volume to become unavailable.

8. Fixed a bug whereby, in rare circumstances, a crash during transaction commit could result in the loss
of CommitTs data for the committing transaction. The actual durability of the transaction was not
impacted by this bug.

9. Fixed a bug in the PostGIS extension whereby PostGIS can crash in the function
gserialized_gist_picksplit_2d().

10. Improved the stability of read-only nodes during heavy write traffic on instances smaller than r4.8xlarge.
    This specifically addresses a situation where the network bandwidth between the writer and the
    reader is constrained.

11. Fixed a bug whereby an Aurora PostgreSQL instance acting as a replication target of an RDS for
    PostgreSQL instance crashed with the following error:

    FATAL: could not open file "base/16411/680897_vm": No such file or directory
    during "xlog redo at 782/3122D540 for Storage/TRUNCATE"

12. Fixed a memory leak on read-only nodes whereby the heap size for the "aurora wal replay process" will
    continue to grow. This is observable via Enhanced Monitoring.

13. Fixed a bug whereby Aurora PostgreSQL can fail to start, with the following message reported in the
    PostgreSQL log:

    FATAL: Storage initialization failed.

14. Fixed a performance limitation on heavy write workloads that caused waits on the
    LWLock:buffer_content and IO:ControlFileSyncUpdate events.

15. Fixed a bug whereby read nodes could crash following a specific type of free space change from the
    write node.

Version 1.2, compatible with PostgreSQL 9.6.8

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.8. For more information about the
improvements in version 9.6.8, see PostgreSQL release 9.6.8.

Patch versions

- Version 1.2.2 (p. 1184)
- Version 1.2.0 (p. 1185)

Version 1.2.2

You can find the following improvements in this engine update.

New features

1. Added the ProcArrayGroupUpdate wait event.

Improvements

1. Fixed a bug which could cause an error running queries. The message reported would be of the form
   "CLOG segment 123 does not exist: No such file or directory".
2. Increased the supported size of IAM passwords to 8KB.
3. Improved consistency of performance under high throughput write workloads.
4. Fixed a bug which could cause a read replica to crash during a restart.
5. Fixed a bug which could cause an error running queries. The message reported would be of the form "SQL ERROR: Attempting to read past EOF of relation".
6. Fixed a bug which could cause an increase in memory usage after a restart.
7. Fixed a bug which could cause a transaction with a large number of subtransactions to fail.
8. Merged a patch from community PostgreSQL which addresses potential failures when using GIN indexes. For more information see https://git.postgresql.org/gitweb/?p=postgresql.git;a=commit;h=f9e66f2fbbb49a493045c8d8086a9b15d95b8f18.
9. Fixed a bug which could cause a snapshot import from RDS for PostgreSQL to fail.

Version 1.2.0

You can find the following improvements in this engine update.

New features

1. Introduced the `aurora_stat_memctx_usage()` function. This function reports internal memory context usage for each PostgreSQL backend. You can use this function to help determine why certain backends are consuming large amounts of memory.

Improvements

1. This release contains all fixes, features, and improvements present in Version 1.1, compatible with PostgreSQL 9.6.6 is deprecated (p. 1186).
2. Updates the following PostgreSQL extensions:
   - `pg_hint_plan` updated to version 1.2.2
   - `plv8` updated to version 2.1.0
3. Improves efficiency of traffic between writer and reader nodes.
4. Improves connection establishment performance.
5. Improve the diagnostic data provided in the PostgreSQL error log when an out-of-memory error is encountered.
6. Multiple fixes to improve the reliability and performance of snapshot import from Amazon RDS for PostgreSQL to Aurora with PostgreSQL compatibility.
7. Multiple fixes to improve the reliability and performance of Aurora PostgreSQL read nodes.
8. Fixes a bug in which an otherwise idle instance can generate unnecessary read traffic on an Aurora storage volume.
9. Fixes a bug in which duplicate sequence values can be encountered during insert. The problem only occurs when migrating a snapshot from RDS for PostgreSQL to Aurora PostgreSQL. The fix prevents the problem from being introduced when performing the migration. Instances migrated before this release can still encounter duplicate key errors.
10. Fixes a bug in which an RDS for PostgreSQL instance migrated to Aurora PostgreSQL using replication can run out of memory doing insert/update of GIST indexes, or cause other issues with GIST indexes.
11. Fixes a bug in which vacuum can fail to update the corresponding `pg_database.datfrozenxid` value for a database.
12. Fixes a bug in which a crash while creating a new MultiXact (contended row level lock) can cause Aurora PostgreSQL to stop responding indefinitely on the first access to the same relation after the engine restarts.
13. Fixes a bug in which a PostgreSQL backend can't be terminated or canceled while invoking an `fdw` call.
14 Fixes a bug in which one vCPU is fully utilized at all times by the Aurora storage daemon. This issue is especially noticeable on smaller instance classes, such as r4.large, where it can lead to 25–50 percent CPU usage when idle.

15 Fixes a bug in which an Aurora PostgreSQL writer node can fail over spuriously.

16 Fixes a bug in which, in a rare scenario, an Aurora PostgreSQL read node can report:

"FATAL: lock buffer_io is not held"

17 Fixes a bug in which stale relcache entries can halt vacuuming of relations and push the system close to transaction ID wraparound. The fix is a port of a PostgreSQL community patch scheduled to be released in a future minor version.

18 Fixes a bug in which a failure while extending a relation can cause Aurora to crash while scanning the partially extended relation.

**Version 1.1, compatible with PostgreSQL 9.6.6 is deprecated**

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.6. For more information about the improvements in version 9.6.6 see, PostgreSQL release 9.6.6.

You can find the following improvements in this engine update:

**New features**

1. Introduced the `aurora_stat_utils` extension. This extension includes two functions:
   - `aurora_wait_report()` function for wait event monitoring
   - `aurora_log_report()` for log record write monitoring

2. Added support for the following extensions:
   - orafce 3.6.1
   - pgrouting 2.4.2
   - postgresql-hll 2.10.2
   - prefix 1.2.6

**Improvements**

1. This release contains all fixes, features, and improvements present in Version 1.0.11 (p. 1187)

2. Updates for the following PostgreSQL extensions:
   - postgis extension updated to version 2.3.4
   - geos library updated to version 3.6.2
   - `pg_repack` updated to version 1.4.2

3. Access to the `pg_statistic` relation enabled.

4. Disabled the 'effective_io_concurrency' guc parameter, as it does not apply to Aurora storage.

5. Changed the 'hot_standby_feedback' guc parameter to not-modifiable and set the value to '1'.

6. Improved heap page read performance during a vacuum operation.

7. Improved performance of snapshot conflict resolution on read nodes.

8. Improved performance of transaction snapshot acquisition on read nodes.

9. Improved write performance for GIN meta page updates.

10. Improved buffer cache recovery performance during startup.

11. Fixes a bug that caused a database engine crash at startup while recovering prepared transactions.

12. Fixes a bug that could result in the inability to start a read node when there are a large number of prepared transactions.
13 Fixes a bug that could cause a read node to report:

ERROR: could not access status of transaction 6080077

DETAIL: * *Could not open file "pg_subtrans/005C": No such file or directory.

14 Fixes a bug that could cause the error below when replicating from RDS PostgreSQL to Aurora PostgreSQL:

FATAL: lock buffer_content is not held

CONTEXT: xlog redo at 46E/F1330870 for Storage/TRUNCATE: base/13322/8058750 to 0 blocks flags 7

15 Fixes a bug that could cause Aurora PostgreSQL to stop responding while replaying a multixact WAL record when replicating from RDS PostgreSQL to Aurora PostgreSQL.

16 Multiple improvements to the reliability of importing snapshots from RDS PostgreSQL to Aurora PostgreSQL.

**Version 1.0, compatible with PostgreSQL 9.6.3 is deprecated**

This version of Aurora PostgreSQL is compatible with PostgreSQL 9.6.3. For more information about the improvements in version 9.6.3 see, [PostgreSQL release 9.6.3](https://www.postgresql.org/docs/9.6/release-9.6.3.html).

This version includes the following patch versions:

**Patch versions**

- Version 1.0.11 (p. 1187)
- Version 1.0.10 (p. 1187)
- Version 1.0.9 (p. 1188)
- Version 1.0.8 (p. 1188)
- Version 1.0.7 (p. 1188)

**Version 1.0.11**

You can find the following improvements in this engine update:

1. Fixes an issue with parallel query processing that can lead to incorrect results.
2. Fixes an issue with visibility map handling during replication from Amazon RDS for PostgreSQL that can cause the Aurora storage volume to become unavailable.
3. Corrects the pg-repack extension.
4. Implements improvements to maintain fresh nodes.
5. Fixes issues that can lead to an engine crash.

**Version 1.0.10**

This update includes a new feature. You can now replicate an Amazon RDS PostgreSQL DB instance to Aurora PostgreSQL. For more information, see [Replication with Amazon Aurora PostgreSQL](https://docs.aws.amazon.com/AmazonAurora/latest/UserGuide/Changelog-1034.html) (p. 1034).

You can find the following improvements in this engine update:

1. Adds error logging when a cache exists and a parameter change results in a mismatched buffer cache, storage format, or size.
2. Fixes an issue that causes an engine reboot if there is an incompatible parameter value for huge pages.
3. Improves handling of multiple truncate table statements during a replay of a write ahead log (WAL) on a read node.
4. Reduces static memory overhead to reduce out-of-memory errors.
5. Fixes an issue that can lead to out-of-memory errors while performing an insert with a GiST index.
6. Improves snapshot import from RDS PostgreSQL, removing the requirement that a vacuum be performed on uninitialized pages.
7. Fixes an issue that causes prepared transactions to return to the previous state following an engine crash.
8. Implements improvements to prevent read nodes from becoming stale.
9. Implements improvements to reduce downtime with an engine restart.
10. Fixes issues that can cause an engine crash.

Version 1.0.9

In this engine update, we fix an issue that can cause the Aurora storage volume to become unavailable when importing a snapshot from RDS PostgreSQL that contained uninitialized pages.

Version 1.0.8

You can find the following improvements in this engine update:

1. Fixes an issue that prevented the engine from starting if the `shared_preload_libraries` instance parameter contained `pg_hint_plan`.
2. Fixes the error "Attempt to fetch heap block XXX is beyond end of heap (YYY blocks)," which can occur during parallel scans.
3. Improves the effectiveness of prefetching on reads for a vacuum.
4. Fixes issues with snapshot import from RDS PostgreSQL, which can fail if there are incompatible `pg_internal.init` files in the source snapshot.
5. Fixes an issue that can cause a read node to crash with the message "aurora wal replay process (PID XXX) was terminated by signal 11: Segmentation fault". This issue occurs when the reader applied a visibility map change for an uncached visibility map page.

Version 1.0.7

This is the first generally available release of Amazon Aurora with PostgreSQL compatibility.

Extensions and modules for Amazon Aurora PostgreSQL

Aurora PostgreSQL apg_plan_mgmt extension

Topics

- The Aurora PostgreSQL apg_plan_mgmt extension version 2.0 (p. 1188)
- The Aurora PostgreSQL apg_plan_mgmt extension version 1.0.1 (p. 1189)

The Aurora PostgreSQL apg_plan_mgmt extension version 2.0

You use the `apg_plan_mgmt` extension with query plan management. For more about how to install, upgrade, and use the `apg_plan_mgmt` extension, see Managing query execution plans for Aurora PostgreSQL (p. 1049).
The apg_plan_mgmt extension changes for version 2.0 include the following:

**New extension features**

1. You can now manage all queries inside SQL functions, whether they have parameters or not.
2. You can now manage all queries inside PL/pgSQL functions, whether they have parameters or not.
3. You can now manage queries in generic plans, whether they have parameters or not. To learn more about generic plans versus custom plans, see the `PREPARE` statement in the PostgreSQL documentation.
4. You can now use query plan management to enforce the use of specific types of aggregate methods in query plans.

**Extension improvements**

1. You can now save plans with a size up to 8KB times the setting of the `max_worker_processes` parameter. Previously the maximum plan size was 8KB.
2. Fixed bugs for unnamed prepared statements such as those from JDBC.
3. Previously, when you tried to do `CREATE EXTENSION apg_plan_mgmt` when it is not loaded in the `shared_preload_libraries`, the PostgreSQL backend connection would be dropped. Now, an error message prints and the connection is not dropped.
4. The default value of the `cardinality_error` in the `apg_plan_mgmt.plans` table is NULL, but it can be set to -1 during the `apg_plan_mgmt.evolve_plan_baselines` function. NULL is now used consistently.
5. Plans are now saved for queries that refer to temporary tables.
6. The default maximum number of plans is increased from 1000 to 10000.
7. The following `pgss` parameters are deprecated because the automatic plan capture mode should be used instead of those parameters.
   - `apg_plan_mgmt.pgss_min_calls`
   - `apg_plan_mgmt.pgss_min_mean_time_ms`
   - `apg_plan_mgmt.pgss_min_stddev_time_ms`
   - `apg_plan_mgmt.pgss_min_total_time_ms`

The Aurora PostgreSQL apg_plan_mgmt extension version 1.0.1

The apg_plan_mgmt extension changes for version 1.0.1 include the following:

**New extension features**

1. A new `update_plan_hash` parameter is available for the `validate_plans` function. This parameter updates the `plan_hash` for plans that can't be reproduced exactly. The `update_plan_hash` parameter also enables you to fix a plan by rewriting the SQL. You can then register the good plan as an Approved plan for the original SQL. Following is an example of using `update_plan_hash`.

   ```sql
   UPDATE apg_plan_mgmt.dba_plans SET plan_hash = new_plan_hash, plan_outline = good_plan_outline
   WHERE sql_hash = bad_plan_sql_hash AND plan_hash = bad_plan_plan_hash;
   SELECT apg_plan_mgmt.validate_plans(bad_plan_sql_hash, bad_plan_plan_hash, 'update_plan_hash');
   SELECT apg_plan_mgmt.reload();
   ```

2. A new `get_explain_stmt` function is available that generates the text of an `EXPLAIN` statement for the specified SQL statement. It includes the parameters `sql_hash`, `plan_hash` and `explain_options`.
The parameter `explain_options` can be any comma-separated list of valid EXPLAIN options, as shown following.

```
analyze,verbose,buffers,hashes,format json
```

If the parameter `explain_options` is NULL or an empty string, the `get_explain_stmt` function generates a simple EXPLAIN statement.

To create an EXPLAIN script for your workload or a portion of it, use the `\a`, `\t`, and `\o` options to redirect the output to a file. For example, you can create an EXPLAIN script for the top-ranked (top-K) statements by using the PostgreSQL `pg_stat_statements` view sorted by `total_time` in DESC order.

3. The precise location of the Gather parallel query operator is determined by costing, and may change slightly over time. To prevent these differences from invalidating the entire plan, query plan management now computes the same `plan_hash` even if the Gather operators move to different places in the plan tree.

4. Support is added for nonparameterized statements inside pl/pgsql functions.

5. Overhead is reduced when the `apg_plan_mgmt` extension is installed on multiple databases in the same cluster while two or more databases are being accessed concurrently. Also, this release fixed a bug in this area that caused plans to not be stored in shared memory.

**Extension improvements**

1. Improvements to the `evolve_plan_baselines` function.
   a. The `evolve_plan_baselines` function now computes a `cardinality_error` metric over all nodes in the plan. Using this metric, you can identify any plan where the cardinality estimation error is large, and the plan quality is more doubtful. Long-running statements with high `cardinality_error` values are high-priority candidates for query tuning.
   b. Reports generated by `evolve_plan_baselines` now include `sql_hash`, `plan_hash`, and the `plan status`.
   c. You can now allow `evolve_plan_baselines` to approve previously `Rejected` plans.
   d. The meaning of `speedup_factor` for `evolve_plan_baselines` is now always relative to the baseline plan. For example, a value of 1.1 now means 10 percent faster than the baseline plan. A value of 0.9 means 10 percent slower than the baseline plan. The comparison is made using running time alone instead of total time.
   e. The `evolve_plan_baselines` function now warms the cache in a new way. It does this by running the baseline plan, then running the baseline plan one more time, and then running the candidate plan once. Previously, `evolve_plan_baselines` ran the candidate plan twice. This approach added significantly to running time, especially for slow candidate plans. However, running the candidate plan twice is more reliable when the candidate plan uses an index that isn't used in the baseline plan.

2. Query plan management no longer saves plans that refer to system tables or views, temporary tables, or the query plan management's own tables.

3. Bug fixes include caching a plan immediately when saved and fixing a bug that caused the back end to terminate.
Best practices with Amazon Aurora

Following, you can find information on general best practices and options for using or migrating data to an Amazon Aurora DB cluster.

Some of the best practices for Amazon Aurora are specific to a particular database engine. For more information about Aurora best practices specific to a database engine, see the following.

<table>
<thead>
<tr>
<th>Database engine</th>
<th>Best practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Aurora MySQL</td>
<td>See Best practices with Amazon Aurora MySQL (p. 840)</td>
</tr>
<tr>
<td>Amazon Aurora PostgreSQL</td>
<td>See Best practices with Amazon Aurora PostgreSQL (p. 1116)</td>
</tr>
</tbody>
</table>

Note
For common recommendations for Aurora, see Using Amazon Aurora recommendations (p. 484).

Topics
- Basic operational guidelines for Amazon Aurora (p. 1191)
- DB instance RAM recommendations (p. 1191)
- Monitoring Amazon Aurora (p. 1192)
- Working with DB parameter groups and DB cluster parameter groups (p. 1192)
- Amazon Aurora best practices presentation video (p. 1192)

Basic operational guidelines for Amazon Aurora

The following are basic operational guidelines that everyone should follow when working with Amazon Aurora. The Amazon RDS Service Level Agreement requires that you follow these guidelines:

- Monitor your memory, CPU, and storage usage. You can set up Amazon CloudWatch to notify you when usage patterns change or when you approach the capacity of your deployment. This way, you can maintain system performance and availability.
- If your client application is caching the Domain Name Service (DNS) data of your DB instances, set a time-to-live (TTL) value of less than 30 seconds. The underlying IP address of a DB instance can change after a failover. Thus, caching the DNS data for an extended time can lead to connection failures if your application tries to connect to an IP address that no longer is in service. Aurora DB clusters with multiple read replicas can experience connection failures also when connections use the reader endpoint and one of the read replica instances is in maintenance or is deleted.
- Test failover for your DB cluster to understand how long the process takes for your use case. Testing failover can help you ensure that the application that accesses your DB cluster can automatically connect to the new DB cluster after failover.

DB instance RAM recommendations

To optimize performance, allocate enough RAM so that your working set resides almost completely in memory. To determine whether your working set is almost all in memory, examine the following metrics in Amazon CloudWatch:
Monitoring Amazon Aurora

Amazon Aurora provides a variety of Amazon CloudWatch metrics that you can monitor to determine the health and performance of your Aurora DB cluster. You can use various tools, such as the AWS Management Console, AWS CLI, and CloudWatch API, to view Aurora metrics. For more information, see Monitoring an Amazon Aurora DB cluster (p. 459).

Working with DB parameter groups and DB cluster parameter groups

We recommend that you try out DB parameter group and DB cluster parameter group changes on a test DB cluster before applying parameter group changes to your production DB cluster. Improperly setting DB engine parameters can have unintended adverse effects, including degraded performance and system instability.

Always use caution when modifying DB engine parameters, and back up your DB cluster before modifying a DB parameter group. For information about backing up your DB cluster, see Backing up and restoring an Amazon Aurora DB cluster (p. 414).

Amazon Aurora best practices presentation video

The 2016 AWS Summit conference in Chicago included a presentation on best practices for creating and configuring an Amazon Aurora DB cluster to be more secure and highly available. For a video of the presentation, see Amazon Aurora best practices on the AWS YouTube channel.
Performing a proof of concept with Amazon Aurora

Following, you can find an explanation of how to set up and run a proof of concept for Aurora. A proof of concept is an investigation that you do to see if Aurora is a good fit with your application. The proof of concept can help you understand Aurora features in the context of your own database applications and how Aurora compares with your current database environment. It can also show what level of effort you need to move data, port SQL code, tune performance, and adapt your current management procedures.

In this topic, you can find an overview and a step-by-step outline of the high-level procedures and decisions involved in running a proof of concept, listed following. For detailed instructions, you can follow links to the full documentation for specific subjects.

Overview of an Aurora proof of concept

When you conduct a proof of concept for Amazon Aurora, you learn what it takes to port your existing data and SQL applications to Aurora. You exercise the important aspects of Aurora at scale, using a volume of data and activity that's representative of your production environment. The objective is to feel confident that the strengths of Aurora match up well with the challenges that cause you to outgrow your previous database infrastructure. At the end of a proof of concept, you have a solid plan to do larger-scale performance benchmarking and application testing. At this point, you understand the biggest work items on your way to a production deployment.

The following advice about best practices can help you avoid common mistakes that cause problems during benchmarking. However, this topic doesn't cover the step-by-step process of performing benchmarks and doing performance tuning. Those procedures vary depending on your workload and the Aurora features that you use. For detailed information, consult performance-related documentation such as Managing performance and scaling for Aurora DB clusters (p. 349), Amazon Aurora MySQL performance enhancements (p. 634), Managing Amazon Aurora PostgreSQL (p. 1028), and Using Amazon RDS Performance Insights (p. 514).

The information in this topic applies mainly to applications where your organization writes the code and designs the schema and that support the MySQL and PostgreSQL open-source database engines. If you're testing a commercial application or code generated by an application framework, you might not have the flexibility to apply all of the guidelines. In such cases, check with your AWS representative to see if there are Aurora best practices or case studies for your type of application.

1. Identify your objectives

When you evaluate Aurora as part of a proof of concept, you choose what measurements to make and how to evaluate the success of the exercise.

You must ensure that all of the functionality of your application is compatible with Aurora. Because Aurora is wire-compatible with MySQL 5.6 and MySQL 5.7 and also PostgreSQL 9.6 and PostgreSQL 10.4, most applications developed for those engines are also compatible with Aurora. However, you must still validate compatibility on a per-application basis.

For example, some of the configuration choices that you make when you set up an Aurora cluster influence whether you can or should use particular database features. You might start with the most
general-purpose kind of Aurora cluster, known as provisioned. You might then decide if a specialized configuration such as serverless or parallel query offers benefits for your workload.

Use the following questions to help identify and quantify your objectives:

- Does Aurora support all functional use cases of your workload?
- What dataset size or load level do you want? Can you scale to that level?
- What are your specific query throughput or latency requirements? Can you reach them?
- What is the minimum acceptable amount of planned or unplanned downtime for your workload? Can you achieve it?
- What are the necessary metrics for operational efficiency? Can you accurately monitor them?
- Does Aurora support your specific business goals, such as cost reduction, increase in deployment, or provisioning speed? Do you have a way to quantify these goals?
- Can you meet all security and compliance requirements for your workload?

Take some time to build knowledge about Aurora database engines and platform capabilities, and review the service documentation. Take note of all the features that can help you achieve your desired outcomes. One of these might be workload consolidation, described in the AWS Database Blog post How to plan and optimize Amazon Aurora with MySQL compatibility for consolidated workloads. Another might be demand-based scaling, described in Using Amazon Aurora Auto Scaling with Aurora replicas (p. 372) in the Amazon Aurora User Guide. Others might be performance gains or simplified database operations.

2. Understand your workload characteristics

Evaluate Aurora in the context of your intended use case. Aurora is a good choice for online transaction processing (OLTP) workloads. You can also run reports on the cluster that holds the real-time OLTP data without provisioning a separate data warehouse cluster. You can recognize if your use case falls into these categories by checking for the following characteristics:

- High concurrency, with dozens, hundreds, or thousands of simultaneous clients.
- Large volume of low-latency queries (milliseconds to seconds).
- Short, real-time transactions.
- Highly selective query patterns, with index-based lookups.
- For HTAP, analytical queries that can take advantage of Aurora parallel query.

One of the key factors affecting your database choices is the velocity of the data. High velocity involves data being inserted and updated very frequently. Such a system might have thousands of connections and hundreds of thousands of simultaneous queries reading from and writing to a database. Queries in high-velocity systems usually affect a relatively small number of rows, and typically access multiple columns in the same row.

Aurora is designed to handle high-velocity data. Depending on the workload, an Aurora cluster with a single r4.16xlarge DB instance can process more than 600,000 SELECT statements per second. Again depending on workload, such a cluster can process 200,000 INSERT, UPDATE, and DELETE statements per second. Aurora is a row store database and is ideally suited for high-volume, high-throughput, and highly parallelized OLTP workloads.

Aurora can also run reporting queries on the same cluster that handles the OLTP workload. Aurora supports up to 15 replicas (p. 57), each of which is on average within 10–20 milliseconds of the primary instance. Analysts can query OLTP data in real time without copying the data to a separate data
warehouse cluster. With Aurora clusters using the parallel query feature, you can offload much of the processing, filtering, and aggregation work to the massively distributed Aurora storage subsystem.

Use this planning phase to familiarize yourself with the capabilities of Aurora, other AWS services, the AWS Management Console, and the AWS CLI. Also, check how these work with the other tooling that you plan to use in the proof of concept.

3. Practice with the AWS Management Console or AWS CLI

As a next step, practice with the AWS Management Console or the AWS CLI, to become familiar with these tools and with Aurora.

**Practice with the AWS Management Console**

The following initial activities with Aurora database clusters are mainly so you can familiarize yourself with the AWS Management Console environment and practice setting up and modifying Aurora clusters. If you use the MySQL-compatible and PostgreSQL-compatible database engines with Amazon RDS, you can build on that knowledge when you use Aurora.

By taking advantage of the Aurora shared storage model and features such as replication and snapshots, you can treat entire database clusters as another kind of object that you freely manipulate. You can set up, tear down, and change the capacity of Aurora clusters frequently during the proof of concept. You aren't locked into early choices about capacity, database settings, and physical data layout.

To get started, set up an empty Aurora cluster. Choose the **provisioned** capacity type and **regional** location for your initial experiments.

Connect to that cluster using a client program such as a SQL command-line application. Initially, you connect using the cluster endpoint. You connect to that endpoint to perform any write operations, such as data definition language (DDL) statements and extract, transform, load (ETL) processes. Later in the proof of concept, you connect query-intensive sessions using the reader endpoint, which distributes the query workload among multiple DB instances in the cluster.

Scale the cluster out by adding more Aurora Replicas. For those procedures, see Replication with Amazon Aurora (p. 57). Scale the DB instances up or down by changing the AWS instance class. Understand how Aurora simplifies these kinds of operations, so that if your initial estimates for system capacity are inaccurate, you can adjust later without starting over.

Create a snapshot and restore it to a different cluster.

Examine cluster metrics to see activity over time, and how the metrics apply to the DB instances in the cluster.

It's useful to become familiar with how to do these things through the AWS Management Console in the beginning. After you understand what you can do with Aurora, you can progress to automating those operations using the AWS CLI. In the following sections, you can find more details about the procedures and best practices for these activities during the proof-of-concept period.

**Practice with the AWS CLI**

We recommend automating deployment and management procedures, even in a proof-of-concept setting. To do so, become familiar with the AWS CLI if you're not already. If you use the MySQL-compatible and PostgreSQL-compatible database engines with Amazon RDS, you can build on that knowledge when you use Aurora.
4. Create your Aurora cluster

Aurora typically involves groups of DB instances arranged in clusters. Thus, many operations involve determining which DB instances are associated with a cluster and then performing administrative operations in a loop for all the instances.

For example, you might automate steps such as creating Aurora clusters, then scaling them up with larger instance classes or scaling them out with additional DB instances. Doing so helps you to repeat any stages in your proof of concept and explore what-if scenarios with different kinds or configurations of Aurora clusters.

Learn the capabilities and limitations of infrastructure deployment tools such as AWS CloudFormation. You might find activities that you do in a proof-of-concept context aren't suitable for production use. For example, the AWS CloudFormation behavior for modification is to create a new instance and delete the current one, including its data. For more details on this behavior, see Update behaviors of stack resources in the AWS CloudFormation User Guide.

4. Create your Aurora cluster

With Aurora, you can explore what-if scenarios by adding DB instances to the cluster and scaling up the DB instances to more powerful instance classes. You can also create clusters with different configuration settings to run the same workload side by side. With Aurora, you have a lot of flexibility to set up, tear down, and reconfigure DB clusters. Given this, it's helpful to practice these techniques in the early stages of the proof-of-concept process. For the general procedures to create Aurora clusters, see Creating an Amazon Aurora DB cluster (p. 118).

Where practical, start with a cluster using the following settings. Skip this step only if you have certain specific use cases in mind. For example, you might skip this step if your use case requires a specialized kind of Aurora cluster. Or you might skip it if you need a particular combination of database engine and version.

- Amazon Aurora.
- MySQL 5.6 compatibility. This combination of database engine and version has the widest compatibility with other Aurora features.
- Turn off quick create. For the proof of concept, we recommend that you be aware of all the settings you choose so that you can create identical or slightly different clusters later.
- Regional. The Global setting is for specific high availability scenarios. You can try it out later after your initial functional and performance experiments.
- One writer, multiple readers. This is the most widely used, general purpose kind of cluster. This setting persists for the life of the cluster. Thus, if you later do experiments with other kinds of clusters such as serverless or parallel query, you create other clusters and compare and contrast the results on each.
- Choose the Dev/Test template. This choice isn't significant for your proof-of-concept activities.
- For Instance Size, choose Memory Optimized and one of the xlarge instance classes. You can adjust the instance class up or down later.
- Under Multi-AZ Deployment, choose Create Replica in Different Zone. Many of the most useful aspects of Aurora involve clusters of multiple DB instances. It makes sense to always start with at least two DB instances in any new cluster. Using a different Availability Zone for the second DB instance helps to test different high availability scenarios.
- When you pick names for the DB instances, use a generic naming convention. Don't refer to any cluster DB instance as the "master" or "writer," because different DB instances assume those roles as needed. We recommend using something like clusternamexazserialnumber, for example myprodappdb-a-01. These pieces uniquely identify the DB instance and its placement.
- Set the backup retention high for the Aurora cluster. With a long retention period, you can do point-in-time recovery (PITR) for a period up to 35 days. You can reset your database to a known state after running tests involving DDL and data manipulation language (DML) statements. You can also recover if you delete or change data by mistake.
5. Set up your schema

On the Aurora cluster, set up databases, tables, indexes, foreign keys, and other schema objects for your application. If you're moving from another MySQL-compatible or PostgreSQL-compatible database system, expect this stage to be simple and straightforward. You use the same SQL syntax and command line or other client applications that you're familiar with for your database engine.

To issue SQL statements on your cluster, find its cluster endpoint and supply that value as the connection parameter to your client application. You can find the cluster endpoint on the Connectivity tab of the detail page of your cluster. The cluster endpoint is the one labeled Writer. The other endpoint, labeled Reader, represents a read-only connection that you can supply to end users who run reports or other read-only queries. For help with any issues around connecting to your cluster, see Connecting to an Amazon Aurora DB cluster (p. 253).

If you're porting your schema and data from a different database system, expect to make some schema changes at this point. These schema changes are to match the SQL syntax and capabilities available in Aurora. You might leave out certain columns, constraints, triggers, or other schema objects at this point. Doing so can be useful particularly if these objects require rework for Aurora compatibility and aren't significant for your objectives with the proof of concept.

If you're migrating from a database system with a different underlying engine than Aurora's, consider using the AWS Schema Conversion Tool (AWS SCT) to simplify the process. For details, see the AWS Schema Conversion Tool User Guide. For general details about migration and porting activities, see the AWS whitepaper Aurora migration handbook.

During this stage, you can evaluate whether there are inefficiencies in your schema setup, for example in your indexing strategy or other table structures such as partitioned tables. Such inefficiencies can be amplified when you deploy your application on a cluster with multiple DB instances and a heavy workload. Consider whether you can fine-tune such performance aspects now, or during later activities such as a full benchmark test.

6. Import your data

During the proof of concept, you bring across the data, or a representative sample, from your former database system. If practical, set up at least some data in each of your tables. Doing so helps to test compatibility of all data types and schema features. After you have exercised the basic Aurora features, scale up the amount of data. By the time you finish the proof of concept, you should test your ETL tools, queries, and overall workload with a dataset that's big enough to draw accurate conclusions.

You can use several techniques to import either physical or logical backup data to Aurora. For details, see Migrating data to an Amazon Aurora MySQL DB cluster (p. 644) or Migrating data to Amazon Aurora with PostgreSQL compatibility (p. 1005) depending on the database engine you're using in the proof of concept.

Experiment with the ETL tools and technologies that you're considering. See which one best meets your needs. Consider both throughput and flexibility. For example, some ETL tools perform a one-time transfer, and others involve ongoing replication from the old system to Aurora.
7. Port your SQL code

Trying out SQL and associated applications requires different levels of effort depending on different cases. In particular, the level of effort depends on whether you move from a MySQL-compatible or PostgreSQL-compatible system or another kind.

- If you're moving from RDS MySQL or PostgreSQL, the SQL changes are small enough that you can try the original SQL code with Aurora and manually incorporate needed changes.
- Similarly, if you move from an on-premises database compatible with MySQL or PostgreSQL, you can try the original SQL code and manually incorporate changes.
- If you're coming from a different commercial database, the required SQL changes are more extensive. In this case, consider using the AWS SCT.

During this stage, you can evaluate whether there are inefficiencies in your schema setup, for example in your indexing strategy or other table structures such as partitioned tables. Consider whether you can fine-tune such performance aspects now, or during later activities such as a full benchmark test.

You can verify the database connection logic in your application. To take advantage of Aurora distributed processing, you might need to use separate connections for read and write operations, and use relatively short sessions for query operations. For information about connections, see 9. Connect to Aurora (p. 1199).

Consider if you had to make compromises and tradeoffs to work around issues in your production database. Build time into the proof-of-concept schedule to make improvements to your schema design and queries. To judge if you can achieve easy wins in performance, operating cost, and scalability, try the original and modified applications side by side on different Aurora clusters.

For details about migration and porting activities, see the AWS whitepaper Aurora migration handbook.

8. Specify configuration settings

You can also review your database configuration parameters as part of the Aurora proof-of-concept exercise. You might already have MySQL or PostgreSQL configuration settings tuned for performance and scalability in your current environment. The Aurora storage subsystem is adapted and tuned for a distributed cloud-based environment with a high-speed storage subsystem. As a result, many former database engine settings don't apply. We recommend conducting your initial experiments with the default Aurora configuration settings. Reapply settings from your current environment only if you encounter performance and scalability bottlenecks. If you're interested, you can look more deeply into this subject in Introducing the Aurora storage engine on the AWS Database Blog.

Aurora makes it easy to reuse the optimal configuration settings for a particular application or use case. Instead of editing a separate configuration file for each DB instance, you manage sets of parameters that you assign to entire clusters or specific DB instances. For example, the time zone setting applies to all DB instances in the cluster, and you can adjust the page cache size setting for each DB instance.
You start with one of the default parameter sets, and apply changes to only the parameters that you need to fine-tune. For details about working with parameter groups, see Amazon Aurora DB cluster and DB instance parameters (p. 300). For the configuration settings that are or aren't applicable to Aurora clusters, see Aurora MySQL parameters (p. 848) or Amazon Aurora PostgreSQL parameters (p. 1137) depending on your database engine.

9. Connect to Aurora

As you find when doing your initial schema and data setup and running sample queries, you can connect to different endpoints in an Aurora cluster. The endpoint to use depends on whether the operation is a read such as `SELECT` statement, or a write such as a `CREATE` or `INSERT` statement. As you increase the workload on an Aurora cluster and experiment with Aurora features, it's important for your application to assign each operation to the appropriate endpoint.

By using the cluster endpoint for write operations, you always connect to a DB instance in the cluster that has read/write capability. By default, only one DB instance in an Aurora cluster has read/write capability. This DB instance is called the primary instance. If the original primary instance becomes unavailable, Aurora activates a failover mechanism and a different DB instance takes over as the primary.

Similarly, by directing `SELECT` statements to the reader endpoint, you spread the work of processing queries among the DB instances in the cluster. Each reader connection is assigned to a different DB instance using round-robin DNS resolution. Doing most of the query work on the read-only DB Aurora Replicas reduces the load on the primary instance, freeing it to handle DDL and DML statements.

Using these endpoints reduces the dependency on hard-coded hostnames, and helps your application to recover more quickly from DB instance failures.

**Note**

Aurora also has custom endpoints that you create. Those endpoints usually aren’t needed during a proof of concept.

The Aurora Replicas are subject to a replica lag, even though that lag is usually 10 to 20 milliseconds. You can monitor the replication lag and decide whether it is within the range of your data consistency requirements. In some cases, your read queries might require strong read consistency (read-after-write consistency). In these cases, you can continue using the cluster endpoint for them and not the reader endpoint.

To take full advantage of Aurora capabilities for distributed parallel execution, you might need to change the connection logic. Your objective is to avoid sending all read requests to the primary instance. The read-only Aurora Replicas are standing by, with all the same data, ready to handle `SELECT` statements. Code your application logic to use the appropriate endpoint for each kind of operation. Follow these general guidelines:

- Avoid using a single hard-coded connection string for all database sessions.
- If practical, enclose write operations such as DDL and DML statements in functions in your client application code. That way, you can make different kinds of operations use specific connections.
- Make separate functions for query operations. Aurora assigns each new connection to the reader endpoint to a different Aurora Replica to balance the load for read-intensive applications.
- For operations involving sets of queries, close and reopen the connection to the reader endpoint when each set of related queries is finished. Use connection pooling if that feature is available in your software stack. Directing queries to different connections helps Aurora to distribute the read workload among the DB instances in the cluster.

For general information about connection management and endpoints for Aurora, see Connecting to an Amazon Aurora DB cluster (p. 253). For a deep dive on this subject, see Aurora MySQL database administrator's handbook – Connection management.
10. Run your workload

After the schema, data, and configuration settings are in place, you can begin exercising the cluster by running your workload. Use a workload in the proof of concept that mirrors the main aspects of your production workload. We recommend always making decisions about performance using real-world tests and workloads rather than synthetic benchmarks such as sysbench or TPC-C. Wherever practical, gather measurements based on your own schema, query patterns, and usage volume.

As much as practical, replicate the actual conditions under which the application will run. For example, you typically run your application code on Amazon EC2 instances in the same AWS Region and the same virtual private cloud (VPC) as the Aurora cluster. If your production application runs on multiple EC2 instances spanning multiple Availability Zones, set up your proof-of-concept environment in the same way. For more information on AWS Regions, see Regions and Availability Zones in the Amazon RDS User Guide. To learn more about the Amazon VPC service, see What is Amazon VPC? in the Amazon VPC User Guide.

After you've verified that the basic features of your application work and you can access the data through Aurora, you can exercise aspects of the Aurora cluster. Some features you might want to try are concurrent connections with load balancing, concurrent transactions, and automatic replication.

By this point, the data transfer mechanisms should be familiar, and so you can run tests with a larger proportion of sample data.

This stage is when you can see the effects of changing configuration settings such as memory limits and connection limits. Revisit the procedures that you explored in 8. Specify configuration settings (p. 1198).

You can also experiment with mechanisms such as creating and restoring snapshots. For example, you can create clusters with different AWS instance classes, numbers of AWS Replicas, and so on. Then on each cluster, you can restore the same snapshot containing your schema and all your data. For the details of that cycle, see Creating a DB cluster snapshot (p. 418) and Restoring from a DB cluster snapshot (p. 420).

11. Measure performance

Best practices in this area are designed to ensure that all the right tools and processes are set up to quickly isolate abnormal behaviors during workload operations. They're also set up to see that you can reliably identify any applicable causes.

You can always see the current state of your cluster, or examine trends over time, by examining the Monitoring tab. This tab is available from the console detail page for each Aurora cluster or DB instance. It displays metrics from the Amazon CloudWatch monitoring service in the form of charts. You can filter the metrics by name, by DB instance, and by time period.

To have more choices on the Monitoring tab, enable Enhanced Monitoring and Performance Insights in the cluster settings. You can also enable those choices later if you didn't choose them when setting up the cluster.

To measure performance, you rely mostly on the charts showing activity for the whole Aurora cluster. You can verify whether the Aurora Replicas have similar load and response times. You can also see how the work is split up between the read/write primary instance and the read-only Aurora Replicas. If there is some imbalance between the DB instances or an issue affecting only one DB instance, you can examine the Monitoring tab for that specific instance.

After the environment and the actual workload are set up to emulate your production application, you can measure how well Aurora performs. The most important questions to answer are as follows:
• How many queries per second is Aurora processing? You can examine the **Throughput** metrics to see the figures for various kinds of operations.

• How long does it take, on average for Aurora to process a given query? You can examine the **Latency** metrics to see the figures for various kinds of operations.

To do so, look at the **Monitoring** tab for a given Aurora cluster in the RDS console as illustrated following.

If you can, establish baseline values for these metrics in your current environment. If that’s not practical, construct a baseline on the Aurora cluster by executing a workload equivalent to your production application. For example, run your Aurora workload with a similar number of simultaneous users and queries. Then observe how the values change as you experiment with different instance classes, cluster size, configuration settings, and so on.

If the throughput numbers are lower than you expect, investigate further the factors affecting database performance for your workload. Similarly, if the latency numbers are higher than you expect, further investigate. To do so, monitor the secondary metrics for the DB server (CPU, memory, and so on). You can see whether the DB instances are close to their limits. You can also see how much extra capacity your DB instances have to handle more concurrent queries, queries against larger tables, and so on.

**Tip**

To detect metric values that fall outside the expected ranges, set up CloudWatch alarms.

When evaluating the ideal Aurora cluster size and capacity, you can find the configuration that achieves peak application performance without over-provisioning resources. One important factor is finding the appropriate size for the DB instances in the Aurora cluster. Start by selecting an instance size that has similar CPU and memory capacity to your current production environment. Collect throughput and latency numbers for the workload at that instance size. Then, scale the instance up to the next larger
size. See if the throughput and latency numbers improve. Also scale the instance size down, and see if the latency and throughput numbers remain the same. Your goal is to get the highest throughput, with the lowest latency, on the smallest instance possible.

**Tip**
Size your Aurora clusters and associated DB instances with enough existing capacity to handle sudden, unpredictable traffic spikes. For mission-critical databases, leave at least 20 percent spare CPU and memory capacity.

Run performance tests long enough to measure database performance in a warm, steady state. You might need to run the workload for many minutes or even a few hours before reaching this steady state. It's normal at the beginning of a run to have some variance. This variance happens because each Aurora Replica warms up its caches based on the `SELECT` queries that it handles.

Aurora performs best with transactional workloads involving multiple concurrent users and queries. To ensure that you're driving enough load for optimal performance, run benchmarks that use multithreading, or run multiple instances of the performance tests concurrently. Measure performance with hundreds or even thousands of concurrent client threads. Simulate the number of concurrent threads that you expect in your production environment. You might also perform additional stress tests with more threads to measure Aurora scalability.

### 12. Exercise Aurora high availability

Many of the main Aurora features involve high availability. These features include automatic replication, automatic failover, automatic backups with point-in-time restore, and ability to add DB instances to the cluster. The safety and reliability from features like these are important for mission-critical applications.

To evaluate these features requires a certain mindset. In earlier activities, such as performance measurement, you observe how the system performs when everything works correctly. Testing high availability requires you to think through worst-case behavior. You must consider various kinds of failures, even if such conditions are rare. You might intentionally introduce problems to make sure that the system recovers correctly and quickly.

**Tip**
For a proof of concept, set up all the DB instances in an Aurora cluster with the same AWS instance class. Doing so makes it possible to try out Aurora availability features without major changes to performance and scalability as you take DB instances offline to simulate failures.

We recommend using at least two instances in each Aurora cluster. The DB instances in an Aurora cluster can span up to three Availability Zones (AZs). Locate each of the first two or three DB instances in a different AZ. When you begin using larger clusters, spread your DB instances across all of the AZs in your AWS Region. Doing so increases fault tolerance capability. Even if a problem affects an entire AZ, Aurora can fail over to a DB instance in a different AZ. If you run a cluster with more than three instances, distribute the DB instances as evenly as you can over all three AZs.

**Tip**
The storage for an Aurora cluster is independent from the DB instances. The storage for each Aurora cluster always spans three AZs. When you test high availability features, always use DB instances with identical capacity in your test cluster. Doing so avoids unpredictable changes in performance, latency, and so on whenever one DB instance takes over for another.

To learn how to simulate failure conditions to test high availability features, see Testing Amazon Aurora using fault injection queries (p. 690).

As part of your proof-of-concept exercise, one objective is to find the ideal number of DB instances and the optimal instance class for those DB instances. Doing so requires balancing the requirements of high availability and performance.
For Aurora, the more DB instances that you have in a cluster, the greater the benefits for high availability. Having more DB instances also improves scalability of read-intensive applications. Aurora can distribute multiple connections for `SELECT` queries among the read-only Aurora Replicas.

On the other hand, limiting the number of DB instances reduces the replication traffic from the primary node. The replication traffic consumes network bandwidth, which is another aspect of overall performance and scalability. Thus, for write-intensive OLTP applications, prefer to have a smaller number of large DB instances rather than many small DB instances.

In a typical Aurora cluster, one DB instance (the primary instance) handles all the DDL and DML statements. The other DB instances (the Aurora Replicas) handle only `SELECT` statements. Although the DB instances don't do exactly the same amount of work, we recommend using the same instance class for all the DB instances in the cluster. That way, if a failure happens and Aurora promotes one of the read-only DB instances to be the new primary instance, the primary instance has the same capacity as before.

If you need to use DB instances of different capacities in the same cluster, set up failover tiers for the DB instances. These tiers determine the order in which Aurora Replicas are promoted by the failover mechanism. Put DB instances that are a lot larger or smaller than the others into a lower failover tier. Doing so ensures that they are chosen last for promotion.

Exercise the data recovery features of Aurora, such as automatic point-in-time restore, manual snapshots and restore, and cluster backtracking. If appropriate, copy snapshots to other AWS Regions and restore into other AWS Regions to mimic DR scenarios.

Investigate your organization's requirements for restore time objective (RTO), restore point objective (RPO), and geographic redundancy. Most organizations group these items under the broad category of disaster recovery. Evaluate the Aurora high availability features described in this section in the context of your disaster recovery process to ensure that your RTO and RPO requirements are met.

### 13. What to do next

At the end of a successful proof-of-concept process, you confirm that Aurora is a suitable solution for you based on the anticipated workload. Throughout the preceding process, you've checked how Aurora works in a realistic operational environment and measured it against your success criteria.

After you get your database environment up and running with Aurora, you can move on to more detailed evaluation steps, leading to your final migration and production deployment. Depending on your situation, these other steps might or might not be included in the proof-of-concept process. For details about migration and porting activities, see the AWS whitepaper [Aurora migration handbook](https://aws.amazon.com/aurora/migration-handbook).

In another next step, consider the security configurations relevant for your workload and designed to meet your security requirements in a production environment. Plan what controls to put in place to protect access to the Aurora cluster master user credentials. Define the roles and responsibilities of database users to control access to data stored in the Aurora cluster. Take into account database access requirements for applications, scripts, and third-party tools or services. Explore AWS services and features such as AWS Secrets Manager and AWS Identity and Access Management (IAM) authentication.

At this point, you should understand the procedures and best practices for running benchmark tests with Aurora. You might find you need to do additional performance tuning. For details, see Managing performance and scaling for Aurora DB clusters (p. 349), Amazon Aurora MySQL performance enhancements (p. 634), Managing Amazon Aurora PostgreSQL (p. 1028), and Using Amazon RDS Performance Insights (p. 514). If you do additional tuning, make sure that you're familiar with the metrics that you gathered during the proof of concept. For a next step, you might create new clusters with different choices for configuration settings, database engine, and database version. Or you might create specialized kinds of Aurora clusters to match the needs of specific use cases.
For example, you can explore Aurora parallel query clusters for hybrid transaction/analytical processing (HTAP) applications. If wide geographic distribution is crucial for disaster recovery or to minimize latency, you can explore Aurora global databases. If your workload is intermittent or you're using Aurora in a development/test scenario, you can explore Aurora Serverless clusters.

Your production clusters might also need to handle high volumes of incoming connections. To learn those techniques, see the AWS whitepaper Aurora MySQL database administrator’s handbook – Connection management.

If, after the proof of concept, you decide that your use case is not suited for Aurora, consider these other AWS services:

- For purely analytic use cases, workloads benefit from a columnar storage format and other features more suitable to OLAP workloads. AWS services that address such use cases include the following:
  - Amazon Redshift
  - Amazon EMR
  - Amazon Athena
- Many workloads benefit from a combination of Aurora with one or more of these services. You can move data between these services by using these:
  - AWS Glue
  - AWS DMS
  - Importing from Amazon S3, as described in the Amazon Aurora User Guide
  - Exporting to Amazon S3, as described in the Amazon Aurora User Guide
  - Many other popular ETL tools
Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs. To learn about the compliance programs that apply to Amazon Aurora (Aurora), see AWS services in scope by compliance program.

- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your organization's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon Aurora. The following topics show you how to configure Amazon Aurora to meet your security and compliance objectives. You also learn how to use other AWS services that help you monitor and secure your Amazon Aurora resources.

You can manage access to your Amazon Aurora resources and your databases on a DB cluster. The method you use to manage access depends on what type of task the user needs to perform with Amazon Aurora:

- Run your DB cluster in a virtual private cloud (VPC) based on the Amazon VPC service for the greatest possible network access control. For more information about creating a DB cluster in a VPC, see Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281).

- Use AWS Identity and Access Management (IAM) policies to assign permissions that determine who is allowed to manage Amazon Aurora resources. For example, you can use IAM to determine who is allowed to create, describe, modify, and delete DB clusters, tag resources, or modify security groups. For information on setting up an IAM user, see Create an IAM user (p. 73).

- Use security groups to control what IP addresses or Amazon EC2 instances can connect to your databases on a DB cluster. When you first create a DB cluster, its firewall prevents any database access except through rules specified by an associated security group.

- Use Secure Socket Layer (SSL) or Transport Layer Security (TLS) connections with DB clusters running the Aurora MySQL or Aurora PostgreSQL. For more information on using SSL/TLS with a DB cluster, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).

- Use Amazon Aurora encryption to secure your DB clusters and snapshots at rest. Amazon Aurora encryption uses the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your DB cluster. For more information, see Encrypting Amazon Aurora resources (p. 1208).

- Use the security features of your DB engine to control who can log in to the databases on a DB cluster. These features work just as if the database was on your local network.

For information about security with Aurora MySQL, see Security with Amazon Aurora MySQL (p. 637). For information about security with Aurora PostgreSQL, see Security with Amazon Aurora PostgreSQL (p. 997).
Aurora is part of the managed database service Amazon Relational Database Service (Amazon RDS). Amazon RDS is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. If you are not already familiar with Amazon RDS, see the Amazon RDS user guide.

Aurora includes a high-performance storage subsystem. Its MySQL- and PostgreSQL-compatible database engines are customized to take advantage of that fast distributed storage. Aurora also automates and standardizes database clustering and replication, which are typically among the most challenging aspects of database configuration and administration.

For both Amazon RDS and Aurora, you can access the RDS API programmatically, and you can use the AWS CLI to access the RDS API interactively. Some RDS API operations and AWS CLI commands apply to both Amazon RDS and Aurora, while others apply to either Amazon RDS or Aurora. For information about RDS API operations, see Amazon RDS API reference. For more information about the AWS CLI, see AWS Command Line Interface reference for Amazon RDS.

Note
You only have to configure security for your use cases. You don't have to configure security access for processes that Amazon Aurora manages. These include creating backups, replicating data between a primary DB instance and a read replica, and other processes.

For more information on managing access to Amazon Aurora resources and your databases on a DB cluster, see the following topics.

Topics
- Database authentication with Amazon Aurora (p. 1206)
- Data protection in Amazon RDS (p. 1207)
- Identity and access management in Amazon Aurora (p. 1222)
- Logging and monitoring in Amazon Aurora (p. 1264)
- Compliance validation for Amazon Aurora (p. 1267)
- Resilience in Amazon Aurora (p. 1268)
- Infrastructure security in Amazon Aurora (p. 1270)
- Amazon Aurora and interface VPC endpoints (AWS PrivateLink) (p. 1271)
- Security best practices for Amazon Aurora (p. 1273)
- Controlling access with security groups (p. 1274)
- Master user account privileges (p. 1276)
- Using service-linked roles for Amazon Aurora (p. 1277)
- Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281)

Database authentication with Amazon Aurora

Amazon Aurora supports several ways to authenticate database users.

Topics
- Password authentication (p. 1206)
- IAM database authentication (p. 1207)
- Kerberos authentication (p. 1207)

Password authentication

With password authentication, your DB instance performs all administration of user accounts. You create users with SQL statements such as CREATE USER and specify passwords in the IDENTIFIED BY clause.
All RDS DB engines support password authentication. For more information about password authentication, see the documentation for your DB engine.

With password authentication, your database controls and authenticates user accounts. If a DB engine has strong password management features, they can enhance security. Database authentication might be easier to administer using password authentication when you have small user communities. Because clear text passwords are generated in this case, integrating with AWS Secrets Manager can enhance security.

For information about using Secrets Manager with Amazon Aurora, see Creating a basic secret and Rotating secrets for supported Amazon RDS databases in the AWS Secrets Manager User Guide. For information about programmatically retrieving your secrets in your custom applications, see Retrieving the secret value in the AWS Secrets Manager User Guide.

IAM database authentication

You can authenticate to your DB cluster using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with Aurora MySQL and Aurora PostgreSQL. With this authentication method, you don't need to use a password when you connect to a DB cluster. Instead, you use an authentication token.

For more information about IAM database authentication, including information about availability for specific DB engines, see IAM database authentication (p. 1238).

Kerberos authentication

Amazon Aurora supports external authentication of database users using Kerberos and Microsoft Active Directory. Kerberos is a network authentication protocol that uses tickets and symmetric-key cryptography to eliminate the need to transmit passwords over the network. Kerberos has been built into Active Directory and is designed to authenticate users to network resources, such as databases.

Amazon Aurora support for Kerberos and Active Directory provides the benefits of single sign-on and centralized authentication of database users. You can keep your user credentials in Active Directory. Active Directory provides a centralized place for storing and managing credentials for multiple DB instances.

You can enable your database users to authenticate against DB instances in two ways. They can use credentials stored either in AWS Directory Service for Microsoft Active Directory or in your on-premises Active Directory.

Currently, Aurora supports Kerberos authentication for Aurora PostgreSQL DB clusters. With Kerberos authentication, Aurora PostgreSQL DB clusters support one- and two-way forest trust relationships. For more information, see Using Kerberos authentication with Aurora PostgreSQL (p. 1124).

Data protection in Amazon RDS

The AWS shared responsibility model applies to data protection in Amazon Relational Database Service. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given
only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put sensitive identifying information, such as your customers' account numbers, into free-form fields such as a Name field. This includes when you work with Amazon RDS or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into Amazon RDS or other services might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

Topics
- Protecting data using encryption (p. 1208)
- Internetwork traffic privacy (p. 1221)

Protecting data using encryption

You can enable encryption for database resources. You can also encrypt connections to DB clusters.

Topics
- Encrypting Amazon Aurora resources (p. 1208)
- Customer master key (CMK) management (p. 1210)
- Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211)
- Rotating your SSL/TLS certificate (p. 1213)

Encrypting Amazon Aurora resources

Amazon Aurora can encrypt your Amazon Aurora DB clusters. Data that is encrypted at rest includes the underlying storage for DB clusters, its automated backups, read replicas, and snapshots.

Amazon Aurora encrypted DB clusters use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon Aurora DB clusters. After your data is encrypted, Amazon Aurora handles authentication of access and decryption of your data transparently with a minimal impact on performance. You don't need to modify your database client applications to use encryption.

Note
For encrypted and unencrypted DB clusters, data that is in transit between the source and the read replicas is encrypted, even when replicating across AWS Regions.

Topics
- Overview of encrypting Amazon Aurora resources (p. 1209)
- Enabling encryption for an Amazon Aurora DB cluster (p. 1209)
Data encryption

- Availability of Amazon Aurora encryption (p. 1210)
- Limitations of Amazon Aurora encrypted DB clusters (p. 1210)

Overview of encrypting Amazon Aurora resources

Amazon Aurora encrypted DB clusters provide an additional layer of data protection by securing your data from unauthorized access to the underlying storage. You can use Amazon Aurora encryption to increase data protection of your applications deployed in the cloud, and to fulfill compliance requirements for encryption at rest.

For an Amazon Aurora encrypted DB cluster, all DB instances, logs, backups, and snapshots are encrypted. You can also encrypt a read replica of an Amazon Aurora encrypted cluster. Amazon Aurora uses an AWS KMS customer master key (CMK) to encrypt these resources. For more information about CMKs, see Customer master keys (CMKs) in the AWS Key Management Service Developer Guide. Each DB instance in the DB cluster is encrypted using the same CMK as the DB cluster. If you copy an encrypted snapshot, you can use a different CMK to encrypt the target snapshot than the one that was used to encrypt the source snapshot.

You can use an AWS managed CMK, or you can create customer managed CMKs. To manage the CMKs used for encrypting and decrypting your Amazon Aurora resources, you use the AWS Key Management Service (AWS KMS). AWS KMS combines secure, highly available hardware and software to provide a key management system scaled for the cloud. Using AWS KMS, you can create CMKs and define the policies that control how these CMKs can be used. AWS KMS supports CloudTrail, so you can audit CMK usage to verify that CMKs are being used appropriately. You can use your AWS KMS CMKs with Amazon Aurora and supported AWS services such as Amazon S3, Amazon EBS, and Amazon Redshift. For a list of services that are integrated with AWS KMS, see AWS Service Integration.

Enabling encryption for an Amazon Aurora DB cluster

To enable encryption for a new DB cluster, choose Enable encryption on the console. For information on creating a DB cluster, see Creating an Amazon Aurora DB cluster (p. 118).

If you use the create-db-cluster AWS CLI command to create an encrypted DB cluster, set the --storage-encrypted parameter. If you use the CreateDBCluster API operation, set the StorageEncrypted parameter to true.

When you create an encrypted DB cluster, you can choose a customer managed CMK or the AWS managed CMK for Amazon Aurora to encrypt your DB cluster. If you don’t specify the key identifier for a customer managed CMK, Amazon Aurora uses the AWS managed CMK for your new DB cluster. Amazon Aurora creates an AWS managed CMK for Amazon Aurora for your AWS account. Your AWS account has a different AWS managed CMK for Amazon Aurora for each AWS Region.

Once you have created an encrypted DB cluster, you can’t change the CMK used by that DB cluster. Therefore, be sure to determine your CMK requirements before you create your encrypted DB cluster.

If you use the AWS CLI create-db-cluster command to create an encrypted DB cluster with a customer managed CMK, set the --kms-key-id parameter to any key identifier for the CMK. If you use the Amazon RDS API CreateDBInstance operation, set the KmsKeyId parameter to any key identifier for the CMK. To use a customer managed CMK in a different AWS account, specify the key ARN or alias ARN.

Important

In some cases, Amazon Aurora can lose access to the CMK for a DB cluster. For example, Aurora loses access when RDS access to a CMK is revoked. In these cases, the encrypted DB cluster goes into a terminal state, and you can only restore the DB cluster from a backup. We strongly recommend that you always enable backups for encrypted DB clusters to guard against the loss of encrypted data in your databases.
Availability of Amazon Aurora encryption

Amazon Aurora encryption is currently available for all database engines and storage types.

**Note**
Amazon Aurora encryption is not available for the db.t2.micro DB instance class.

Limitations of Amazon Aurora encrypted DB clusters

The following limitations exist for Amazon Aurora encrypted DB clusters:

- You can’t disable encryption on an encrypted DB cluster.
- You can’t create an encrypted snapshot of an unencrypted DB cluster.
- A snapshot of an encrypted DB cluster must be encrypted using the same CMK as the DB cluster.
- You can’t convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted snapshot to an encrypted Aurora DB cluster. To do this, specify a CMK when you restore from the unencrypted snapshot.
- You can’t create an encrypted Aurora Replica from an unencrypted Aurora DB cluster. You can’t create an unencrypted Aurora Replica from an encrypted Aurora DB cluster.
- To copy an encrypted snapshot from one AWS Region to another, you must specify the CMK in the destination AWS Region. This is because CMKs are specific to the AWS Region that they are created in. The source snapshot remains encrypted throughout the copy process. Amazon Aurora uses envelope encryption to protect data during the copy process. For more information about envelope encryption, see [Envelope encryption](#) in the *AWS Key Management Service Developer Guide*.
- You can’t unencrypt an encrypted DB cluster. However, you can export data from an encrypted DB cluster and import the data into an unencrypted DB cluster.

Customer master key (CMK) management

Amazon Aurora automatically integrates with AWS Key Management Service (AWS KMS) for key management. Amazon Aurora uses envelope encryption. For more information about envelope encryption, see [Envelope encryption](#) in the *AWS Key Management Service Developer Guide*.

A customer master key (CMK) is a logical representation of a master key. The CMK includes metadata, such as the key ID, creation date, description, and key state. The CMK also contains the key material used to encrypt and decrypt data. For more information about customer managed CMKs, see [Customer managed CMKs](#) in the *AWS Key Management Service Developer Guide*.

You can manage CMKs used for Amazon Aurora encrypted DB clusters using the AWS Key Management Service (AWS KMS) in the AWS KMS console, the AWS CLI, or the AWS KMS API. If you want full control over a CMK, then you must create a customer managed CMK.

AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. You can’t delete, edit, or rotate AWS managed CMKs. For more information about AWS managed CMKs, see [AWS managed CMKs](#) in the *AWS Key Management Service Developer Guide*.

You can’t share a snapshot that has been encrypted using the AWS managed CMK of the AWS account that shared the snapshot.

You can view audit logs of every action taken with an AWS managed or customer managed CMK by using [AWS CloudTrail](#).

**Important**
When Aurora encounters a DB cluster encrypted by a CMK that Aurora doesn’t have access to, Aurora puts the DB cluster into a terminal state. In this state, the DB cluster is no longer
available and the current state of the database can't be recovered. To restore the DB cluster, you must re-enable access to the CMK for Aurora, and then restore the DB cluster from a backup.

**Authorizing use of the CMK**

When Aurora uses a CMK in cryptographic operations, it acts on behalf of the user who is creating or changing the Aurora resource.

To use the customer managed CMK for an Aurora resource on your behalf, a user must have permissions to call the following operations on the CMK:

- kms:GenerateDataKey
- kms:Decrypt

You can specify these required permissions in a key policy, or in an IAM policy if the key policy allows it.

You can make the IAM policy stricter in various ways. For example, to allow the CMK to be used only for requests that originate in Aurora, you can use the `kms:ViaService` condition key with the `rds.<region>.amazonaws.com` value.

You can also use the keys or values in the encryption context as a condition for using the CMK for cryptographic operations.

**Using SSL/TLS to encrypt a connection to a DB cluster**

You can use Secure Socket Layer (SSL) or Transport Layer Security (TLS) from your application to encrypt a connection to a DB cluster running Aurora MySQL or Aurora PostgreSQL. Each DB engine has its own process for implementing SSL/TLS. To learn how to implement SSL/TLS for your DB cluster, use the link following that corresponds to your DB engine:

- Security with Amazon Aurora MySQL (p. 637)
- Security with Amazon Aurora PostgreSQL (p. 997)

**Important**
For information about rotating your certificate, see Rotating your SSL/TLS certificate (p. 1213).

**Note**
All certificates are only available for download using SSL/TLS connections.


This root certificate is a trusted root entity and should work in most cases but might fail if your application doesn't accept certificate chains. If your application doesn't accept certificate chains, download the AWS Region-specific certificate from the list of intermediate certificates found later in this section.

To get a certificate bundle that contains both the intermediate and root certificates, download from https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem.

If your application is on Microsoft Windows and requires a PKCS7 file, you can download the PKCS7 certificate bundle. This bundle contains both the intermediate and root certificates at https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.p7b.

**Note**
Amazon RDS Proxy and Aurora Serverless use certificates from the AWS Certificate Manager (ACM). If you are using RDS Proxy, you don't need to download Amazon RDS certificates or update applications that use RDS Proxy connections. For more information about using TLS/SSL with RDS Proxy, see Using TLS/SSL with RDS Proxy (p. 262).
If you are Aurora Serverless, downloading Amazon RDS certificates isn't required. For more information about using TLS/SSL with Aurora Serverless, see Using TLS/SSL with Aurora Serverless v1 (p. 137).

Root certificates for opt-in AWS Regions

If you are using an opt-in AWS Region, you can download the root certificate from the following table.

<table>
<thead>
<tr>
<th>Opt-in AWS Region</th>
<th>Root certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa (Cape Town)</td>
<td>rds-ca-af-south-1-2019-root.pem</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>rds-ca-ap-east-1-2019-root.pem</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>rds-ca-eu-south-1-2019-root.pem</td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td>rds-ca-me-south-1-2019-root.pem</td>
</tr>
</tbody>
</table>

Intermediate certificates

You might need to use an intermediate certificate to connect to your AWS Region. For example, you must use an intermediate certificate to connect to the AWS GovCloud (US-West) Region using SSL/TLS. If you need an intermediate certificate for a particular AWS Region, download the certificate from the following table.

<table>
<thead>
<tr>
<th>AWS Region</th>
<th>Intermediate certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>rds-ca-2019-ap-south-1.pem</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>rds-ca-2019-ap-northeast-1.pem</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>rds-ca-2019-ap-northeast-2.pem</td>
</tr>
<tr>
<td>Asia Pacific (Osaka-Local)</td>
<td>rds-ca-2019-ap-northeast-3.pem</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>rds-ca-2019-ap-southeast-1.pem</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>rds-ca-2019-ca-central-1.pem</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>rds-ca-2019-eu-central-1.pem</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>rds-ca-2019-eu-west-1.pem</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>rds-ca-2019-eu-west-2.pem</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>rds-ca-2019-eu-west-3.pem</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>rds-ca-2019-eu-north-1.pem</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>rds-ca-2019-sa-east-1.pem</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>rds-ca-2019-us-east-1.pem</td>
</tr>
<tr>
<td>US East (Ohio)</td>
<td>rds-ca-2019-us-east-2.pem</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>rds-ca-2019-us-west-1.pem</td>
</tr>
</tbody>
</table>
AWS Region | Intermediate certificate
---|---
US West (Oregon) | rds-ca-2019-us-west-2.pem

**AWS GovCloud (US) certificates**

You can download the root certificate for an AWS GovCloud (US) Region from the following list:

- **AWS GovCloud (US-East)** (Root CA-2017)
- **AWS GovCloud (US-West)** (Root CA-2017)

You can download the intermediate certificate for an AWS GovCloud (US) Region from the following list:

- **AWS GovCloud (US-East)** (CA-2017)
- **AWS GovCloud (US-West)** (CA-2017)
- **AWS GovCloud (US-West)** (CA-2012)


**Rotating your SSL/TLS certificate**

As of March 5, 2020, Amazon RDS CA-2015 certificates have expired. If you use or plan to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) with certificate verification to connect to your RDS DB instances, you require Amazon RDS CA-2019 certificates, which are enabled by default for new DB instances. If you currently do not use SSL/TLS with certificate verification, you might still have expired CA-2015 certificates and must update them to CA-2019 certificates if you plan to use SSL/TLS with certificate verification to connect to your RDS databases.

Follow these instructions to complete your updates. Before you update your DB instances to use the new CA certificate, make sure that you update your clients or applications connecting to your RDS databases.

Amazon RDS provides new CA certificates as an AWS security best practice. For information about the new certificates and the supported AWS Regions, see [Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211)](https://docs.aws.amazon.com/aurora/latest/userguide/using-ssl-tls.html).

**Note**

Amazon RDS Proxy and Aurora Serverless use certificates from the AWS Certificate Manager (ACM). If you are using RDS Proxy, when you rotate your SSL/TLS certificate, you don't need to update applications that use RDS Proxy connections. For more information about using SSL/SSL with RDS Proxy, see [Using TLS/SSL with RDS Proxy (p. 262)](https://docs.aws.amazon.com/aurora/latest/userguide/using-ssl-tls.html).

If you are Aurora Serverless, rotating your SSL/TLS certificate isn't required. For more information about using TLS/SSL with Aurora Serverless, see [Using TLS/SSL with Aurora Serverless v1 (p. 137)](https://docs.aws.amazon.com/aurora/latest/userguide/using-ssl-tls.html).

**Note**

If you are using a Go version 1.15 application with a DB instance that was created or updated to the *rds-ca-2019* certificate prior to July 28, 2020, you must update the certificate again. Run the `modify-db-instance` command shown in the AWS CLI section using *rds-ca-2019* as the CA certificate identifier. In this case, it isn't possible to update the certificate using the AWS Management Console. If you created your DB instance or updated its certificate after July 28, 2020, no action is required. For more information, see [Go GitHub issue #39568](https://github.com/aws/aws-encryption-support/issues/39568).

**Topics**

- [Updating your CA certificate by modifying your DB instance (p. 1214)](https://docs.aws.amazon.com/aurora/latest/userguide/using-ssl-tls.html)
Updating your CA certificate by modifying your DB instance

Complete the following steps to update your CA certificate.

**To update your CA certificate by modifying your DB instance**

1. Download the new SSL/TLS certificate as described in Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).
2. Update your applications to use the new SSL/TLS certificate.
   
   The methods for updating applications for new SSL/TLS certificates depend on your specific applications. Work with your application developers to update the SSL/TLS certificates for your applications.
   
   For information about checking for SSL/TLS connections and updating applications for each DB engine, see the following topics:
   
   - Updating applications to connect to Aurora MySQL DB clusters using new SSL/TLS certificates (p. 640)
   - Updating applications to connect to Aurora PostgreSQL DB clusters using new SSL/TLS certificates (p. 1001)
   
   For a sample script that updates a trust store for a Linux operating system, see Sample script for importing certificates into your trust store (p. 1220).

   **Note**
   
   The certificate bundle contains certificates for both the old and new CA, so you can upgrade your application safely and maintain connectivity during the transition period. If you are using the AWS Database Migration Service to migrate a database to a DB cluster, we recommend using the certificate bundle to ensure connectivity during the migration.
   
3. Modify the DB instance to change the CA from rds-ca-2015 to rds-ca-2019.

   **Important**
   
   By default, this operation restarts your DB instance. If you don't want to restart your DB instance during this operation, you can use the `modify-db-instance` CLI command and specify the `--no-certificate-rotation-restart` option.
   
   This option will not rotate the certificate until the next time the database restarts, either for planned or unplanned maintenance. This option is only recommended if you don't use SSL/TLS.
   
   If you are experiencing connectivity issues after certificate expiry, use the apply immediately option by specifying `Apply immediately` in the console or by specifying the `--apply-immediately` option using the AWS CLI. By default, this operation is scheduled to run during your next maintenance window.

You can use the AWS Management Console or the AWS CLI to change the CA certificate from rds-ca-2015 to rds-ca-2019 for a DB instance.

**Console**

**To change the CA from rds-ca-2015 to rds-ca-2019 for a DB instance**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.

3. Choose **Modify**.

   ![Modify DB Instance page](image)

   The **Modify DB Instance** page appears.

4. In the **Network & Security** section, choose **rds-ca-2019**.

   ![Certificate authority](image)

   EC2 instances and devices outside of the VPC hosting the DB instance will connect to the DB instances. You can have more VPC security groups that specify which EC2 instances and devices can connect to the DB instance.

5. Choose **Continue** and check the summary of modifications.

6. To apply the changes immediately, choose **Apply immediately**.

   **Important**
   Choosing this option restarts your database immediately.

7. On the confirmation page, review your changes. If they are correct, choose **Modify DB Instance** to save your changes.

   **Important**
   When you schedule this operation, make sure that you have updated your client-side trust store beforehand.

   Or choose **Back** to edit your changes or **Cancel** to cancel your changes.
AWS CLI

To use the AWS CLI to change the CA from rds-ca-2015 to rds-ca-2019 for a DB instance, call the modify-db-instance command. Specify the DB instance identifier and the --ca-certificate-identifier option.

Important
When you schedule this operation, make sure that you have updated your client-side trust store beforehand.

Example

The following code modifies mydbinstance by setting the CA certificate to rds-ca-2019. The changes are applied during the next maintenance window by using --no-apply-immediately. Use --apply-immediately to apply the changes immediately.

Important
By default, this operation reboots your DB instance. If you don't want to reboot your DB instance during this operation, you can use the modify-db-instance CLI command and specify the --no-certificate-rotation-restart option.
This option will not rotate the certificate until the next time the database restarts, either for planned or unplanned maintenance. This option is only recommended if you do not use SSL/TLS.
Use --apply-immediately to apply the update immediately. By default, this operation is scheduled to run during your next maintenance window.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
   --db-instance-identifier mydbinstance \
   --ca-certificate-identifier rds-ca-2019 \
   --no-apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
   --db-instance-identifier mydbinstance ^
   --ca-certificate-identifier rds-ca-2019 ^
   --no-apply-immediately
```

Updating your CA certificate by applying DB instance maintenance

Complete the following steps to update your CA certificate by applying DB instance maintenance.

To update your CA certificate by applying DB instance maintenance

1. Download the new SSL/TLS certificate as described in Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).

2. Update your database applications to use the new SSL/TLS certificate.

   The methods for updating applications for new SSL/TLS certificates depend on your specific applications. Work with your application developers to update the SSL/TLS certificates for your applications.

   For information about checking for SSL/TLS connections and updating applications for each DB engine, see the following topics:
• Updating applications to connect to Aurora MySQL DB clusters using new SSL/TLS certificates (p. 640)
• Updating applications to connect to Aurora PostgreSQL DB clusters using new SSL/TLS certificates (p. 1001)

For a sample script that updates a trust store for a Linux operating system, see Sample script for importing certificates into your trust store (p. 1220).

Note
The certificate bundle contains certificates for both the old and new CA, so you can upgrade your application safely and maintain connectivity during the transition period.

3. Apply DB instance maintenance to change the CA from rds-ca-2015 to rds-ca-2019.

Important
You can choose to apply the change immediately. By default, this operation is scheduled to run during your next maintenance window.

You can use the AWS Management Console to apply DB instance maintenance to change the CA certificate from rds-ca-2015 to rds-ca-2019 for multiple DB instances.

Updating your CA certificate by applying maintenance to multiple DB instances

Use the AWS Management Console to change the CA certificate for multiple DB instances.

To change the CA from rds-ca-2015 to rds-ca-2019 for multiple DB instances

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose Databases.
   In the navigation pane, there is a Certificate update option that shows the total number of affected DB instances.
Choose **Certificate update** in the navigation pane.

The **Update your Amazon RDS SSL/TLS certificates** page appears.
Note
This page only shows the DB instances for the current AWS Region. If you have DB instances in more than one AWS Region, check this page in each AWS Region to see all DB instances with old SSL/TLS certificates.

3. Choose the DB instance you want to update.

You can schedule the certificate rotation for your next maintenance window by choosing Update at the next maintenance window. Apply the rotation immediately by choosing Update now.

Important
When your CA certificate is rotated, the operation restarts your DB instance.
If you experience connectivity issues after certificate expiry, use the Update now option.

4. If you choose Update at the next maintenance window or Update now, you are prompted to confirm the CA certificate rotation.

Important
Before scheduling the CA certificate rotation on your database, update any client applications that use SSL/TLS and the server certificate to connect. These updates are specific to your DB engine. To determine whether your applications use SSL/TLS and the server certificate to connect, see Step 2: Update Your Database Applications to Use the New SSL/TLS Certificate (p. 1216). After you have updated these client applications, you can confirm the CA certificate rotation.

To continue, choose the check box, and then choose Confirm.

5. Repeat steps 3 and 4 for each DB instance that you want to update.
Sample script for importing certificates into your trust store

The following are sample shell scripts that import the certificate bundle into a trust store.

Topics
- Sample script for importing certificates on Linux (p. 1220)
- Sample script for importing certificates on macOS (p. 1220)

Sample script for importing certificates on Linux

The following is a sample shell script that imports the certificate bundle into a trust store on a Linux operating system.

```bash
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
  mkdir -p "${mydir}"
fi

truststore=${mydir}/rds-truststore.jks
storepassword=changeit
awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/ {split_after=1}{print > "rds-ca-" n ".pem"} < ${mydir}/rds-combined-ca-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}/rds-combined-ca-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: (.*?)/) { print "$1"; }'`
  echo " Certificate ${alias} expires in '${expiry}'"
done
```

Sample script for importing certificates on macOS

The following is a sample shell script that imports the certificate bundle into a trust store on macOS.

```bash
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
  mkdir -p "${mydir}"
fi
```
Internetwork traffic privacy

Connections are protected both between Amazon Aurora and on-premises applications and between Amazon Aurora and other AWS resources within the same AWS Region.

Traffic between service and on-premises clients and applications

You have two connectivity options between your private network and AWS:

- An AWS Site-to-Site VPN connection. For more information, see What is AWS Site-to-Site VPN?
- An AWS Direct Connect connection. For more information, see What is AWS Direct Connect?

You get access to Amazon Aurora through the network by using AWS-published API operations. Clients must support Transport Layer Security (TLS) 1.0. We recommend TLS 1.2. Clients must also support cipher suites with Perfect Forward Secrecy (PFS), such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Most modern systems such as Java 7 and later support these modes. Additionally, you must sign requests using an access key identifier and a secret access key that are associated with an IAM principal. Or you can use the AWS security token service (STS) to generate temporary security credentials to sign requests.
Identity and access management in Amazon Aurora

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use Aurora resources. IAM is an AWS service that you can use with no additional charge.

Topics
- Audience (p. 1222)
- Authenticating with identities (p. 1222)
- Managing access using policies (p. 1224)
- How Amazon Aurora works with IAM (p. 1225)
- Amazon Aurora identity-based policy examples (p. 1228)
- IAM database authentication (p. 1238)
- Troubleshooting Amazon Aurora identity and access (p. 1263)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work you do in Aurora.

Service user – If you use the Aurora service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Aurora features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Aurora, see Troubleshooting Amazon Aurora identity and access (p. 1263).

Service administrator – If you’re in charge of Aurora resources at your company, you probably have full access to Aurora. It’s your job to determine which Aurora features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Aurora, see How Amazon Aurora works with IAM (p. 1225).

IAM administrator – If you’re an IAM administrator, you might want to learn details about how you can write policies to manage access to Aurora. To view example Aurora identity-based policies that you can use in IAM, see Amazon Aurora identity-based policy examples (p. 1228).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see The IAM console and sign-in page in the IAM User Guide.

You must be authenticated (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company’s single sign-on authentication, or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email or your IAM user name. You can access AWS programmatically using your root user or IAM user access keys. AWS
provides SDK and command line tools to cryptographically sign your request using your credentials. If you don’t use AWS tools, you must sign the request yourself. Do this using Signature Version 4, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 signing process in the AWS General Reference.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Using multi-factor authentication (MFA) in AWS in the IAM User Guide.

**AWS account root user**

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

**IAM users and groups**

An IAM user is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing access keys for IAM users in the IAM User Guide. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

An IAM group is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named IAMAdmins and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the IAM User Guide.

You can authenticate to your DB cluster using IAM database authentication.

IAM database authentication works with Aurora. For more information about authenticating to your DB cluster using IAM, see IAM database authentication (p. 1238).

**IAM roles**

An IAM role is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the IAM User Guide.

IAM roles with temporary credentials are useful in the following situations:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as
Managing access using policies

You control access in AWS by creating policies and attaching them to IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an entity (root user, IAM user, or IAM role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the IAM User Guide.

An IAM administrator can use policies to specify who has access to AWS resources, and what actions they can perform on those resources. Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

**Identity-based policies**

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, role, or group. These policies control what actions that identity can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the IAM User Guide.

Identity-based policies can be further categorized as inline policies or managed policies. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing between managed policies and inline policies in the IAM User Guide.
The following AWS managed policies, which you can attach to users in your account, are specific to Amazon Aurora:

- **AmazonRDSReadOnlyAccess** – Grants read-only access to all Amazon Aurora resources for the AWS account specified.
- **AmazonRDSFullAccess** – Grants full access to all Amazon Aurora resources for the AWS account specified.

### Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the IAM User Guide.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the AWS Organizations User Guide.

- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the IAM User Guide.

### Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the IAM User Guide.

For more information about identity and access management for Aurora, continue to the following pages:

- How Amazon Aurora works with IAM (p. 1225)
- Troubleshooting Amazon Aurora identity and access (p. 1263)

### How Amazon Aurora works with IAM

Before you use IAM to manage access to Aurora, you should understand what IAM features are available to use with Aurora. To get a high-level view of how Aurora and other AWS services work with IAM, see AWS services that work with IAM in the IAM User Guide.

**Topics**

- Aurora identity-based policies (p. 1226)
Aurora identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. Aurora supports specific actions, resources, and condition keys. To learn about all of the elements that you use in a JSON policy, see IAM JSON policy elements reference in the IAM User Guide.

Actions

The **Action** element of an IAM identity-based policy describes the specific action or actions that will be allowed or denied by the policy. Policy actions usually have the same name as the associated AWS API operation. The action is used in a policy to grant permissions to perform the associated operation.

Policy actions in Aurora use the following prefix before the action: `rds:`. For example, to grant someone permission to describe DB instances with the Amazon RDS `DescribeDBInstances` API operation, you include the `rds:DescribeDBInstances` action in their policy. Policy statements must include either an **Action** or **NotAction** element. Aurora defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows:

```
"Action": [n
    "rds:action1",
    "rds:action2"
]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action:

```
"Action": "rds:Describe*"
```

To see a list of Aurora actions, see Actions Defined by Amazon RDS in the Service Authorization Reference.

Resources

The **Resource** element specifies the object or objects to which the action applies. Statements must include either a **Resource** or a **NotResource** element. You specify a resource using an ARN or using the wildcard (*) to indicate that the statement applies to all resources.

The DB instance resource has the following ARN:

```
arn:{Partition}:rds:{Region}:{Account}:{ResourceType}/{Resource}
```

For more information about the format of ARNs, see Amazon Resource Names (ARNs) and AWS service namespaces.

For example, to specify the `dbtest` DB instance in your statement, use the following ARN:

```
```

To specify all DB instances that belong to a specific account, use the wildcard (*):
Some RDS API operations, such as those for creating resources, cannot be performed on a specific resource. In those cases, you must use the wildcard (*)

```json
"Resource": "*"
```

Many Amazon RDS API operations involve multiple resources. For example, `CreateDBInstance` creates a DB instance. You can specify that an IAM user must use a specific security group and parameter group when creating a DB instance. To specify multiple resources in a single statement, separate the ARNs with commas.

```json
"Resource": [  "resource1",  "resource2"
]
```

To see a list of Aurora resource types and their ARNs, see Resources Defined by Amazon RDS in the Service Authorization Reference. To learn with which actions you can specify the ARN of each resource, see Actions Defined by Amazon RDS.

### Condition keys

The `Condition` element (or `Condition block`) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can build conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical AND operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical OR operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: Variables and tags in the IAM User Guide.

Aurora defines its own set of condition keys and also supports using some global condition keys. To see all AWS global condition keys, see AWS global condition context keys in the IAM User Guide.

All RDS API operations support the `aws:RequestedRegion` condition key.

To see a list of Aurora condition keys, see Condition Keys for Amazon RDS in the Service Authorization Reference. To learn with which actions and resources you can use a condition key, see Actions Defined by Amazon RDS.

### Examples

To view examples of Aurora identity-based policies, see Amazon Aurora identity-based policy examples (p. 1228).

### Aurora resource-based policies

Aurora does not support resource-based policies.

### Authorization based on Aurora tags

You can attach tags to Aurora resources or pass tags in a request to Aurora. To control access based on tags, you provide tag information in the condition element of a policy using the
rds:ResourceTag/*key-name*, aws:RequestTag/*key-name*, or aws:TagKeys condition keys. For more information about tagging Aurora resources, see Specifying conditions: Using custom tags (p. 1235).

To view an example identity-based policy for limiting access to a resource based on the tags on that resource, see Grant permission for actions on a resource with a specific tag with two different values (p. 1232).

**Aurora IAM roles**

An IAM role is an entity within your AWS account that has specific permissions.

**Using temporary credentials with Aurora**

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as AssumeRole or GetFederationToken.

Aurora supports using temporary credentials.

**Service-linked roles**

Service-linked roles allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in the Roles list in the IAM Management Console and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.

Aurora supports service-linked roles. For details about creating or managing Aurora service-linked roles, see Using service-linked roles for Amazon Aurora (p. 1277).

**Service roles**

This feature allows a service to assume a service role on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in the Roles list in the IAM Management Console and are owned by your account. This means that an IAM administrator can change the permissions for this role. However, doing so might break the functionality of the service.

Aurora supports service roles.

**Amazon Aurora identity-based policy examples**

By default, IAM users and roles don't have permission to create or modify Aurora resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating policies on the JSON tab in the IAM User Guide.

**Topics**

- Policy best practices (p. 1229)
- Using the Aurora console (p. 1229)
- Allow users to view their own permissions (p. 1229)
- Allow a user to create DB instances in an AWS account (p. 1230)
- Permissions required to use the console (p. 1231)
- Allow a user to perform any describe action on any RDS resource (p. 1232)
- Allow a user to create a DB instance that uses the specified DB parameter and security groups (p. 1232)
• Grant permission for actions on a resource with a specific tag with two different values (p. 1232)
• Prevent a user from deleting a DB instance (p. 1233)
• Deny all access to a resource (p. 1233)
• Example policies: Using condition keys (p. 1233)
• Specifying conditions: Using custom tags (p. 1235)

Policy best practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete Aurora resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

• Get Started Using AWS Managed Policies – To start using Aurora quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get started using permissions with AWS managed policies in the IAM User Guide.
• Grant Least Privilege – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant least privilege in the IAM User Guide.
• Enable MFA for Sensitive Operations – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using multi-factor authentication (MFA) in AWS in the IAM User Guide.
• Use Policy Conditions for Extra Security – To the extent that it’s practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON policy elements: Condition in the IAM User Guide.

Using the Aurora console

To access the Amazon Aurora console, you must have a minimum set of permissions. These permissions must enable you to list and view details about the Aurora resources in your AWS account. You can create an identity-based policy that is more restrictive than the minimum required permissions. However, if you do, the console doesn’t function as intended for entities (IAM users or roles) with that policy.

To ensure that those entities can still use the Aurora console, also attach the following AWS managed policy to the entities. For more information, see Adding permissions to a user in the IAM User Guide.

AmazonRDSReadOnlyAccess

You don’t need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you’re trying to perform.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```json
{
   "Version": "2012-10-17",
   "Statement": []
}
```
Identity-based policy examples

```json
{
    "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": "*"
}
}```

Allow a user to create DB instances in an AWS account

The following is an example policy that allows the user with the ID 123456789012 to create DB instances for your AWS account. The policy requires that the name of the new DB instance begin with `test`. The new DB instance must also use the MySQL database engine and the `db.t2.micro` DB instance class. In addition, the new DB instance must use an option group and a DB parameter group that starts with `default`, and it must use the default subnet group.

```json
{
    "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"
                }
            }
        }
    ]
}
```
The policy includes a single statement that specifies the following permissions for the IAM user:

- The policy allows the IAM user to create a DB instance using the CreateDBInstance API operation (this also applies to the create-db-instance AWS CLI command and the AWS Management Console).
- The Resource element specifies that the user can perform actions on or with resources. You specify resources using an Amazon Resources Name (ARN). This ARN includes the name of the service that the resource belongs to (rds), the AWS Region (* indicates any region in this example), the user account number (123456789012 is the user ID in this example), and the type of resource. For more information about creating ARNs, see Working with Amazon Resource Names (ARNs) in Amazon RDS (p. 406).

The Resource element in the example specifies the following policy constraints on resources for the user:

- The DB instance identifier for the new DB instance must begin with test (for example, testCustomerData1, test-region2-data).
- The option group for the new DB instance must begin with default.
- The DB parameter group for the new DB instance must begin with default.
- The subnet group for the new DB instance must be the default subnet group.
- The Condition element specifies that the DB engine must be MySQL and the DB instance class must be db.t2.micro. The Condition element specifies the conditions when a policy should take effect. You can add additional permissions or restrictions by using the Condition element. For more information about specifying conditions, see Condition keys (p. 1227). This example specifies the rds:DatabaseEngine and rds:DatabaseClass conditions. For information about the valid condition values for rds:DatabaseEngine, see the list under the Engine parameter in CreateDBInstance. For information about the valid condition values for rds:DatabaseClass, see Supported DB engines for DB instance classes (p. 47).

The policy doesn't specify the Principal element because in an identity-based policy you don't specify the principal who gets the permission. When you attach policy to a user, the user is the implicit principal. When you attach a permission policy to an IAM role, the principal identified in the role's trust policy gets the permissions.

To see a list of Aurora actions, see Actions Defined by Amazon RDS in the Service Authorization Reference.

Permissions required to use the console

For a user to work with the console, that user must have a minimum set of permissions. These permissions allow the user to describe the Amazon Aurora resources for their AWS account and to provide other related information, including Amazon EC2 security and network information.

If you create an IAM policy that is more restrictive than the minimum required permissions, the console doesn't function as intended for users with that IAM policy. To ensure that those users can still use the console, also attach the AmazonRDSReadOnlyAccess managed policy to the user, as described in Managing access using policies (p. 1224).

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the Amazon RDS API.

The following policy grants full access to all Amazon Aurora resources for the root AWS account:

```
AmazonRDSFullAccess
```

1231
Allow a user to perform any describe action on any RDS resource

The following permissions policy grants permissions to a user to run all of the actions that begin with Describe. These actions show information about an RDS resource, such as a DB instance. The wildcard character (*) in the Resource element indicates that the actions are allowed for all Amazon Aurora resources owned by the account.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowRDSDescribe",
         "Effect": "Allow",
         "Action": "rds:Describe*",
         "Resource": "*"
      }
   ]
}
```

Allow a user to create a DB instance that uses the specified DB parameter and security groups

The following permissions policy grants permissions to allow a user to only create a DB instance that must use the mysql-production DB parameter group and the db-production DB security group.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowMySQLProductionCreate",
         "Effect": "Allow",
         "Action": "rds:CreateDBInstance",
         "Resource": [
         ]
      }
   ]
}
```

Grant permission for actions on a resource with a specific tag with two different values

You can use conditions in your identity-based policy to control access to Aurora resources based on tags. The following policy allows permission to perform the ModifyDBInstance and CreateDBSnapshot APIs on DB instances with either the stage tag set to development or test.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowDevTestCreate",
         "Effect": "Allow",
         "Action": [
            "rds:ModifyDBInstance",
            "rds:CreateDBSnapshot"
         ]
      }
   ]
}
```
Prevent a user from deleting a DB instance

The following permissions policy grants permissions to prevent a user from deleting a specific DB instance. For example, you might want to deny the ability to delete your production DB instances to any user that is not an administrator.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyDelete1",
            "Effect": "Deny",
            "Action": "rds:DeleteDBInstance",
        }
    ]
}
```

Deny all access to a resource

You can explicitly deny access to a resource. Deny policies take precedence over allow policies. The following policy explicitly denies a user the ability to manage a resource:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "rds:*",
        }
    ]
}
```

Example policies: Using condition keys

Following are examples of how you can use condition keys in Amazon Aurora IAM permissions policies.

**Example 1: Grant permission to create a DB instance that uses a specific DB engine and isn't MultiAZ**

The following policy uses an RDS condition key and allows a user to create only DB instances that use the MySQL database engine and don't use MultiAZ. The `Condition` element indicates the requirement that the database engine is MySQL.
Identity-based policy examples

Example 2: Explicitly deny permission to create DB instances for certain DB instance classes and create DB instances that use Provisioned IOPS

The following policy explicitly denies permission to create DB instances that use the DB instance classes r3.8xlarge and m4.10xlarge, which are the largest and most expensive DB instance classes. This policy also prevents users from creating DB instances that use Provisioned IOPS, which incurs an additional cost.

Explicitly denying permission supersedes any other permissions granted. This ensures that identities to not accidentally get permission that you never want to grant.

```json
{
  "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
        }
      }
    }
  ]
}
```
Example 3: Limit the set of tag keys and values that can be used to tag a resource

The following policy uses an RDS condition key and allows the addition of a tag with the key stage to be added to a resource with the values test, qa, and production.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [ "rds:AddTagsToResource", "rds:RemoveTagsFromResource" ],
    "Resource": "*",
    "Condition": { "streq": { "rds:req-tag/stage": [ "test", "qa", "production" ] } }
  }]
}
```

Specifying conditions: Using custom tags

Amazon Aurora supports specifying conditions in an IAM policy using custom tags.

For example, suppose that you add a tag named environment to your DB instances with values such as beta, staging, production, and so on. If you do, you can create a policy that restricts certain users to DB instances based on the environment tag value.

**Note**

Custom tag identifiers are case-sensitive.

The following table lists the RDS tag identifiers that you can use in a Condition element.

<table>
<thead>
<tr>
<th>RDS tag identifier</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>db-tag</td>
<td>DB instances, including read replicas</td>
</tr>
<tr>
<td>snapshot-tag</td>
<td>DB snapshots</td>
</tr>
<tr>
<td>ri-tag</td>
<td>Reserved DB instances</td>
</tr>
<tr>
<td>secgrp-tag</td>
<td>DB security groups</td>
</tr>
<tr>
<td>og-tag</td>
<td>DB option groups</td>
</tr>
<tr>
<td>pg-tag</td>
<td>DB parameter groups</td>
</tr>
<tr>
<td>subgrp-tag</td>
<td>DB subnet groups</td>
</tr>
<tr>
<td>es-tag</td>
<td>Event subscriptions</td>
</tr>
<tr>
<td>cluster-tag</td>
<td>DB clusters</td>
</tr>
<tr>
<td>cluster-pg-tag</td>
<td>DB cluster parameter groups</td>
</tr>
<tr>
<td>cluster-snapshot-tag</td>
<td>DB cluster snapshots</td>
</tr>
</tbody>
</table>

The syntax for a custom tag condition is as follows:
Identity-based policy examples

"Condition":{"StringEquals":{"rds:db-tag/identifier/tag-name": ["value"]} }

For example, the following Condition element applies to DB instances with a tag named environment and a tag value of production.

"Condition":{"StringEquals":{"rds:db-tag/environment": ["production"]} }

For information about creating tags, see Tagging Amazon RDS resources (p. 401).

Important

If you manage access to your RDS resources using tagging, we recommend that you secure access to the tags for your RDS resources. You can manage access to tags by creating policies for the AddTagsToResource and RemoveTagsFromResource actions. For example, the following policy denies users the ability to add or remove tags for all resources. You can then create policies to allow specific users to add or remove tags.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"DenyTagUpdates",
      "Effect":"Deny",
      "Action": [
        "rds:AddTagsToResource",
        "rds:RemoveTagsFromResource"
      ],
      "Resource":"*"
    }
  ]
}
```

To see a list of Aurora actions, see Actions Defined by Amazon RDS in the Service Authorization Reference.

Example policies: Using custom tags

Following are examples of how you can use custom tags in Amazon Aurora IAM permissions policies. For more information about adding tags to an Amazon Aurora resource, see Working with Amazon Resource Names (ARNs) in Amazon RDS (p. 406).

Note

All examples use the us-west-2 region and contain fictitious account IDs.

Example 1: Grant permission for actions on a resource with a specific tag with two different values

The following policy allows permission to perform the ModifyDBInstance and CreateDBSnapshot APIs on DB instances with either the stage tag set to development or test.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AllowDevTestCreate",
      "Effect":"Allow",
      "Action": [
        "rds:ModifyDBInstance",
        "rds:CreateDBSnapshot"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "rds:db-tag/stage": 
```
Example 2: Explicitly deny permission to create a DB instance that uses specified DB parameter groups

The following policy explicitly denies permission to create a DB instance that uses DB parameter groups with specific tag values. You might apply this policy if you require that a specific customer-created DB parameter group always be used when creating DB instances. Policies that use *Deny* are most often used to restrict access that was granted by a broader policy.

Explicitly denying permission supersedes any other permissions granted. This ensures that identities to not accidentally get permission that you never want to grant.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "DenyProductionCreate",
         "Effect": "Deny",
         "Action": "rds:CreateDBInstance",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "rds:pg-tag/usage": "prod"
            }
         }
      }
   ]
}
```

Example 3: Grant permission for actions on a DB instance with an instance name that is prefixed with a user name

The following policy allows permission to call any API (except to *AddTagsToResource* or *RemoveTagsFromResource*) on a DB instance that has a DB instance name that is prefixed with the user's name and that has a tag called *stage* equal to *devo* or that has no tag called *stage*.

The *Resource* line in the policy identifies a resource by its Amazon Resource Name (ARN). For more information about using ARNs with Amazon Aurora resources, see Working with Amazon Resource Names (ARNs) in Amazon RDS (p. 406).

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowFullDevAccessNoTags",
         "Effect": "Allow",
         "NotAction": [
            "rds:AddTagsToResource",
            "rds:RemoveTagsFromResource"
         ],
         "Resource": "arn:aws:rds:*:123456789012:db:#{aws:username}*",
         "Condition": {
            "StringEqualsIfExists": {
            }
         }
      }
   ]
}
```
IAM database authentication

You can authenticate to your DB cluster using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with Aurora MySQL and Aurora PostgreSQL. With this authentication method, you don't need to use a password when you connect to a DB cluster. Instead, you use an authentication token.

An authentication token is a unique string of characters that Amazon Aurora generates on request. Authentication tokens are generated using AWS Signature Version 4. Each token has a lifetime of 15 minutes. You don't need to store user credentials in the database, because authentication is managed externally using IAM. You can also still use standard database authentication.

IAM database authentication provides the following benefits:

- Network traffic to and from the database is encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). For more information about using SSL/TLS with Amazon Aurora, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).
- You can use IAM to centrally manage access to your database resources, instead of managing access individually on each DB cluster.
- For applications running on Amazon EC2, you can use profile credentials specific to your EC2 instance to access your database instead of a password, for greater security.

Topics
- Availability for IAM database authentication (p. 1238)
- Limitations for IAM database authentication (p. 1239)
- Aurora MySQL recommendations for IAM database authentication (p. 1239)
- Enabling and disabling IAM database authentication (p. 1239)
- Creating and using an IAM policy for IAM database access (p. 1241)
- Creating a database account using IAM authentication (p. 1244)
- Connecting to your DB cluster using IAM authentication (p. 1245)

Availability for IAM database authentication

IAM database authentication is available for the following database engines:

- **Aurora MySQL**
  - Aurora MySQL version 2, all minor versions
    - For more information, see Database engine updates for Amazon Aurora MySQL 2.0 (p. 881).
  - Aurora MySQL version 1.10 and higher 1.1 minor versions
    - For more information, see Database engine updates for Amazon Aurora MySQL 1.1 (p. 930).
- **Aurora PostgreSQL**
  - Aurora PostgreSQL version 3, all minor versions
  - Aurora PostgreSQL version 2, all minor versions
• Aurora PostgreSQL version 1.3 and higher 1 minor versions

For more information, see Engine versions for Amazon Aurora PostgreSQL (p. 1148).

For Aurora MySQL, all supported DB instance classes support IAM database authentication, except for db.t2.small and db.t3.small. For information about the supported DB instance classes, see Supported DB engines for DB instance classes (p. 47).

Limitations for IAM database authentication

When using IAM database authentication, the following limitations apply:

• The maximum number of connections per second for your DB cluster might be limited depending on its DB instance class and your workload.
• Currently, IAM database authentication doesn't support global condition context keys.

For more information about global condition context keys, see AWS global condition context keys in the IAM User Guide.
• Currently, IAM database authentication isn't supported for CNAMEs.

Aurora MySQL recommendations for IAM database authentication

We recommend the following when using the Aurora MySQL DB engine:

• Use IAM database authentication as a mechanism for temporary, personal access to databases.
• Use IAM database authentication only for workloads that can be easily retried.
• Use IAM database authentication when your application requires fewer than 200 new IAM database authentication connections per second.

The database engines that work with Amazon Aurora don't impose any limits on authentication attempts per second. However, when you use IAM database authentication, your application must generate an authentication token. Your application then uses that token to connect to the DB cluster. If you exceed the limit of maximum new connections per second, then the extra overhead of IAM database authentication can cause connection throttling. The extra overhead can cause even existing connections to drop. For information about the maximum total connections for Aurora MySQL, see Maximum connections to an Aurora MySQL DB instance (p. 675).

Enabling and disabling IAM database authentication

By default, IAM database authentication is disabled on DB clusters. You can enable or disable IAM database authentication using the AWS Management Console, AWS CLI, or the API.

You can enable IAM database authentication when you perform one of the following actions:

• To create a new DB cluster with IAM database authentication enabled, see Creating an Amazon Aurora DB cluster (p. 118).
• To modify a DB cluster to enable IAM database authentication, see Modifying an Amazon Aurora DB cluster (p. 327).
• To restore a DB cluster from a snapshot with IAM database authentication enabled, see Restoring from a DB cluster snapshot (p. 420).
• To restore a DB cluster to a point in time with IAM database authentication enabled, see Restoring a DB cluster to a specified time (p. 454).
Console

Each creation or modification workflow has a **Database authentication** section, where you can enable or disable IAM database authentication. In that section, choose **Password and IAM database authentication** to enable IAM database authentication.

**To enable or disable IAM database authentication for an existing DB cluster**

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**.
3. Choose the DB cluster that you want to modify.
   
   **Note**
   You can only enable IAM authentication if all DB instances in the DB cluster are compatible with IAM. Check the compatibility requirements in *Availability for IAM database authentication* (p. 1238).
4. Choose **Modify**.
5. In the **Database authentication** section, choose **Password and IAM database authentication** to enable IAM database authentication, or choose a different option to disable it.
6. Choose **Continue**.
7. To apply the changes immediately, choose **Immediately** in the **Scheduling of modifications** section.
8. Choose **Modify cluster**.

AWS CLI

To create a new DB cluster with IAM authentication by using the AWS CLI, use the **create-db-cluster** command. Specify the **--enable-iam-database-authentication** option.

To update an existing DB cluster to have or not have IAM authentication, use the AWS CLI command **modify-db-cluster**. Specify either the **--enable-iam-database-authentication** or **--no-enable-iam-database-authentication** option, as appropriate.

**Note**

You can only enable IAM authentication if all DB instances in the DB cluster are compatible with IAM. Check the compatibility requirements in *Availability for IAM database authentication* (p. 1238).

By default, Aurora performs the modification during the next maintenance window. If you want to override this and enable IAM DB authentication as soon as possible, use the **--apply-immediately** parameter.

If you are restoring a DB cluster, use one of the following AWS CLI commands:

- **restore-db-cluster-to-point-in-time**
- **restore-db-cluster-from-db-snapshot**

The IAM database authentication setting defaults to that of the source snapshot. To change this setting, set the **--enable-iam-database-authentication** or **--no-enable-iam-database-authentication** option, as appropriate.

RDS API

To create a new DB instance with IAM authentication by using the API, use the API operation **CreateDBCluster**. Set the **EnableIAMDatabaseAuthentication** parameter to **true**.
To update an existing DB cluster to have IAM authentication, use the API operation `ModifyDBCluster`. Set the `EnableIAMDatabaseAuthentication` parameter to `true` to enable IAM authentication, or `false` to disable it.

**Note**
You can only enable IAM authentication if all DB instances in the DB cluster are compatible with IAM. Check the compatibility requirements in Availability for IAM database authentication (p. 1238).

If you are restoring a DB cluster, use one of the following API operations:

- `RestoreDBClusterFromSnapshot`
- `RestoreDBClusterToPointInTime`

The IAM database authentication setting defaults to that of the source snapshot. To change this setting, set the `EnableIAMDatabaseAuthentication` parameter to `true` to enable IAM authentication, or `false` to disable it.

**Creating and using an IAM policy for IAM database access**

To allow an IAM user or role to connect to your DB cluster, you must create an IAM policy. After that, you attach the policy to an IAM user or role.

**Note**
To learn more about IAM policies, see Identity and access management in Amazon Aurora (p. 1222).

The following example policy allows an IAM user to connect to a DB cluster using IAM database authentication.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["rds-db:connect"],
    }
  ]
}
```

**Important**
An IAM administrator user can access DB clusters without explicit permissions in an IAM policy. The example in Create an IAM user (p. 73) creates an IAM administrator user. If you want to restrict administrator access to DB clusters, you can create an IAM role with the appropriate, lesser privileged permissions and assign it to the administrator.

**Note**
Don't confuse the `rds-db:` prefix with other RDS API operation prefixes that begin with `rds:`. You use the `rds-db:` prefix and the `rds-db:connect` action only for IAM database authentication. They aren't valid in any other context. Currently, the IAM console displays an error for policies with the `rds-db:connect` action. You can ignore this error.
The example policy includes a single statement with the following elements:

- **Effect** – Specify `Allow` to grant access to the DB cluster. If you don’t explicitly allow access, then access is denied by default.
- **Action** – Specify `rds-db:connect` to allow connections to the DB cluster.
- **Resource** – Specify an Amazon Resource Name (ARN) that describes one database account in one DB cluster. The ARN format is as follows.

```
arn:aws:rds-db:region:account-id:dbuser:DbClusterResourceId/db-user-name
```

In this format, replace the following:

- **region** is the AWS Region for the DB cluster. In the example policy, the AWS Region is `us-east-2`.
- **account-id** is the AWS account number for the DB cluster. In the example policy, the account number is `1234567890`.
- **DbClusterResourceId** is the identifier for the DB cluster. This identifier is unique to an AWS Region and never changes. In the example policy, the identifier is `cluster-ABCDEFGHIJKL01234`.

To find a DB cluster resource ID in the AWS Management Console for Amazon Aurora, choose the DB cluster to see its details. Then choose the **Configuration** tab. The **Resource ID** is shown in the **Configuration** section.

Alternatively, you can use the AWS CLI command to list the identifiers and resource IDs for all of your DB cluster in the current AWS Region, as shown following.

```
aws rds describe-db-clusters --query "DBClusters[*].
[DBClusterIdentifier,DbClusterResourceId]"
```

**Note**

If you are connecting to a database through RDS Proxy, specify the proxy resource ID, such as `prx-ABCDEFGHIJKL01234`. For information about using IAM database authentication with RDS Proxy, see Connecting to a proxy using IAM authentication (p. 276).

- **db-user-name** is the name of the database account to associate with IAM authentication. In the example policy, the database account is `db_user`.

You can construct other ARNs to support various access patterns. The following policy allows access to two different database accounts in a DB cluster.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds-db:connect"
      ],
      "Resource": [
      ]
    }
  ]
}
```
The following policy uses the "*" character to match all DB clusters and database accounts for a particular AWS account and AWS Region.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["rds-db:connect"],
        }
    ]
}
```

The following policy matches all of the DB clusters for a particular AWS account and AWS Region. However, the policy only grants access to DB clusters that have a jane_doe database account.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["rds-db:connect"],
        }
    ]
}
```

The IAM user or role has access to only those databases that the database user does. For example, suppose that your DB cluster has a database named dev, and another database named test. If the database user jane_doe has access only to dev, any IAM users or roles that access that DB cluster with the jane_doe user also have access only to dev. This access restriction is also true for other database objects, such as tables, views, and so on.

An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions. For examples of policies, see Amazon Aurora identity-based policy examples (p. 1228).

**Attaching an IAM policy to an IAM user or role**

After you create an IAM policy to allow database authentication, you need to attach the policy to an IAM user or role. For a tutorial on this topic, see Create and attach your first customer managed policy in the IAM User Guide.
As you work through the tutorial, you can use one of the policy examples shown in this section as a starting point and tailor it to your needs. At the end of the tutorial, you have an IAM user with an attached policy that can make use of the rds-db:connect action.

**Note**
You can map multiple IAM users or roles to the same database user account. For example, suppose that your IAM policy specified the following resource ARN.

```
arn:aws:rds-db:us-east-2:123456789012:dbuser:cluster-12ABC34DEFG5HIJ6KLMNOP78QR/jane_doe
```

If you attach the policy to IAM users *Jane*, *Bob*, and *Diego*, then each of those users can connect to the specified DB cluster using the *jane_doe* database account.

### Creating a database account using IAM authentication

With IAM database authentication, you don't need to assign database passwords to the user accounts you create. If you remove an IAM user that is mapped to a database account, you should also remove the database account with the **DROP USER** statement.

#### Using IAM authentication with PostgreSQL

To use IAM authentication with PostgreSQL, connect to the DB cluster, create database users, and then grant them the rds_iam role as shown in the following example.

```
CREATE USER db_userx;
GRANT rds_iam TO db_userx;
```

The specified database account should have the same name as the IAM user or role. In this example, both the database account and the IAM user or role are named *db_userx*.

#### Using IAM authentication with MySQL

With MySQL, authentication is handled by **AWSAuthenticationPlugin**—an AWS-provided plugin that works seamlessly with IAM to authenticate your IAM users. Connect to the DB cluster and issue the **CREATE USER** statement, as shown in the following example.

```
CREATE USER jane_doe IDENTIFIED WITH AWSAuthenticationPlugin AS 'RDS';
```

The **IDENTIFIED WITH** clause allows MySQL to use the **AWSAuthenticationPlugin** to authenticate the database account (*jane_doe*). The **AS 'RDS'** clause refers to the authentication method, and the specified database account should have the same name as the IAM user or role. In this example, both the database account and the IAM user or role are named *jane_doe*.

**Note**
If you see the following message, it means that the AWS-provided plugin is not available for the current DB cluster.

```
ERROR 1524 (HY000): Plugin 'AWSAuthenticationPlugin' is not loaded
```

To troubleshoot this error, verify that you are using a supported configuration and that you have enabled IAM database authentication on your DB cluster. For more information, see Availability for IAM database authentication (p. 1238) and Enabling and disabling IAM database authentication (p. 1239).

After you create an account using **AWSAuthenticationPlugin**, you manage it in the same way as other database accounts. For example, you can modify account privileges with **GRANT** and **REVOKE** statements, or modify various account attributes with the **ALTER USER** statement.
Connecting to your DB cluster using IAM authentication

With IAM database authentication, you use an authentication token when you connect to your DB cluster. An authentication token is a string of characters that you use instead of a password. After you generate an authentication token, it's valid for 15 minutes before it expires. If you try to connect using an expired token, the connection request is denied.

Every authentication token must be accompanied by a valid signature, using AWS signature version 4. (For more information, see Signature Version 4 signing process in the AWS General Reference.) The AWS CLI and an AWS SDK, such as the AWS SDK for Java or AWS SDK for Python (Boto3), can automatically sign each token you create.

You can use an authentication token when you connect to Amazon Aurora from another AWS service, such as AWS Lambda. By using a token, you can avoid placing a password in your code. Alternatively, you can use an AWS SDK to programmatically create and programmatically sign an authentication token.

After you have a signed IAM authentication token, you can connect to an Aurora DB cluster. Following, you can find out how to do this using either a command line tool or an AWS SDK, such as the AWS SDK for Java or AWS SDK for Python (Boto3).

For more information, see the following blog posts:

- Use IAM authentication to connect with SQL Workbench/J to Amazon Aurora MySQL or Amazon RDS for MySQL
- Using IAM authentication to connect with pgAdmin Amazon Aurora PostgreSQL or Amazon RDS for PostgreSQL

The following are prerequisites for connecting to your DB cluster using IAM authentication:

- Enabling and disabling IAM database authentication (p. 1239)
- Creating and using an IAM policy for IAM database access (p. 1241)
- Creating a database account using IAM authentication (p. 1244)

Topics

- Connecting to your DB cluster using IAM authentication from the command line: AWS CLI and mysql client (p. 1245)
- Connecting to your DB cluster using IAM authentication from the command line: AWS CLI and psql client (p. 1247)
- Connecting to your DB cluster using IAM authentication and the AWS SDK for .NET (p. 1248)
- Connecting to your DB cluster using IAM authentication and the AWS SDK for Go (p. 1250)
- Connecting to your DB cluster using IAM authentication and the AWS SDK for Java (p. 1253)
- Connecting to your DB cluster using IAM authentication and the AWS SDK for Python (Boto3) (p. 1260)

Connecting to your DB cluster using IAM authentication from the command line: AWS CLI and mysql client

You can connect from the command line to an Aurora DB cluster with the AWS CLI and `mysql` command line tool as described following.

The following are prerequisites for connecting to your DB cluster using IAM authentication:

- Enabling and disabling IAM database authentication (p. 1239)
- Creating and using an IAM policy for IAM database access (p. 1241)
• Creating a database account using IAM authentication (p. 1244)

Topics
• Generating an IAM authentication token (p. 1246)
• Connecting to a DB cluster (p. 1246)

Generating an IAM authentication token
The following example shows how to get a signed authentication token using the AWS CLI.

```bash
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 the example, the parameters are as follows:
- `--hostname` – The host name of the DB cluster that you want to access
- `--port` – The port number used for connecting to your DB cluster
- `--region` – The AWS Region where the DB cluster is running
- `--username` – The database account that you want to access

The first several characters of the token look like the following.

```
rdsmysql.123456789012.us-west-2.rds.amazonaws.com:3306/?Action=connect&DBUser=jane_doe&X-
Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

Connecting to a DB cluster
The general format for connecting is shown following.

```bash
mysql --host=hostName --port=portNumber --ssl-ca=[full path]rds-combined-ca-bundle.pem --
enable-cleartext-plugin --user=userName --password=authToken
```

The parameters are as follows:
- `--host` – The host name of the DB cluster that you want to access
- `--port` – The port number used for connecting to your DB cluster
- `--ssl-ca` – The SSL certificate file that contains the public key

For more information, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).
- `--enable-cleartext-plugin` – A value that specifies that AWSAuthenticationPlugin must be
  used for this connection
- `--user` – The database account that you want to access
- `--password` – A signed IAM authentication token

The authentication token consists of several hundred characters. It can be unwieldy on the command
line. One way to work around this is to save the token to an environment variable, and then use that
variable when you connect. The following example shows one way to perform this workaround.

```
RDSHOST="rdsmysql.123456789012.us-west-2.rds.amazonaws.com"
```
When you connect using AWSAuthenticationPlugin, the connection is secured using SSL. To verify this, type the following at the mysql> command prompt.

```sql
show status like 'Ssl%';
```

The following lines in the output show more details.

```sql
+---------------+-------------+
| Variable_name | Value       |
|---------------+-------------+
| ...           | ...         |
| Ssl_cipher    | AES256-SHA  |
| ...           | ...         |
| Ssl_version   | TLSv1.1     |
| ...           | ...         |
```

Connecting to your DB cluster using IAM authentication from the command line:
AWS CLI and psql client

You can connect from the command line to an Aurora PostgreSQL DB cluster with the AWS CLI and psql command line tool as described following.

The following are prerequisites for connecting to your DB cluster using IAM authentication:

- Enabling and disabling IAM database authentication (p. 1239)
- Creating and using an IAM policy for IAM database access (p. 1241)
- Creating a database account using IAM authentication (p. 1244)

Topics

- Generating an IAM authentication token (p. 1247)
- Connecting to an Aurora PostgreSQL cluster (p. 1248)

Generating an IAM authentication token

The authentication token consists of several hundred characters so it can be unwieldy on the command line. One way to work around this is to save the token to an environment variable, and then use that variable when you connect. The following example shows how to use the AWS CLI to get a signed authentication token using the generated-db-auth-token command, and store it in a PGPASSWORD environment variable.

```bash
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 the example, the parameters to the `generate-db-auth-token` command are as follows:

- `--hostname` – The host name of the DB cluster (cluster endpoint) that you want to access
- `--port` – The port number used for connecting to your DB cluster
- `--region` – The AWS Region where the DB cluster is running
- `--username` – The database account that you want to access

The first several characters of the generated token look like the following.

```
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...
```

**Connecting to an Aurora PostgreSQL cluster**

The general format for using `psql` to connect is shown following.

```
psql "host=hostName port=portNumber sslmode=verify-full sslrootcert=certificateFile dbname=DBName user=userName password=authToken"
```

The parameters are as follows:

- `host` – The host name of the DB cluster (cluster endpoint) that you want to access
- `port` – The port number used for connecting to your DB cluster
- `sslmode` – The SSL mode to use

  When you use `sslmode=verify-full`, the SSL connection verifies the DB cluster endpoint against the endpoint in the SSL certificate.

- `sslrootcert` – The SSL certificate file that contains the public key

  For more information, see Using SSL with a PostgreSQL DB instance.

- `dbname` – The database that you want to access
- `user` – The database account that you want to access
- `password` – A signed IAM authentication token

The following example shows using `psql` to connect. In the example `psql` uses the environment variable `PGPASSWORD` that was set when the token was generated in the previous section.

```
psql "host=$RDSHOST port=5432 sslmode=verify-full sslrootcert=/sample_dir/rds-combined-ca-bundle.pem dbname=DBName user=jane_doe password=$PGPASSWORD"
```

**Connecting to your DB cluster using IAM authentication and the AWS SDK for .NET**

You can connect to an Aurora MySQL or Aurora PostgreSQL DB cluster with the AWS SDK for .NET as described following.

The following are prerequisites for connecting to your DB cluster using IAM authentication:

- Enabling and disabling IAM database authentication (p. 1239)
- Creating and using an IAM policy for IAM database access (p. 1241)
- Creating a database account using IAM authentication (p. 1244)
The following code example shows how to generate an authentication token, and then use it to connect to a DB cluster.

To run this code example, you need the AWS SDK for .NET, found on the AWS site. The AWSSDK.Core and the AWSSDK.RDS packages are required. To connect to a DB instance, use the .NET database connector for the DB engine, such as MySqlConnector for MySQL or Npgsql for PostgreSQL.

Modify the values of the following variables as needed:

- server – The endpoint of the DB cluster that you want to access
- port – The port number used for connecting to your DB cluster
- user – The database account that you want to access.

This code connects to an Aurora MySQL DB cluster.

```
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, "mysqldb.123456789012.us-east-1.rds.amazonaws.com", 3306, "jane_doe");
            // for debug only
            Console.WriteLine("{0}\n", pwd); // this verifies the token is generated

            MySqlConnection conn = new MySqlConnection("server=mysqldb.123456789012.us-east-1.rds.amazonaws.com;user=jane_doe;database=mydB;port=3306;password={pwd};SslMode=Required;SslCa=../rds-ca-2019-root.pem");
            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();
        }
    }
}
```

This code connects to an Aurora PostgreSQL DB cluster.

```
using System;
using Npgsql;
using Amazon.RDS.Util;

namespace ConsoleApp1
{
    class Program
    {
        static void Main(string[] args)
        {
            var pwd = Amazon.RDS.Util.RDSAuthTokenGenerator.GenerateAuthToken(RegionEndpoint.USEast1, "mysqldb.123456789012.us-east-1.rds.amazonaws.com", 3306, "jane_doe");
            // for debug only
            Console.WriteLine("{0}\n", pwd); // this verifies the token is generated

            NpgsqlConnection conn = new NpgsqlConnection("server=mysqldb.123456789012.us-east-1.rds.amazonaws.com;user=jane_doe;database=mydB;port=3306;password={pwd};SslMode=Required;SslCa=../rds-ca-2019-root.pem");
            conn.Open();

            // Define a query
            NpgsqlCommand sampleCommand = new NpgsqlCommand("SHOW DATABASES;", conn);

            // Execute a query
            NpgsqlDataReader sqlDataRdr = sampleCommand.ExecuteReader();

            // Read all rows and output the first column in each row
            while (sqlDataRdr.Read())
            {
                Console.WriteLine(sqlDataRdr[0]);
            }
            sqlDataRdr.Close();
            // Close connection
            conn.Close();
        }
    }
}
```
Connecting to your DB cluster using IAM authentication and the AWS SDK for Go

You can connect to an Aurora MySQL or Aurora PostgreSQL DB cluster with the AWS SDK for Go as described following.

The following are prerequisites for connecting to your DB cluster using IAM authentication:

- Enabling and disabling IAM database authentication (p. 1239)
- Creating and using an IAM policy for IAM database access (p. 1241)
- Creating a database account using IAM authentication (p. 1244)

To run these code examples, you need the AWS SDK for Go, found on the AWS site.

Modify the values of the following variables as needed:

- `dbName` – The database that you want to access
- `dbUser` – The database account that you want to access
- `dbHost` – The endpoint of the DB cluster that you want to access
- `dbPort` – The port number used for connecting to your DB cluster
- `region` – The AWS Region where the DB cluster is running

In addition, make sure the imported libraries in the sample code exist on your system.

**Topics**

- Generating an IAM authentication token (p. 1251)
- Connecting to a DB cluster (p. 1252)
Generating an IAM authentication token

You can use the rdsutils package to generate tokens used to connect to a DB cluster. Call the BuildAuthToken function to generate a token. Provide the DB instance endpoint, AWS region, username, and IAM credentials to generate the token for connecting to a DB cluster with IAM credentials.

The following example shows how to use BuildAuthToken to create an authentication token for connecting to an Aurora MySQL DB cluster.

```go
package main

import (
    "database/sql"
    "fmt"
    "log"
    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/service/rds/rdsutils"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "mydb.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 {
        log.Fatal("failed to build auth token %v", err)
    }
}
```

The following example shows how to use BuildAuthToken to create an authentication token for connecting to an Aurora PostgreSQL DB cluster.

```go
package main

import (
    "database/sql"
    "fmt"
    "log"
    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/service/rds/rdsutils"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "mydb.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 {
        log.Fatal("failed to build auth token %v", err)
    }
}
```
Connecting to a DB cluster

The following code example shows how to generate an authentication token, and then use it to connect to a DB cluster.

This code connects to an Aurora MySQL DB cluster.

```go
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 := "mydb.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)
    }
}
```

This code connects to an Aurora PostgreSQL DB cluster.

```go
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"
```
Connecting to your DB cluster using IAM authentication and the AWS SDK for Java

You can connect to an Aurora MySQL or Aurora PostgreSQL DB cluster with the AWS SDK for Java as described following.

The following are prerequisites for connecting to your DB cluster using IAM authentication:

- Enabling and disabling IAM database authentication (p. 1239)
- Creating and using an IAM policy for IAM database access (p. 1241)
- Creating a database account using IAM authentication (p. 1244)

Topics

- Generating an IAM authentication token (p. 1253)
- Manually constructing an IAM authentication token (p. 1254)
- Connecting to a DB cluster (p. 1257)

Generating an IAM authentication token

If you are writing programs using the AWS SDK for Java, you can get a signed authentication token using the RdsIamAuthTokenGenerator class. Using this class requires that you provide AWS credentials. To do this, you create an instance of the DefaultAWSCredentialsProviderChain class. DefaultAWSCredentialsProviderChain uses the first AWS access key and secret key that it finds in the default credential provider chain. For more information about AWS access keys, see Managing access keys for IAM users.

After you create an instance of RdsIamAuthTokenGenerator, you can call the getAuthToken method to obtain a signed token. Provide the AWS Region, host name, port number, and user name. The following code example illustrates how to do this.

```java
package com.amazonaws.codesamples;

dbHost := "mydb.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)
}
erroc = db.Ping()
if err != nil {
    panic(err)
}
```
Manually constructing an IAM authentication token

In Java, the easiest way to generate an authentication token is to use RdsIamAuthTokenGenerator. This class creates an authentication token for you, and then signs it using AWS signature version 4. For more information, see Signature version 4 signing process in the AWS General Reference.

However, you can also construct and sign an authentication token manually, as shown in the following code example.
public class CreateRDSAuthTokenManually 
{
  public static String httpMethod = "GET";
  public static String action = "connect";
  public static String canonicalURIParameter = "/";
  public static 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 + "/" + date + "/" + region + "/%2F" + serviceName + "/%2Faws4_request");
    canonicalQueryParameters.put("X-Amz-Date", dateTime);
    canonicalQueryParameters.put("X-Amz-Expires", expiryPeriod);
    canonicalQueryParameters.put("X-Amz-SignedHeaders", signedHeader);

    canonicalQueryParameters.put("Action", action);
    canonicalQueryParameters.put("DBUser", user);
    canonicalQueryParameters.put("X-Amz-Algorithm", "AWS4-HMAC-SHA256");
    canonicalQueryParameters.put("X-Amz-Credential", accessKey + "/" + date + "/" + 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);
}
IAM database authentication

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);
    }
}

Connecting to a DB cluster

The following code example shows how to generate an authentication token, and then use it to connect to a cluster running MySQL.

To run this code example, you need the AWS SDK for Java, found on the AWS site. In addition, you need the following:

- MySQL Connector/J. This code example was tested with mysql-connector-java-5.1.33-bin.jar.
- An intermediate certificate for Amazon Aurora that is specific to an AWS Region. (For more information, see Using SSL/TLS to encrypt a connection to a DB cluster (p. 1211).) At runtime, the class loader looks for the certificate in the same directory as this Java code example, so that the class loader can find it.
- Modify the values of the following variables as needed:
  - RDS_INSTANCE_HOSTNAME – The host name of the DB cluster that you want to access.
  - RDS_INSTANCE_PORT – The port number used for connecting to your PostgreSQL DB cluster.
  - REGION_NAME – The AWS Region where the DB cluster is running.
  - DB_USER – The database account that you want to access.
  - SSL_CERTIFICATE – An SSL certificate for Amazon Aurora that is specific to an AWS Region.

To download a certificate for your AWS Region, see Intermediate certificates (p. 1212). Place the SSL certificate in the same directory as this Java program file, so that the class loader can find the certificate at runtime.

This code example obtains AWS credentials from the default credential provider chain.
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();
    }
}

1258
/**
 * 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=8996&X-Amz-Credential=AKIAPFXHGVDI5RNFO4AQ%2F20171003%2Fcnc-north-1%2Frds-db%2Faws4_request&X-Amz-Signature=f9f45ef9f6c1f770cddad11a53e33f4a4c37730bc03fdee820c6f1322edd15483b
 * @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
 */
Connecting to your DB cluster using IAM authentication and the AWS SDK for Python (Boto3)

You can connect to an Aurora MySQL or Aurora PostgreSQL DB cluster with the AWS SDK for Python (Boto3) as described following.

The following are prerequisites for connecting to your DB cluster using IAM authentication:

- Enabling and disabling IAM database authentication (p. 1239)
- Creating and using an IAM policy for IAM database access (p. 1241)
- Creating a database account using IAM authentication (p. 1244)
In addition, make sure the imported libraries in the sample code exist on your system.

The code examples use profiles for shared credentials. For information about the specifying credentials, see Credentials in the AWS SDK for Python (Boto3) documentation.

**Topics**

- Generating an IAM authentication token (p. 1261)
- Connecting to a DB cluster (p. 1252)

**Generating an IAM authentication token**

You can call the `generate_db_auth_token` method to obtain a signed token. Provide the DB cluster endpoint, port, user name, AWS Region, and DB engine to generate the token for connecting to a DB cluster with IAM credentials.

This code generates an IAM authentication token for an Aurora MySQL DB cluster.

```python
import sys
import boto3

ENDPOINT="mysqlcluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
PORT="3306"
USR="jane_doe"
REGION="us-east-1"
os.environ['LIBMYSQL_ENABLE_CLEARTEXT_PLUGIN'] = '1'

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
client = boto3.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USR, Region=REGION)
```

This code generates an IAM authentication token for an Aurora PostgreSQL DB cluster.

```python
import sys
import boto3

ENDPOINT="postgresmycluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
PORT="5432"
USR="jane_doe"
REGION="us-east-1"

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
client = boto3.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USR, Region=REGION)
```

**Connecting to a DB cluster**

The following code example shows how to generate an authentication token, and then use it to connect to a DB cluster.

To run this code example, you need the AWS SDK for Python (Boto3), found on the AWS site.
Modify the values of the following variables as needed:

- **ENDPOINT** – The endpoint of the DB cluster that you want to access
- **PORT** – The port number used for connecting to your DB cluster
- **USER** – The database account that you want to access.
- **REGION** – The AWS Region where the DB cluster is running
- **DBNAME** – The database that you want to access

This code connects to an Aurora MySQL DB cluster.

```python
import mysql.connector
import sys
import os

ENDPOINT="mysqlcluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
PORT="3306"
USR="jane_doe"
REGION="us-east-1"
DBNAME="mydb"
observer['LIBMYSQL_ENABLE_CLEARTEXT_PLUGIN'] = '1'

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='default')
client = boto3.client('rds')
token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USR, Region=REGION)

try:
    conn = mysql.connector.connect(host=ENDPOINT, user=USR, passwd=token, port=PORT, database=DBNAME)
    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))
```

This code connects to an Aurora PostgreSQL DB cluster.

```python
import psycopg2
import sys
import boto3

ENDPOINT="postgresmycluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
PORT="5432"
USR="jane_doe"
REGION="us-east-1"
DBNAME="mydb"

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
client = boto3.client('rds')
token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USR, Region=REGION)

try:
    conn = psycopg2.connect(host=ENDPOINT, user=USR, password=token, port=PORT, database=DBNAME)
    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))
```
try:
  conn = psycopg2.connect(host=ENDPOINT, port=PORT, database=DBNAME, user=USR, password=token)
  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))

Troubleshooting Amazon Aurora identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Aurora and IAM.

Topics
- I Am not authorized to perform an action in Aurora (p. 1263)
- I Am not authorized to perform iam:PassRole (p. 1263)
- I want to view my access keys (p. 1264)
- I'm an administrator and want to allow others to access Aurora (p. 1264)
- I want to allow people outside of my AWS account to access my Aurora resources (p. 1264)

I Am not authorized to perform an action in Aurora

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

The following example error occurs when the mateojackson IAM user tries to use the console to view details about a widget but does not have rds:GetWidget permissions.

User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: rds:GetWidget on resource: my-example-widget

In this case, Mateo asks his administrator to update his policies to allow him to access the my-example-widget resource using the rds:GetWidget action.

I Am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the iam:PassRole action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to Aurora.

Some AWS services allow you to pass an existing role to that service, instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named marymajor tries to use the console to perform an action in Aurora. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole

In this case, Mary asks her administrator to update her policies to allow her to perform the iam:PassRole action.
I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can’t view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

**Important**

Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing access keys in the *IAM User Guide*.

I'm an administrator and want to allow others to access Aurora

To enable others to access Aurora, you must create an IAM entity (user or role) for the person or application that needs access. They use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Aurora.

To get started right away, see Creating your first IAM delegated user and group in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my Aurora resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Aurora supports these features, see How Amazon Aurora works with IAM (p. 1225).
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.

Logging and monitoring in Amazon Aurora

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Aurora and your AWS solutions. You should collect monitoring data from all of the parts of your AWS solution so that you can more easily debug a multi-point failure if one occurs. AWS provides several tools for monitoring your Amazon Aurora resources and responding to potential incidents:
Amazon CloudWatch Alarms

Using Amazon CloudWatch alarms, you watch a single metric over a time period that you specify. If the metric exceeds a given threshold, a notification is sent to an Amazon SNS topic or AWS Auto Scaling policy. CloudWatch alarms do not invoke actions because they are in a particular state. Rather the state must have changed and been maintained for a specified number of periods. For more information, see Monitoring with Amazon CloudWatch (p. 463).

AWS CloudTrail Logs

CloudTrail provides a record of actions taken by a user, role, or an AWS service in Amazon Aurora. CloudTrail captures all API calls for Amazon Aurora as events, including calls from the console and from code calls to Amazon RDS API operations. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Aurora, the IP address from which the request was made, who made the request, when it was made, and additional details. For more information, see Working with AWS CloudTrail and Amazon RDS (p. 630).

Enhanced Monitoring

Amazon Aurora provides metrics in real time for the operating system (OS) that your DB cluster runs on. You can view the metrics for your DB cluster using the console, or consume the Enhanced Monitoring JSON output from Amazon CloudWatch Logs in a monitoring system of your choice. For more information, see Enhanced Monitoring (p. 504).

Amazon RDS Performance Insights

Performance Insights expands on existing Amazon Aurora monitoring features to illustrate your database's performance and help you analyze any issues that affect it. With the Performance Insights dashboard, you can visualize the database load and filter the load by waits, SQL statements, hosts, or users. For more information, see Using Amazon RDS Performance Insights (p. 514).

Database Logs

You can view, download, and watch database logs using the AWS Management Console, AWS CLI, or RDS API. For more information, see Amazon Aurora database log files (p. 618).

Amazon Aurora Recommendations

Amazon Aurora provides automated recommendations for database resources. These recommendations provide best practice guidance by analyzing DB cluster configuration, usage, and performance data. For more information, see Using Amazon Aurora recommendations (p. 484).

Amazon Aurora Event Notification

Amazon Aurora uses the Amazon Simple Notification Service (Amazon SNS) to provide notification when an Amazon Aurora event occurs. These notifications can be in any notification form supported by Amazon SNS for an AWS Region, such as an email, a text message, or a call to an HTTP endpoint. For more information, see Using Amazon RDS event notification (p. 594).

AWS Trusted Advisor

Trusted Advisor draws upon best practices learned from serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and then makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps. All AWS customers have access to five Trusted Advisor checks. Customers with a Business or Enterprise support plan can view all Trusted Advisor checks.

Trusted Advisor has the following Amazon Aurora-related checks:

- Amazon Aurora Idle DB Instances
- Amazon Aurora Security Group Access Risk
- Amazon Aurora Backups
- Amazon Aurora Multi-AZ
- Aurora DB Instance Accessibility
For more information on these checks, see Trusted Advisor best practices (checks).

**Database activity streams**

Database activity streams can protect your databases from internal threats by controlling DBA access to the database activity streams. Thus, the collection, transmission, storage, and subsequent processing of the database activity stream is beyond the access of the DBAs that manage the database. Database activity streams can provide safeguards for your database and meet compliance and regulatory requirements. For more information, see Using Database Activity Streams with Amazon Aurora (p. 565).

For more information about monitoring Aurora see Monitoring an Amazon Aurora DB cluster (p. 459).
Compliance validation for Amazon Aurora

Third-party auditors assess the security and compliance of Amazon Aurora as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS services in scope by compliance program. For general information, see AWS compliance programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading reports in AWS Artifact.

Your compliance responsibility when using Amazon Aurora is determined by the sensitivity of your data, your organization's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- **Security and compliance quick start guides** – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- **Architecting for HIPAA security and compliance whitepaper** – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- **AWS compliance resources** – This collection of workbooks and guides that might apply to your industry and location.
- **AWS Config** – This AWS service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.
Resilience in Amazon Aurora

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS global infrastructure.

In addition to the AWS global infrastructure, Aurora offers features to help support your data resiliency and backup needs.

Backup and restore

Aurora backs up your cluster volume automatically and retains restore data for the length of the backup retention period. Aurora backups are continuous and incremental so you can quickly restore to any point within the backup retention period. No performance impact or interruption of database service occurs as backup data is being written. You can specify a backup retention period, from 1 to 35 days, when you create or modify a DB cluster.

If you want to retain a backup beyond the backup retention period, you can also take a snapshot of the data in your cluster volume. Aurora retains incremental restore data for the entire backup retention period. Thus, you need to create a snapshot only for data that you want to retain beyond the backup retention period. You can create a new DB cluster from the snapshot.

You can recover your data by creating a new Aurora DB cluster from the backup data that Aurora retains, or from a DB cluster snapshot that you have saved. You can quickly create a new copy of a DB cluster from backup data to any point in time during your backup retention period. The continuous and incremental nature of Aurora backups during the backup retention period means you don't need to take frequent snapshots of your data to improve restore times.

For more information, see Backing up and restoring an Amazon Aurora DB cluster (p. 414).

Replication

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region. The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary DB instance and to Aurora Replicas in the DB cluster. If the primary DB instance fails, an Aurora Replica is promoted to be the primary DB instance.

Aurora also supports replication options that are specific to Aurora MySQL and Aurora PostgreSQL.

For more information, see Replication with Amazon Aurora (p. 57).

Failover

Aurora stores copies of the data in a DB cluster across multiple Availability Zones in a single AWS Region. This storage occurs regardless of whether the DB instances in the DB cluster span multiple Availability Zones. When you create Aurora Replicas across Availability Zones, Aurora automatically provisions and maintains them synchronously. The primary DB instance is synchronously replicated across Availability Zones to Aurora Replicas to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB cluster with high availability can enhance availability during
planned system maintenance, and help protect your databases against failure and Availability Zone disruption.

For more information, see High availability for Amazon Aurora (p. 55).
Infrastructure security in Amazon Aurora

As a managed service, Amazon RDS is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of security processes whitepaper.

You use AWS published API calls to access Amazon Aurora through the network. Clients must support Transport Layer Security (TLS) 1.0. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

In addition, Aurora offers features to help support infrastructure security.

Security groups

Security groups control the access that traffic has in and out of a DB instance. By default, network access is turned off to a DB instance. You can specify rules in a security group that allow access from an IP address range, port, or security group. After ingress rules are configured, the same rules apply to all DB instances that are associated with that security group.

For more information, see Controlling access with security groups (p. 1274).

Public accessibility

When you launch a DB instance inside a virtual private cloud (VPC) based on the Amazon VPC service, you can turn on or off public accessibility for that instance. To designate whether the DB instance that you create has a DNS name that resolves to a public IP address, you use the Public accessibility parameter. By using this parameter, you can designate whether there is public access to the DB instance. You can modify a DB instance to turn on or off public accessibility by modifying the Public accessibility parameter.

For more information, see Hiding a DB instance in a VPC from the internet (p. 1293).

Note

If your DB instance is in a VPC but isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 1221).
Amazon Aurora and interface VPC endpoints (AWS PrivateLink)

You can establish a private connection between your VPC and Amazon RDS API endpoints by creating an *interface VPC endpoint*. Interface endpoints are powered by AWS PrivateLink.

AWS PrivateLink enables you to privately access Amazon Aurora API operations without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with Amazon RDS API endpoints to launch, modify, or terminate DB clusters. Your instances also don't need public IP addresses to use any of the available RDS API operations. Traffic between your VPC and Amazon Aurora doesn't leave the Amazon network.

Each interface endpoint is represented by one or more elastic network interfaces in your subnets. For more information on elastic network interfaces, see Elastic network interfaces in the Amazon EC2 User Guide.

For more information about VPC endpoints, see Interface VPC endpoints (AWS PrivateLink) in the Amazon VPC User Guide. For more information about RDS API operations, see Amazon RDS API Reference.

Considerations for Amazon Aurora VPC endpoints

Before you set up an interface VPC endpoint for Amazon RDS API endpoints, ensure that you review Interface endpoint properties and limitations in the Amazon VPC User Guide.

Amazon Aurora supports making calls to all of its API actions from your VPC.

VPC endpoint policies are supported for Amazon Aurora. By default, full access to Amazon Aurora is allowed through the endpoint. For more information, see Controlling access to services with VPC endpoints in the Amazon VPC User Guide.

Availability

Amazon Aurora currently supports VPC endpoints in the following AWS Regions:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
Creating an interface VPC endpoint for Amazon Aurora

You can create a VPC endpoint for the Amazon RDS API using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see Creating an interface endpoint in the Amazon VPC User Guide.

Create a VPC endpoint for Amazon Aurora using the service name `com.amazonaws.region.rds`.

Excluding AWS Regions in China, if you enable private DNS for the endpoint, you can make API requests to Amazon Aurora with the VPC endpoint using its default DNS name for the AWS Region, for example `rds.us-east-1.amazonaws.com`. For the China (Beijing) and China (Ningxia) AWS Regions, you can make API requests with the VPC endpoint using `rds-api.cn-north-1.amazonaws.com.cn` and `rds-api.cn-northwest-1.amazonaws.com.cn`, respectively.

For more information, see Accessing a service through an interface endpoint in the Amazon VPC User Guide.

Creating a VPC endpoint policy for Amazon Aurora

You can attach an endpoint policy to your VPC endpoint that controls access to Amazon Aurora. The policy specifies the following information:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

For more information, see Controlling access to services with VPC endpoints in the Amazon VPC User Guide.

Example: VPC endpoint policy for Amazon Aurora actions

The following is an example of an endpoint policy for Amazon Aurora. When attached to an endpoint, this policy grants access to the listed Amazon Aurora actions for all principals on all resources.

```
{
    "Statement": [
        {
            "Principal": "*",
            "Effect": "Allow",
            "Action": [
                "rds:CreateDBInstance",
                "rds:ModifyDBInstance"
            ]
        }
    ]
}
```
Security best practices for Amazon Aurora

Use AWS Identity and Access Management (IAM) accounts to control access to Amazon RDS API operations, especially operations that create, modify, or delete Amazon Aurora resources. Such resources include DB clusters, security groups, and parameter groups. Also use IAM to control actions that perform common administrative actions such as backing up and restoring DB clusters.

- Create an individual IAM user for each person who manages Amazon Aurora resources, including yourself. Don’t use AWS root credentials to manage Amazon Aurora resources.
- Grant each user the minimum set of permissions required to perform his or her duties.
- Use IAM groups to effectively manage permissions for multiple users.
- Rotate your IAM credentials regularly.
- Configure AWS Secrets Manager to automatically rotate the secrets for Amazon Aurora. For more information, see Rotating your AWS Secrets Manager secrets in the AWS Secrets Manager User Guide. You can also retrieve the credential from AWS Secrets Manager programmatically. For more information, see Retrieving the secret value in the AWS Secrets Manager User Guide.

For more information about IAM, see AWS Identity and Access Management. For information on IAM best practices, see IAM best practices.

Use the AWS Management Console, the AWS CLI, or the RDS API to change the password for your master user. If you use another tool, such as a SQL client, to change the master user password, it might result in privileges being revoked for the user unintentionally.
Controlling access with security groups

Security groups control the access that traffic has in and out of a DB instance. Aurora supports VPC security groups.

VPC security groups

Each VPC security group rule enables a specific source to access a DB instance in a VPC that is associated with that VPC security group. The source can be a range of addresses (for example, 203.0.113.0/24), or another VPC security group. By specifying a VPC security group as the source, you allow incoming traffic from all instances (typically application servers) that use the source VPC security group. VPC security groups can have rules that govern both inbound and outbound traffic, though the outbound traffic rules typically do not apply to DB instances. Outbound traffic rules only apply if the DB instance acts as a client. You must use the Amazon EC2 API or the Security Group option on the VPC Console to create VPC security groups.

When you create rules for your VPC security group that allow access to the instances in your VPC, you must specify a port for each range of addresses that the rule allows access for. For example, if you want to enable SSH access to instances in the VPC, then you create a rule allowing access to TCP port 22 for the specified range of addresses.

You can configure multiple VPC security groups that allow access to different ports for different instances in your VPC. For example, you can create a VPC security group that allows access to TCP port 80 for web servers in your VPC. You can then create another VPC security group that allows access to TCP port 3306 for Aurora MySQL DB instances in your VPC.

Note

In an Aurora DB cluster, the VPC security group associated with the DB cluster is also associated with all of the DB instances in the DB cluster. If you change the VPC security group for the DB cluster or for a DB instance, the change is applied automatically to all of the DB instances in the DB cluster.

For more information on VPC security groups, see Security groups in the Amazon Virtual Private Cloud User Guide.

Note

If your DB cluster is in a VPC but isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 1221).

Security group scenario

A common use of a DB instance in a VPC is to share data with an application server running in an Amazon EC2 instance in the same VPC, which is accessed by a client application outside the VPC. For this scenario, you use the RDS and VPC pages on the AWS Management Console or the RDS and EC2 API operations to create the necessary instances and security groups:

1. Create a VPC security group (for example, sg-appsrv1) and define inbound rules that use the IP addresses of the client application as the source. This security group allows your client application to connect to EC2 instances in a VPC that uses this security group.
2. Create an EC2 instance for the application and add the EC2 instance to the VPC security group (sg-appsrv1) that you created in the previous step. The EC2 instance in the VPC shares the VPC security group with the DB instance.
3. Create a second VPC security group (for example, sg-dbsrv1) and create a new rule by specifying the VPC security group that you created in step 1 (sg-appsrv1) as the source.
4. Create a new DB instance and add the DB instance to the VPC security group (sg-dbsrv1) that you created in the previous step. When you create the DB instance, use the same port number as the one specified for the VPC security group (sg-dbsrv1) rule that you created in step 3.

The following diagram shows this scenario.

For more information about using a VPC, see Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281).

**Creating a VPC security group**

You can create a VPC security group for a DB instance by using the VPC console. For information about creating a security group, see Provide access to the DB cluster in the VPC by creating a security group (p. 76) and Security groups in the Amazon Virtual Private Cloud User Guide.

**Associating a security group with a DB instance**

You can associate a security group with a DB instance by using **Modify** on the RDS console, the ModifyDBInstance Amazon RDS API, or the modify-db-instance AWS CLI command.

For information about modifying a DB instance in a DB cluster, see Modify a DB instance in a DB cluster (p. 328). For security group considerations when you restore a DB instance from a DB snapshot, see Security group considerations (p. 420).

**Associating a security group with a DB cluster**

You can associate a security group with a DB cluster by using **Modify cluster** on the RDS console, the ModifyDBCluster Amazon RDS API, or the modify-db-cluster AWS CLI command.

For information about modifying a DB cluster, see Modifying an Amazon Aurora DB cluster (p. 327).
Master user account privileges

When you create a new DB cluster, the default master user that you use gets certain privileges for that DB cluster. The following table shows the privileges and database roles the master user gets for each of the database engines.

**Important**
We strongly recommend that you do not use the master user directly in your applications. Instead, adhere to the best practice of using a database user created with the minimal privileges required for your application.

**Note**
If you accidentally delete the permissions for the master user, you can restore them by modifying the DB cluster and setting a new master user password. For more information about modifying a DB cluster, see Modifying an Amazon Aurora DB cluster (p. 327).

<table>
<thead>
<tr>
<th>Database engine</th>
<th>System privilege</th>
<th>Database role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Aurora</td>
<td>CREATE, DROP, GRANT OPTION, REFERENCES, EVENT, ALTER, DELETE, INDEX, INSERT, SELECT, UPDATE, CREATE TEMPORARY TABLES, LOCK TABLES, TRIGGER, CREATE VIEW, SHOW VIEW, LOAD FROM S3, SELECT INTO S3, ALTER ROUTINE, CREATE ROUTINE, EXECUTE, CREATE USER, PROCESS, SHOW DATABASES, RELOAD, REPLICATION CLIENT, REPLICATION SLAVE</td>
<td>—</td>
</tr>
<tr>
<td>MySQL</td>
<td>LOGIN, NOSUPERUSER, INHERIT, CREATEDB, CREATEROLE, NOREPLICATION, VALID UNTIL 'infinity'</td>
<td>RDS_SUPERUSER</td>
</tr>
<tr>
<td>Amazon Aurora PostgreSQL</td>
<td>LOGIN, NOSUPERUSER, INHERIT, CREATEDB, CREATEROLE, NOREPLICATION, VALID UNTIL 'infinity'</td>
<td>RDS_SUPERUSER</td>
</tr>
</tbody>
</table>
Using service-linked roles for Amazon Aurora

Amazon Aurora uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon Aurora. Service-linked roles are predefined by Amazon Aurora and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes using Amazon Aurora easier because you don’t have to manually add the necessary permissions. Amazon Aurora defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Aurora can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete the roles only after first deleting their related resources. This protects your Amazon Aurora resources because you can’t inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have Yes in the Service-Linked Role column. Choose a Yes with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Amazon Aurora

Amazon Aurora uses the service-linked role named AWSServiceRoleForRDS – to allow Amazon RDS to call AWS services on behalf of your DB clusters.

The AWSServiceRoleForRDS service-linked role trusts the following services to assume the role:

- rds.amazonaws.com

The role permissions policy allows Amazon Aurora to complete the following actions on the specified resources:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource": "*
```
Note
You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. If you encounter the following error message:
Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.
Make sure you have the following permissions enabled:

```json
{
  "Action": "iam:CreateServiceLinkedRole",
  "Effect": "Allow",
  "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
}```
Creating a service-linked role for Amazon Aurora

You don't need to manually create a service-linked role. When you create a DB cluster, Amazon Aurora creates the service-linked role for you.

**Important**

If you were using the Amazon Aurora service before December 1, 2017, when it began supporting service-linked roles, then Amazon Aurora created the AWSServiceRoleForRDS role in your account. To learn more, see A new role appeared in my AWS account.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a DB cluster, Amazon Aurora creates the service-linked role for you again.

Editing a service-linked role for Amazon Aurora

Amazon Aurora does not allow you to edit the AWSServiceRoleForRDS service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

Deleting a service-linked role for Amazon Aurora

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must delete all of your DB clusters before you can delete the service-linked role.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first confirm that the role has no active sessions and remove any resources used by the role.

**To check whether the service-linked role has an active session in the IAM console**

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the IAM console, choose Roles. Then choose the name (not the check box) of the AWSServiceRoleForRDS role.
3. On the Summary page for the chosen role, choose the Access Advisor tab.
4. On the Access Advisor tab, review recent activity for the service-linked role.

**Note**

If you are unsure whether Amazon Aurora is using the AWSServiceRoleForRDS role, you can try to delete the role. If the service is using the role, then the deletion fails and you can view the AWS Regions where the role is being used. If the role is being used, then you must wait.
for the session to end before you can delete the role. You cannot revoke the session for a
service-linked role.

If you want to remove the AWSServiceRoleForRDS role, you must first delete all of your DB clusters.

Deleting all of your clusters

Use one of the following procedures to delete a single cluster. Repeat the procedure for each of your
clusters.

To delete a cluster (console)

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the Databases list, choose the cluster that you want to delete.
3. For Cluster Actions, choose Delete.
4. Choose Delete.

To delete a cluster (CLI)

See delete-db-cluster in the AWS CLI Command Reference.

To delete a cluster (API)

See DeleteDBCluster in the Amazon RDS API Reference.

You can use the IAM console, the IAM CLI, or the IAM API to delete the AWSServiceRoleForRDS service-
linked role. For more information, see Deleting a service-linked role in the IAM User Guide.
Amazon Virtual Private Cloud VPCs and Amazon Aurora

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources, such as Aurora DB clusters, into a virtual private cloud (VPC).

When you use an Amazon VPC, you have control over your virtual networking environment: you can choose your own IP address range, create subnets, and configure routing and access control lists. There is no additional cost to run your DB instance in an Amazon VPC.

Accounts that support only the EC2-VPC platform have a default VPC. All new DB instances are created in the default VPC unless you specify otherwise. If you are a new Amazon Aurora customer, if you have never created a DB instance before, or if you are creating a DB instance in an AWS Region you have not used before, you are most likely on the EC2-VPC platform and have a default VPC.

Topics
- How to create a VPC for use with Amazon Aurora (p. 1281)
- Scenarios for accessing a DB instance in a VPC (p. 1288)
- Working with a DB instance in a VPC (p. 1291)
- Tutorial: Create an Amazon VPC for use with a DB instance (p. 1298)

This documentation only discusses VPC functionality relevant to Amazon Aurora DB clusters. For more information about Amazon VPC, see Amazon VPC Getting Started Guide and Amazon VPC User Guide. For information about using a network address translation (NAT) gateway, see NAT gateways in the Amazon Virtual Private Cloud User Guide.

How to create a VPC for use with Amazon Aurora

The following sections discuss how to create a VPC for use with Amazon Aurora.

Note
For a helpful and detailed guide on connecting to an Amazon Aurora DB cluster, you can see Aurora MySQL database administrator’s handbook – Connection management.

Create a VPC and subnets

You can only create an Amazon Aurora DB cluster in a Virtual Private Cloud (VPC) that spans two Availability Zones, and each zone must contain at least one subnet. You can create an Aurora DB cluster
in the default VPC for your AWS account, or you can create a user-defined VPC. For information, see Amazon Virtual Private Cloud VPCs and Amazon Aurora (p. 1281).

Amazon Aurora optionally can create a VPC and subnet group for you to use with your DB cluster. Doing this can be helpful if you have never created a VPC, or if you would like to create a new VPC that is separate from your other VPCs. If you want Amazon Aurora to create a VPC and subnet group for you, then skip this procedure and see Create an Aurora MySQL DB cluster (p. 78).

**Note**
All VPC and EC2 resources that you use with your Aurora DB cluster must be in one of the regions listed in Regions and Availability Zones (p. 5).

**To create a VPC for use with an Aurora DB cluster**

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the top-right corner of the AWS Management Console, choose the AWS Region to create your VPC in. This example uses the US East (Ohio) Region.
3. In the upper-left corner, choose VPC Dashboard. Choose Start VPC Wizard to begin creating a VPC.
4. In the Create VPC wizard, choose VPC with a Single Public Subnet. Choose Select.

![Select VPC with a Single Public Subnet](image)

5. Set the following values in the Create VPC panel:
   - **IP CIDR block**: 10.0.0.0/16
   - **VPC name**: gs-cluster-vpc
   - **Public subnet**: 10.0.0.0/24
   - **Availability Zone**: us-east-1a
   - **Subnet name**: gs-subnet1
   - **Enable DNS hostnames**: Yes
   - **Hardware tenancy**: Default
6. Choose **Create VPC**.

7. When your VPC has been created, choose **Close** on the notification page.

**To create additional subnets**

1. To add the second subnet to your VPC, in the VPC Dashboard choose **Subnets**, and then choose **Create Subnet**. An Amazon Aurora DB cluster requires at least two VPC subnets.

2. Set the following values in the **Create Subnet** panel:
   - **Name tag**: `gs-subnet2`
   - **VPC**: Choose the VPC that you created in the previous step, for example: `vpc-a464d1c1 (10.0.0.0/16) | gs-cluster-vpc`.
   - **Availability Zone**: `us-east-1c`
   - **CIDR block**: `10.0.1.0/24`
3. Choose Yes Create.

4. To ensure that the second subnet that you created uses the same route table as the first subnet, in the VPC Dashboard, choose Subnets, and then choose the first subnet that was created for the VPC, gs-subnet1. Choose the Route Table tab, and note the Current Route Table, for example: rtb-c16ce5bc.

5. In the list of subnets, clear the first subnet and choose the second subnet, gs-subnet2. Choose the Route Table tab, and then choose Edit. In the Change to list, choose the route table from the previous step, for example: rtb-c16ce5bc. Choose Save to save your choice.

Create a security group and add inbound rules

After you've created your VPC and subnets, the next step is to create a security group and add inbound rules.

To create a security group

The last step in creating a VPC for use with your Amazon Aurora DB cluster is to create a VPC security group, which identifies which network addresses and protocols are allowed to access DB instances in your VPC.

1. In the VPC Dashboard, choose Security Groups, and then choose Create Security Group.
2. Set the following values in the Create Security Group panel:
• **Name tag:** gs-securitygroup1
• **Group name:** gs-securitygroup1
• **Description:** Getting Started Security Group
• **VPC:** Choose the VPC that you created earlier, for example: vpc-b5754bcd | gs-cluster-vpc.

3. Choose **Yes, Create** to create the security group.

**To add inbound rules to the security group**

To connect to your Aurora DB cluster, you need to add an inbound rule to your VPC security group that allows inbound traffic to connect.

1. Determine the IP address to use to connect to the Aurora cluster. You can use the service at [https://checkip.amazonaws.com](https://checkip.amazonaws.com) to determine your public IP address. If you are connecting through an ISP or from behind your firewall without a static IP address, you need to find out the range of IP addresses used by client computers.

   **Warning**
   
   If you use 0.0.0.0/0, you enable all IP addresses to access your DB cluster. This is acceptable for a short time in a test environment, but it's unsafe for production environments. In production, you'll authorize only a specific IP address or range of addresses to access your DB cluster.

2. In the VPC Dashboard, choose **Security Groups**, and then choose the gs-securitygroup1 security group that you created in the previous procedure.

3. Choose the **Inbound** tab, and then choose the **Edit** button.

4. Set the following values for your new inbound rule:
   • **Type:** All Traffic
   • **Source:** The IP address or range from the previous step, for example 203.0.113.25/32.

5. Choose **Save** to save your settings.
Create a DB subnet group

The last thing that you need before you can create an Aurora DB cluster is a DB subnet group. Your DB subnet group identifies the subnets that your DB cluster uses from the VPC that you created in the previous steps. Your DB subnet group must include at least one subnet in at least two of the Availability Zones in the AWS Region where you want to deploy your DB cluster.

To create a DB subnet group for use with your Aurora DB cluster

1. Open the Amazon Aurora console at https://console.aws.amazon.com/rds.
2. Choose Subnet Groups, and then choose Create DB Subnet Group.
3. Set the following values for your new DB subnet group:
   - **Name**: gs-subnetgroup1
   - **Description**: Getting Started Subnet Group
   - **VPC ID**: Choose the VPC that you created in the previous procedure, for example, gs-cluster-vpc (vpc-b5754bcd).
4. In the Add subnets section, choose the Availability Zones that include the subnets from Availability Zones, and then choose the subnets from Subnets.
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.

![Name field](gs-subnetgroup1)

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

**Description**

Getting Started 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.

![VPC field](gs-cluster-vpc (vpc-068fe388385af014))

**Add subnets**

**Availability Zones**
Choose the Availability Zones that include the subnets you want to add.

- 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.

- subnet-079bd4b8953aee1cd (10.0.0.0/24)
- subnet-057e85b72c46fdd9a (10.0.1.0/24)

**Subnets selected (2)**

<table>
<thead>
<tr>
<th>Availability zone</th>
<th>Subnet ID</th>
<th>CIDR block</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-1a</td>
<td>subnet-079bd4b8953aee1cd</td>
<td>10.0.0.0/24</td>
</tr>
<tr>
<td>us-east-1c</td>
<td>subnet-057e85b72c46fdd9a</td>
<td>10.0.1.0/24</td>
</tr>
</tbody>
</table>
5. Choose **Create** to create the subnet group.

### Scenarios for accessing a DB instance in a VPC

Amazon Aurora supports the following scenarios for accessing a DB instance:

- An EC2 instance in the same VPC (p. 1288)
- An EC2 instance in a different VPC (p. 1289)
- An EC2 instance not in a VPC (p. 1290)
- A client application through the internet (p. 1291)

**Note**

If your DB cluster is in a VPC but isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see [Internetwork traffic privacy](p. 1221).

### A DB instance in a VPC accessed by an EC2 instance in the same VPC

A common use of a DB instance in a VPC is to share data with an application server that is running in an EC2 instance in the same VPC. This is the user scenario created if you use AWS Elastic Beanstalk to create an EC2 instance and a DB instance in the same VPC.

The following diagram shows this scenario.

![Diagram](image)

The simplest way to manage access between EC2 instances and DB instances in the same VPC is to do the following:

- Create a VPC security group for your DB instances to be in. This security group can be used to restrict access to the DB instances. For example, you can create a custom rule for this security group that allows TCP access using the port you assigned to the DB instance when you created it and an IP address you use to access the DB instance for development or other purposes.
- Create a VPC security group for your EC2 instances (web servers and clients) to be in. This security group can, if needed, allow access to the EC2 instance from the internet by using the VPC's routing table. For example, you can set rules on this security group to allow TCP access to the EC2 instance over port 22.

- Create custom rules in the security group for your DB instances that allow connections from the security group you created for your EC2 instances. This would allow any member of the security group to access the DB instances.

For a tutorial that shows you how to create a VPC with both public and private subnets for this scenario, see Tutorial: Create an Amazon VPC for use with a DB instance (p. 1298).

**To create a rule in a VPC security group that allows connections from another security group, do the following:**

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc.
2. In the navigation pane, choose **Security Groups**.
3. Choose or create a security group for which you want to allow access to members of another security group. In the scenario preceding, this is the security group that you use for your DB instances. Choose the **Inbound Rules** tab, and then choose **Edit rule**.
4. On the **Edit inbound rules** page, choose **Add Rule**.
5. From **Type**, choose the entry that corresponds to the port you used when you created your DB instance, such as **MYSQL/Aurora**.
6. In the **Source** box, start typing the ID of the security group, which lists the matching security groups. Choose the security group with members that you want to have access to the resources protected by this security group. In the scenario preceding, this is the security group that you use for your EC2 instance.
7. If required, repeat the steps for the TCP protocol by creating a rule with **All TCP** as the **Type** and your security group in the **Source** box. If you intend to use the UDP protocol, create a rule with **All UDP** as the **Type** and your security group in the **Source** box.
8. Choose **Save** when you are done.

The following screen shows several inbound rules.

![](image)

**A DB instance in a VPC accessed by an EC2 instance in a different VPC**

When your DB instance is in a different VPC from the EC2 instance you are using to access it, you can use VPC peering to access the DB instance.

The following diagram shows this scenario.
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region. To learn more about VPC peering, see VPC peering in the Amazon Virtual Private Cloud User Guide.

A DB instance in a VPC accessed by an EC2 instance not in a VPC

You can communicate between an Amazon Aurora DB instance that is in a VPC and an EC2 instance that is not in an Amazon VPC by using ClassicLink. When you use ClassicLink, an application on the EC2 instance can connect to the DB instance by using the endpoint for the DB instance. ClassicLink is available at no charge.

The following diagram shows this scenario.

Using ClassicLink, you can connect an EC2 instance to a logically isolated database where you define the IP address range and control the access control lists (ACLs) to manage network traffic. You don’t have to use public IP addresses or tunneling to communicate with the DB instance in the VPC. This arrangement provides you with higher throughput and lower latency connectivity for inter-instance communications.

To enable ClassicLink between a DB instance in a VPC and an EC2 instance not in a VPC

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc.
2. In the navigation pane, choose Your VPCs.
3. Choose the VPC used by the DB instance.
4. In Actions, choose Enable ClassicLink. In the confirmation dialog box, choose Yes, Enable.
5. On the EC2 console, choose the EC2 instance you want to connect to the DB instance in the VPC.
6. In Actions, choose ClassicLink, and then choose Link to VPC.
7. On the Link to VPC page, choose the security group you want to use, and then choose Link to VPC.

Note
The ClassicLink features are only visible in the consoles for accounts and regions that support EC2-Classic. For more information, see ClassicLink in the Amazon EC2 User Guide for Linux Instances.

A DB instance in a VPC accessed by a client application through the internet

To access a DB instance in a VPC from a client application through the internet, you configure a VPC with a single public subnet, and an internet gateway to enable communication over the internet.

The following diagram shows this scenario.

We recommend the following configuration:

- A VPC of size /16 (for example CIDR: 10.0.0.0/16). This size provides 65,536 private IP addresses.
- A subnet of size /24 (for example CIDR: 10.0.0.0/24). This size provides 256 private IP addresses.
- An Amazon Aurora DB instance that is associated with the VPC and the subnet. Amazon RDS assigns an IP address within the subnet to your DB instance.
- An internet gateway which connects the VPC to the internet and to other AWS products.
- A security group associated with the DB instance. The security group's inbound rules allow your client application to access to your DB instance.

For information about creating a DB instance in a VPC, see Creating a DB instance in a VPC (p. 1294).

Working with a DB instance in a VPC

Your DB instance is in a virtual private cloud (VPC). A VPC is a virtual network that is logically isolated from other virtual networks in the AWS Cloud. Amazon VPC lets you launch AWS resources, such as an Amazon Aurora DB instance or Amazon EC2 instance, into a VPC. The VPC can either be a default VPC that comes with your account or one that you create. All VPCs are associated with your AWS account.
Your default VPC has three subnets you can use to isolate resources inside the VPC. The default VPC also
has an internet gateway that can be used to provide access to resources inside the VPC from outside the
VPC.

For a list of scenarios involving Amazon Aurora DB instances in a VPC, see Scenarios for accessing a DB
instance in a VPC (p. 1288).

For a tutorial that shows you how to create a VPC that you can use with a common Amazon Aurora
scenario, see Tutorial: Create an Amazon VPC for use with a DB instance (p. 1298).

To learn how to work with DB instances inside a VPC, see the following:

Topics
- Working with a DB instance in a VPC (p. 1292)
- Working with DB subnet groups (p. 1292)
- Hiding a DB instance in a VPC from the internet (p. 1293)
- Creating a DB instance in a VPC (p. 1294)

Working with a DB instance in a VPC

Here are some tips on working with a DB instance in a VPC:

- Your VPC must have at least two subnets. These subnets must be in two different Availability Zones
  in the AWS Region where you want to deploy your DB instance. A subnet is a segment of a VPC's
  IP address range that you can specify and that lets you group instances based on your security and
  operational needs.
- If you want your DB instance in the VPC to be publicly accessible, you must enable the VPC attributes
  DNS hostnames and DNS resolution.
- Your VPC must have a DB subnet group that you create (for more information, see the next section).
  You create a DB subnet group by specifying the subnets you created. Amazon Aurora uses that DB
  subnet group and your preferred Availability Zone to choose a subnet and an IP address within that
  subnet to assign to your DB instance.
- Your VPC must have a VPC security group that allows access to the DB instance.
- The CIDR blocks in each of your subnets must be large enough to accommodate spare IP addresses for
  Amazon Aurora to use during maintenance activities, including failover and compute scaling.
- A VPC can have an instance tenancy attribute of either default or dedicated. All default VPCs have the
  instance tenancy attribute set to default, and a default VPC can support any DB instance class.

If you choose to have your DB instance in a dedicated VPC where the instance tenancy attribute is
set to dedicated, the DB instance class of your DB instance must be one of the approved Amazon EC2
dedicated instance types. For example, the m3.medium EC2 dedicated instance corresponds to the
db.m3.medium DB instance class. For information about instance tenancy in a VPC, see Dedicated
instances in the Amazon Elastic Compute Cloud User Guide.

For more information about the instance types that can be in a dedicated instance, see Amazon EC2
dedicated instances on the EC2 pricing page.

Note
When you set the instance tenancy attribute to dedicated for an Amazon RDS DB instance, it
doesn't guarantee that the DB instance will run on a dedicated host.

Working with DB subnet groups

Subnets are segments of a VPC's IP address range that you designate to group your resources based
on security and operational needs. A DB subnet group is a collection of subnets (typically private) that
you create in a VPC and that you then designate for your DB instances. A DB subnet group allows you to specify a particular VPC when creating DB instances using the CLI or API; if you use the console, you can just choose the VPC and subnets you want to use.

Each DB subnet group should have subnets in at least two Availability Zones in a given AWS Region. When creating a DB instance in a VPC, you must choose a DB subnet group. Amazon Aurora uses that DB subnet group and your preferred Availability Zone to choose a subnet and an IP address within that subnet to associate with your DB instance. If the primary DB instance of a Multi-AZ deployment fails, Amazon Aurora can promote the corresponding standby and subsequently create a new standby using an IP address of the subnet in one of the other Availability Zones.

The subnets in a DB subnet group are either public or private. They can’t be a mix of both public and private subnets. The subnets are public or private, depending on the configuration that you set for their network access control lists (network ACLs) and routing tables.

When Amazon Aurora creates a DB instance in a VPC, it assigns a network interface to your DB instance by using an IP address from your DB subnet group. However, we strongly recommend that you use the DNS name to connect to your DB instance because the underlying IP address changes during failover.

Note
For each DB instance that you run in a VPC, make sure to reserve at least one address in each subnet in the DB subnet group for use by Amazon Aurora for recovery actions.

Hiding a DB instance in a VPC from the internet

One common Amazon Aurora scenario is to have a VPC in which you have an EC2 instance with a public-facing web application and a DB instance with a database that is not publicly accessible. For example, you can create a VPC that has a public subnet and a private subnet. Amazon EC2 instances that function as web servers can be deployed in the public subnet, and the DB instances are deployed in the private subnet. In such a deployment, only the web servers have access to the DB instances. For an illustration of this scenario, see A DB instance in a VPC accessed by an EC2 instance in the same VPC (p. 1288).

When you launch a DB instance inside a VPC, the DB instance has a private IP address for traffic inside the VPC. This private IP address isn’t publicly accessible. You can use the Public access option to designate whether the DB instance also has a public IP address in addition to the private IP address. If the DB instance is designated as publicly accessible, its DNS endpoint resolves to the private IP address from within the DB instance’s VPC, and to the public IP address from outside of the DB instance’s VPC. Access to the DB instance is ultimately controlled by the security group it uses, and that public access is not permitted if the security group assigned to the DB instance doesn’t permit it.

You can modify a DB instance to turn on or off public accessibility by modifying the Public access option. For more information, see the modifying section for your DB engine.

The following illustration shows the Public access option in the Additional connectivity configuration section. To set the option, open the Additional connectivity configuration section in the Connectivity section.
For information about modifying a DB instance to set the Public access option, see Modify a DB instance in a DB cluster (p. 328).

**Note**
If your DB instance isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 1221).

**Creating a DB instance in a VPC**

The following procedures help you create a DB instance in a VPC. If your account has a default VPC, you can begin with step 3 because the VPC and DB subnet group have already been created for you. If your AWS account doesn't have a default VPC, or if you want to create an additional VPC, you can create a new VPC.

**Note**
If you want your DB instance in the VPC to be publicly accessible, you must update the DNS information for the VPC by enabling the VPC attributes DNS hostnames and DNS resolution. For
information about updating the DNS information for a VPC instance, see Updating DNS support for your VPC.

Follow these steps to create a DB instance in a VPC:

- **Step 1: Create a VPC (p. 1295)**
- **Step 2: Add subnets to the VPC (p. 1295)**
- **Step 3: Create a DB subnet group (p. 1295)**
- **Step 4: Create a VPC security group (p. 1297)**
- **Step 5: Create a DB instance in the VPC (p. 1297)**

**Step 1: Create a VPC**

If your AWS account does not have a default VPC or if you want to create an additional VPC, follow the instructions for creating a new VPC. See Create a VPC with private and public subnets (p. 1298), or see Step 1: Create a VPC in the Amazon VPC documentation.

**Step 2: Add subnets to the VPC**

Once you have created a VPC, you need to create subnets in at least two Availability Zones. You use these subnets when you create a DB subnet group. If you have a default VPC, a subnet is automatically created for you in each Availability Zone in the AWS Region.

For instructions on how to create subnets in a VPC, see Create a VPC with private and public subnets (p. 1298).

**Step 3: Create a DB subnet group**

A DB subnet group is a collection of subnets (typically private) that you create for a VPC and that you then designate for your DB instances. A DB subnet group allows you to specify a particular VPC when you create DB instances using the CLI or API. If you use the console, you can just choose the VPC and subnets you want to use. Each DB subnet group must have at least one subnet in at least two Availability Zones in the AWS Region.

For a DB instance to be publicly accessible, the subnets in the DB subnet group must have an internet gateway. For more information about internet gateways for subnets, see Internet gateways in the Amazon VPC documentation.

When you create a DB instance in a VPC, make sure to choose a DB subnet group. Amazon Aurora then uses that DB subnet group and your preferred Availability Zone to choose a subnet and an IP address within that subnet. Amazon Aurora creates and associates an Elastic Network Interface to your DB instance with that IP address. For Multi-AZ deployments, defining a subnet for two or more Availability Zones in an AWS Region allows Amazon Aurora to create a new standby in another Availability Zone should the need arise. You need to do this even for Single-AZ deployments, just in case you want to convert them to Multi-AZ deployments at some point.

In this step, you create a DB subnet group and add the subnets that you created for your VPC.

**To create a DB subnet group**

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Subnet groups**.
3. Choose **Create DB Subnet Group**.
4. For **Name**, type the name of your DB subnet group.
5. For **Description**, type a description for your DB subnet group.

6. For **VPC**, choose the VPC that you created.

7. In the **Add subnets** section, choose the Availability Zones that include the subnets from **Availability Zones**, and then choose the subnets from **Subnets**.

8. Choose **Create**.

Your new DB subnet group appears in the DB subnet groups list on the RDS console. You can choose the DB subnet group to see details, including all of the subnets associated with the group, in the details pane at the bottom of the window.
Step 4: Create a VPC security group

Before you create your DB instance, you must create a VPC security group to associate with your DB instance. For instructions on how to create a security group for your DB instance, see Create a VPC security group for a private DB instance (p. 1301), or see Security groups for your VPC in the Amazon VPC documentation.

Step 5: Create a DB instance in the VPC

In this step, you create a DB instance and use the VPC name, the DB subnet group, and the VPC security group you created in the previous steps.

Note

If you want your DB instance in the VPC to be publicly accessible, you must enable the VPC attributes DNS hostnames and DNS resolution. For information on updating the DNS information for a VPC instance, see Updating DNS support for your VPC.

For details on how to create a DB instance, see Creating an Amazon Aurora DB cluster (p. 118).

When prompted in the Network & Security section, enter the VPC name, the DB subnet group, and the VPC security group you created in the previous steps.

Note

Updating VPCs is not currently supported for Aurora clusters.
Tutorial: Create an Amazon VPC for use with a DB instance

A common scenario includes a DB instance in an Amazon VPC, that shares data with a web server that is running in the same VPC. In this tutorial you create the VPC for this scenario.

The following diagram shows this scenario. For information about other scenarios, see Scenarios for accessing a DB instance in a VPC (p. 1288).

Because your DB instance only needs to be available to your web server, and not to the public Internet, you create a VPC with both public and private subnets. The web server is hosted in the public subnet, so that it can reach the public Internet. The DB instance is hosted in a private subnet. The web server is able to connect to the DB instance because it is hosted within the same VPC, but the DB instance is not available to the public Internet, providing greater security.

This tutorial describes configuring a VPC for Amazon Aurora DB clusters. For more information about Amazon VPC, see Amazon VPC Getting Started Guide and Amazon VPC User Guide.

Note
For a tutorial that shows you how to create a web server for this VPC scenario, see Tutorial: Create a web server and an Amazon Aurora DB cluster (p. 99).

Create a VPC with private and public subnets

Use the following procedure to create a VPC with both public and private subnets.

To create a VPC and subnets

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the top-right corner of the AWS Management Console, choose the region to create your VPC in. This example uses the US West (Oregon) region.
3. In the upper-left corner, choose VPC Dashboard. To begin creating a VPC, choose Launch VPC Wizard.
4. On the Step 1: Select a VPC Configuration page, choose VPC with Public and Private Subnets, and then choose Select.
5. On the Step 2: VPC with Public and Private Subnets page, set these values:

- **IPv4 CIDR block:** 10.0.0.0/16
- **IPv6 CIDR block:** No IPv6 CIDR Block
- **VPC name:** tutorial-vpc
- **Public subnet's IPv4 CIDR:** 10.0.0.0/24
- **Availability Zone:** us-west-2a
- **Public subnet name:** Tutorial public
- **Private subnet's IPv4 CIDR:** 10.0.1.0/24
- **Availability Zone:** us-west-2a
- **Private subnet name:** Tutorial Private 1
- **Instance type:** t2.small
  
  **Important**
  If you don’t see the **Instance type** box in the console, choose **Use a NAT instance instead**. This link is on the right.

  **Note**
  If the t2.small instance type is not listed, you can choose a different instance type.

- **Key pair name:** No key pair
- **Service endpoints:** Skip this field.
- **Enable DNS hostnames:** Yes
- **Hardware tenancy:** Default

6. When you're finished, choose **Create VPC**.

### Create additional subnets

You must have either two private subnets or two public subnets available to create a DB subnet group for a DB instance to use in a VPC. Because the DB instance for this tutorial is private, add a second private subnet to the VPC.

**To create an additional subnet**

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. To add the second private subnet to your VPC, choose **VPC Dashboard**, choose **Subnets**, and then choose **Create subnet**.
3. On the **Create subnet** page, set these values:

   - **Name tag:** Tutorial private 2
   - **VPC:** Choose the VPC that you created in the previous step, for example: vpc-identifier
     tutorial-vpc
   - **Availability Zone:** us-west-2b
     
     **Note**
     Choose an Availability Zone that is different from the one that you chose for the first private subnet.
   - **IPv4 CIDR block:** 10.0.2.0/24

4. When you’re finished, choose **Create**. Next, choose **Close** on the confirmation page.
5. To ensure that the second private subnet that you created uses the same route table as the first private subnet, complete the following steps:

   a. Choose **VPC Dashboard**, choose **Subnets**, and then choose the first private subnet that you created for the VPC, Tutorial private 1.
b. Below the list of subnets, choose the **Route Table** tab, and note the value for **Route Table**—for example: `rtb-98b613fd`.

c. In the list of subnets, deselect the first private subnet.

d. In the list of subnets, choose the second private subnet *Tutorial private 2*, and choose the **Route Table** tab.

e. If the current route table is not the same as the route table for the first private subnet, choose **Edit route table association**. For **Route Table ID**, choose the route table that you noted earlier—for example: `rtb-98b613fd`. Next, to save your selection, choose **Save**.

## Create a VPC security group for a public web server

Next you create a security group for public access. To connect to public instances in your VPC, you add inbound rules to your VPC security group that allow traffic to connect from the internet.

### To create a VPC security group

1. Open the Amazon VPC console at [https://console.aws.amazon.com/vpc/](https://console.aws.amazon.com/vpc/).
2. Choose **VPC Dashboard**, choose **Security Groups**, and then choose **Create security group**.
3. On the **Create security group** page, set these values:
   - **Security group name**: `tutorial-securitygroup`
   - **Description**: `Tutorial Security Group`
   - **VPC**: Choose the VPC that you created earlier, for example: `vpc-identifier` *(tutorial-vpc)*
4. Add inbound rules to the security group.
   a. Determine the IP address to use to connect to instances in your VPC. To determine your public IP address, in a different browser window or tab, you can use the service at [https://checkip.amazonaws.com](https://checkip.amazonaws.com). An example of an IP address is `203.0.113.25/32`.
      If you are connecting through an Internet service provider (ISP) or from behind your firewall without a static IP address, you need to find out the range of IP addresses used by client computers.

      **Warning**
      If you use `0.0.0.0/0`, you enable all IP addresses to access your public instances. This approach is acceptable for a short time in a test environment, but it's unsafe for production environments. In production, you'll authorize only a specific IP address or range of addresses to access your instances.

   b. In the **Inbound rules** section, choose **Add rule**.
   c. Set the following values for your new inbound rule to allow Secure Shell (SSH) access to your EC2 instance. If you do this, you can connect to your EC2 instance to install the web server and other utilities, and to upload content for your web server.
      - **Type**: SSH
      - **Source**: The IP address or range from Step a, for example: `203.0.113.25/32`.
   d. Choose **Add rule**.
   e. Set the following values for your new inbound rule to allow HTTP access to your web server.
      - **Type**: HTTP
      - **Source**: `0.0.0.0/0`.
   5. To create the security group, choose **Create security group**.

   Note the security group ID because you need it later in this tutorial.
Create a VPC security group for a private DB instance

To keep your DB instance private, create a second security group for private access. To connect to private instances in your VPC, you add inbound rules to your VPC security group that allow traffic from your web server only.

To create a VPC security group

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose VPC Dashboard, choose Security Groups, and then choose Create security group.
3. On the Create security group page, set these values:
   - Security group name: tutorial-db-securitygroup
   - Description: Tutorial DB Instance Security Group
   - VPC: Choose the VPC that you created earlier, for example: vpc-identifier (tutorial-vpc)
4. Add inbound rules to the security group.
   a. In the Inbound rules section, choose Add rule.
   b. Set the following values for your new inbound rule to allow MySQL traffic on port 3306 from your EC2 instance. If you do this, you can connect from your web server to your DB instance to store and retrieve data from your web application to your database.
      - Type: MySQL/Aurora
      - Source: The identifier of the tutorial-securitygroup security group that you created previously in this tutorial, for example: sg-9edd5cfb.
5. To create the security group, choose Create security group.

Create a DB subnet group

A DB subnet group is a collection of subnets that you create in a VPC and that you then designate for your DB instances. A DB subnet group allows you to specify a particular VPC when creating DB instances.

To create a DB subnet group

1. Open the Amazon RDS console at https://console.aws.amazon.com/rds/.
   Note
   Make sure you connect to the Amazon RDS console, not to the Amazon VPC console.
2. In the navigation pane, choose Subnet groups.
3. Choose Create DB Subnet Group.
4. On the Create DB subnet group page, set these values in Subnet group details:
   - Name: tutorial-db-subnet-group
   - Description: Tutorial DB Subnet Group
   - VPC: tutorial-vpc (vpc-identifier)
5. In the Add subnets section, choose the Availability Zones and Subnets.
   For this tutorial, choose us-west-2a and us-west-2b for the Availability Zones. Next, for Subnets, choose the subnets for IPv4 CIDR block 10.0.0.0/24, 10.0.1.0/24, and 10.0.2.0/24.
6. Choose Create.

Your new DB subnet group appears in the DB subnet groups list on the RDS console. You can click the DB subnet group to see details, including all of the subnets associated with the group, in the details pane at the bottom of the window.
Note
If you created this VPC to complete Tutorial: Create a web server and an Amazon Aurora DB cluster (p. 99), create the DB cluster by following the instructions in Create an Amazon Aurora DB cluster (p. 100).
Quotas and constraints for Amazon Aurora

Following, you can find a description of the resource quotas and naming constraints for Amazon Aurora.

Topics

- Quotas in Amazon Aurora (p. 1303)
- Naming constraints in Amazon Aurora (p. 1304)
- Amazon Aurora table size limits (p. 1305)

Quotas in Amazon Aurora

Each AWS account has quotas, for each AWS Region, on the number of Amazon Aurora resources that can be created. After a quota for a resource has been reached, additional calls to create that resource fail with an exception.

The following table lists the resources and their quotas per AWS Region.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorizations per DB security group</td>
<td>20</td>
</tr>
<tr>
<td>Concurrent DB snapshot export tasks</td>
<td>5</td>
</tr>
<tr>
<td>Cross-Region DB snapshot copy requests</td>
<td>5</td>
</tr>
<tr>
<td>Custom endpoints per DB cluster</td>
<td>5</td>
</tr>
<tr>
<td>Data API maximum result set size</td>
<td>1 MB</td>
</tr>
<tr>
<td>Data API requests per second</td>
<td>1000</td>
</tr>
<tr>
<td>DB clusters</td>
<td>40</td>
</tr>
<tr>
<td>DB cluster parameter groups</td>
<td>50</td>
</tr>
<tr>
<td>DB instances</td>
<td>40</td>
</tr>
<tr>
<td>DB subnet groups</td>
<td>50</td>
</tr>
<tr>
<td>Event subscriptions</td>
<td>20</td>
</tr>
<tr>
<td>AWS Identity and Access Management (IAM) roles per DB cluster</td>
<td>5</td>
</tr>
<tr>
<td>IAM roles per DB instance</td>
<td>5</td>
</tr>
<tr>
<td>Manual DB cluster snapshots</td>
<td>100</td>
</tr>
<tr>
<td>Parameter groups</td>
<td>50</td>
</tr>
</tbody>
</table>
### Naming constraints in Amazon Aurora

The following table describes naming constraints in Amazon Aurora.

<table>
<thead>
<tr>
<th>Resource or item</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB cluster identifier</td>
<td>Identifiers have these naming constraints:</td>
</tr>
<tr>
<td></td>
<td>• Must contain 1–63 alphanumeric characters or hyphens.</td>
</tr>
<tr>
<td></td>
<td>• First character must be a letter.</td>
</tr>
<tr>
<td></td>
<td>• Can't end with a hyphen or contain two consecutive hyphens.</td>
</tr>
<tr>
<td></td>
<td>• Must be unique for all DB instances per AWS account, per AWS Region.</td>
</tr>
<tr>
<td>Initial database name</td>
<td>Database name constraints differ between Aurora MySQL and PostgreSQL. For more information, see the available settings when creating each DB cluster.</td>
</tr>
<tr>
<td>Master user name</td>
<td>Master user name constraints differ for each database engine. For more information, see the available settings when creating each DB cluster.</td>
</tr>
<tr>
<td>Master password</td>
<td>The password for the database master user can include any printable ASCII character except /, *, @, or a space. Master password length constraints differ for each database engine. For more information, see the available settings when creating each DB cluster.</td>
</tr>
<tr>
<td>Resource or item</td>
<td>Constraints</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DB parameter group name</td>
<td>These names have these constraints:</td>
</tr>
<tr>
<td></td>
<td>• Must contain 1–255 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>• First character must be a letter.</td>
</tr>
<tr>
<td></td>
<td>• Hyphens are allowed, but the name cannot end with a hyphen or contain two</td>
</tr>
<tr>
<td></td>
<td>consecutive hyphens.</td>
</tr>
<tr>
<td>DB subnet group name</td>
<td>These names have these constraints:</td>
</tr>
<tr>
<td></td>
<td>• Must contain 1–255 characters.</td>
</tr>
<tr>
<td></td>
<td>• Alphanumeric characters, spaces, hyphens, underscores, and periods are</td>
</tr>
<tr>
<td></td>
<td>allowed.</td>
</tr>
</tbody>
</table>

**Amazon Aurora table size limits**

For Aurora MySQL, the maximum table size is 64 tebibytes (TiB). For an Aurora PostgreSQL DB cluster, the maximum table size is 32 tebibytes (TiB). We recommend that you follow table design best practices, such as partitioning of large tables.
Troubleshooting for Aurora

Use the following sections to help troubleshoot problems you have with DB instances in Amazon RDS and Aurora.

Topics
- Can't connect to Amazon RDS DB instance (p. 1306)
- Amazon RDS security issues (p. 1308)
- Resetting the DB instance owner password (p. 1308)
- Amazon RDS DB instance outage or reboot (p. 1308)
- Amazon RDS DB parameter changes not taking effect (p. 1309)
- Amazon Aurora MySQL out of memory issues (p. 1309)
- Amazon Aurora MySQL replication issues (p. 1310)
- No space left on device (p. 1312)

For information about debugging problems using the Amazon RDS API, see Troubleshooting applications on Aurora (p. 1315).

Can't connect to Amazon RDS DB instance

When you can't connect to a DB instance, the following are common causes:

- **Inbound rules** – The access rules enforced by your local firewall and the IP addresses authorized to access your DB instance might not match. The problem is most likely the inbound rules in your security group.

  By default, DB instances don't allow access. Access is granted through a security group associated with the VPC that allows traffic into and out of the DB instance. If necessary, add inbound and outbound rules for your particular situation to the security group. You can specify an IP address, a range of IP addresses, or another VPC security group.

  **Note**
  When adding a new inbound rule, you can choose My IP for Source to allow access to the DB instance from the IP address detected in your browser.

  For more information about setting up security groups, see Provide access to the DB cluster in the VPC by creating a security group (p. 76).

  **Note**
  Client connections from IP addresses within the range 169.254.0.0/16 aren't permitted. This is the Automatic Private IP Addressing Range (APIPA), which is used for local-link addressing.

- **Public accessibility** – To connect to your DB instance from outside of the VPC, such as by using a client application, the instance must have a public IP address assigned to it.

  To make the instance publicly accessible, modify it and choose Yes under Public accessibility. For more information, see Hiding a DB instance in a VPC from the internet (p. 1293).

- **Port** – The port that you specified when you created the DB instance can't be used to send or receive communications due to your local firewall restrictions. To determine if your network allows the specified port to be used for inbound and outbound communication, check with your network administrator.
• **Availability** – For a newly created DB instance, the DB instance has a status of *creating* until the DB instance is ready to use. When the state changes to *available*, you can connect to the DB instance. Depending on the size of your DB instance, it can take up to 20 minutes before an instance is available.

• **Internet gateway** – For a DB instance to be publicly accessible, the subnets in its DB subnet group must have an internet gateway.

**To configure an internet gateway for a subnet**

1. Sign in to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/.
2. In the navigation pane, choose **Databases**, and then choose the name of the DB instance.
3. In the **Connectivity & security** tab, write down the values of the VPC ID under **VPC** and the subnet ID under **Subnets**.
4. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
5. In the navigation pane, choose **Internet Gateways**. Verify that there is an internet gateway attached to your VPC. Otherwise, choose **Create Internet Gateway** to create an internet gateway. Select the internet gateway, and then choose **Attach to VPC** and follow the directions to attach it to your VPC.
6. In the navigation pane, choose **Subnets**, and then select your subnet.
7. On the **Route Table** tab, verify that there is a route with `0.0.0.0/0` as the destination and the internet gateway for your VPC as the target.
   a. Choose the ID of the route table (rtb-xxxxxxx) to navigate to the route table.
   b. On the **Routes** tab, choose **Edit routes**. Choose **Add route**, use `0.0.0.0/0` as the destination and the internet gateway as the target.
   c. Choose **Save routes**.

For more information, see Working with a DB instance in a VPC (p. 1291).

**Testing a connection to a DB instance**

You can test your connection to a DB instance using common Linux or Microsoft Windows tools.

From a Linux or Unix terminal, you can test the connection by entering the following (replace **DB-instance-endpoint** with the endpoint and **port** with the port of your DB instance).

```bash
cn -zv DB-instance-endpoint port
```

For example, the following shows a sample command and the return value.

```bash
cn -zv postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 8299
```

```
Connection to postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 8299 port [tcp/v4r-data] succeeded!
```

Windows users can use Telnet to test the connection to a DB instance. Telnet actions aren't supported other than for testing the connection. If a connection is successful, the action returns no message. If a connection isn't successful, you receive an error message such as the following.

```
C:\>telnet sg-postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 819

Connecting To sg-postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com...Could not open connection to the host, on port 819: Connect failed
```
If Telnet actions return success, your security group is properly configured.

Note
Amazon RDS doesn't accept internet control message protocol (ICMP) traffic, including ping.

Troubleshooting connection authentication

If you can connect to your DB instance but you get authentication errors, you might want to reset the master user password for the DB instance. You can do this by modifying the RDS instance.

Amazon RDS security issues

To avoid security issues, never use your master AWS user name and password for a user account. Best practice is to use your master AWS account to create AWS Identity and Access Management (IAM) users and assign those to DB user accounts. You can also use your master account to create other user accounts, if necessary.

For more information on creating IAM users, see Create an IAM user (p. 73).

Error message "failed to retrieve account attributes, certain console functions may be impaired."

You can get this error for several reasons. It might be because your account is missing permissions, or your account hasn't been properly set up. If your account is new, you might not have waited for the account to be ready. If this is an existing account, you might lack permissions in your access policies to perform certain actions such as creating a DB instance. To fix the issue, your IAM administrator needs to provide the necessary roles to your account. For more information, see the IAM documentation.

Resetting the DB instance owner password

If you get locked out of your DB cluster, you can log in as the master user. Then you can reset the credentials for other administrative users or roles. If you can't log in as the master user, the AWS account owner can reset the master user password. For details of which administrative accounts or roles you might need to reset, see Master user account privileges (p. 1276).

You can change the DB instance password by using the Amazon RDS console, the AWS CLI command modify-db-instance, or by using the ModifyDBInstance API operation. For more information about modifying a DB instance in a DB cluster, see Modify a DB instance in a DB cluster (p. 328).

Amazon RDS DB instance outage or reboot

A DB instance outage can occur when a DB instance is rebooted. It can also occur when the DB instance is put into a state that prevents access to it, and when the database is restarted. A reboot can occur when you either manually reboot your DB instance or change a DB instance setting that requires a reboot before it can take effect.

A DB instance reboot occurs when you change a setting that requires a reboot, or when you manually cause a reboot. A reboot can occur immediately if you change a setting and request that the change take effect immediately or it can occur during the DB instance's maintenance window.
A DB instance reboot occurs immediately when one of the following occurs:

- You change the backup retention period for a DB instance from 0 to a nonzero value or from a nonzero value to 0 and set **Apply Immediately** to **true**.
- You change the DB instance class, and **Apply Immediately** is set to **true**.

A DB instance reboot occurs during the maintenance window when one of the following occurs:

- You change the backup retention period for a DB instance from 0 to a nonzero value or from a nonzero value to 0, and **Apply Immediately** is set to **false**.
- You change the DB instance class, and **Apply Immediately** is set to **false**.

When you change a static parameter in a DB parameter group, the change doesn't take effect until the DB instance associated with the parameter group is rebooted. The change requires a manual reboot. The DB instance isn't automatically rebooted during the maintenance window.

### Amazon RDS DB parameter changes not taking effect

In some cases, you might change a parameter in a DB parameter group but don't see the changes take effect. If so, you likely need to reboot the DB instance associated with the DB parameter group. When you change a dynamic parameter, the change takes effect immediately. When you change a static parameter, the change doesn't take effect until you reboot the DB instance associated with the parameter group.

You can reboot a DB instance using the RDS console or explicitly calling the **RebootDBInstance** API operation (without failover, if the DB instance is in a Multi-AZ deployment). The requirement to reboot the associated DB instance after a static parameter change helps mitigate the risk of a parameter misconfiguration affecting an API call. An example of this might be calling **ModifyDBInstance** to change the DB instance class. For more information, see **Modifying parameters in a DB parameter group** (p. 303).

### Amazon Aurora MySQL out of memory issues

The Aurora MySQL **aurora_oom_response** instance-level parameter can enable the DB instance to monitor the system memory and estimate the memory consumed by various statements and connections. If the system runs low on memory, it can perform a list of actions to release that memory in an attempt to avoid out-of-memory (OOM) and database restart. The instance-level parameter takes a string of comma-separated actions that a DB instance should take when its memory is low. Valid actions include **print**, **tune**, **decline**, **kill_query**, or any combination of these. An empty string means that no action should be taken and effectively disables the feature.

The following are usage examples for the **aurora_oom_response** parameter:

- **print** – Only prints the queries taking high amount of memory.
- **tune** – Tunes the internal table caches to release some memory back to the system.
- **decline** – Declines new queries once the instance is low on memory.
- **kill_query** – Ends the queries in descending order of memory consumption until the instance memory surfaces above the low threshold. Data definition language (DDL) statements aren’t ended.
• print, tune – Performs actions described for both print and tune.
• tune, decline, kill_query – Performs the actions described for tune, decline, and kill_query.

For the db.t2.small DB instance class, the aurora_oom_response parameter is set to print, tune by default. For all other DB instance classes, the parameter value is empty by default (disabled).

Amazon Aurora MySQL replication issues

Some MySQL replication issues also apply to Aurora MySQL. You can diagnose and correct these.

Topics
• Diagnosing and resolving lag between read replicas (p. 1310)
• Diagnosing and resolving a MySQL read replication failure (p. 1311)
• Replication stopped error (p. 1312)

Diagnosing and resolving lag between read replicas

After you create a MySQL read replica and the replica is available, Amazon RDS first replicates the changes made to the source DB instance from the time the read replica create operation started. During this phase, the replication lag time for the read replica is greater than 0. You can monitor this lag time in Amazon CloudWatch by viewing the Amazon RDS AuroraBinlogReplicaLag metric.

The AuroraBinlogReplicaLag metric reports the value of the Seconds_Behind_Master field of the MySQL SHOW SLAVE STATUS command. For more information, see SHOW SLAVE STATUS. When the AuroraBinlogReplicaLag metric reaches 0, the replica has caught up to the source DB instance. If the AuroraBinlogReplicaLag metric returns -1, replication might not be active. To troubleshoot a replication error, see Diagnosing and resolving a MySQL read replication failure (p. 1311). A AuroraBinlogReplicaLag value of -1 can also mean that the Seconds_Behind_Master value can't be determined or is NULL.

The AuroraBinlogReplicaLag metric returns -1 during a network outage or when a patch is applied during the maintenance window. In this case, wait for network connectivity to be restored or for the maintenance window to end before you check the AuroraBinlogReplicaLag metric again.

The MySQL read replication technology is asynchronous. Thus, you can expect occasional increases for the BinLogDiskUsage metric on the source DB instance and for the AuroraBinlogReplicaLag metric on the read replica. For example, consider a situation where a high volume of write operations to the source DB instance occur in parallel. At the same time, write operations to the read replica are serialized using a single I/O thread. Such a situation can lead to a lag between the source instance and read replica.

For more information about read replicas and MySQL, see Replication implementation details in the MySQL documentation.

You can reduce the lag between updates to a source DB instance and the subsequent updates to the read replica by doing the following:

• Set the DB instance class of the read replica to have a storage size comparable to that of the source DB instance.
• Make sure that parameter settings in the DB parameter groups used by the source DB instance and the read replica are compatible. For more information and an example, see the discussion of the max_allowed_packet parameter in the next section.
• Disable the query cache. For tables that are modified often, using the query cache can increase replica lag because the cache is locked and refreshed often. If this is the case, you might see less replica lag if you disable the query cache. You can disable the query cache by setting the query_cache_type parameter to 0 in the DB parameter group for the DB instance. For more information on the query cache, see Query cache configuration.

• Warm the buffer pool on the read replica for InnoDB for MySQL. For example, suppose that you have a small set of tables that are being updated often and you’re using the InnoDB or XtraDB table schema. In this case, dump those tables on the read replica. Doing this causes the database engine to scan through the rows of those tables from the disk and then cache them in the buffer pool. This approach can reduce replica lag. The following shows an example.

For Linux, macOS, or Unix:

```
PROMPT> mysqldump \
    -h <endpoint> \
    --port=<port> \
    -u=<username> \
    -p <password> \
    database_name table1 table2 > /dev/null
```

For Windows:

```
PROMPT> mysqldump ^
    -h <endpoint> ^
    --port=<port> ^
    -u=<username> ^
    -p <password> ^
    database_name table1 table2 > /dev/null
```

Diagnosing and resolving a MySQL read replication failure

Amazon RDS monitors the replication status of your read replicas and updates the Replication State field of the read replica instance to Error if replication stops for any reason. You can review the details of the associated error thrown by the MySQL engines by viewing the Replication Error field. Events that indicate the status of the read replica are also generated, including RDS-EVENT-0045 (p. 599), RDS-EVENT-0046 (p. 599), and RDS-EVENT-0047 (p. 598). For more information about events and subscribing to events, see Using Amazon RDS event notification (p. 594). If a MySQL error message is returned, check the error in the MySQL error message documentation.

Common situations that can cause replication errors include the following:

• The value for the max_allowed_packet parameter for a read replica is less than the max_allowed_packet parameter for the source DB instance.

    The max_allowed_packet parameter is a custom parameter that you can set in a DB parameter group. The max_allowed_packet parameter is used to specify the maximum size of data manipulation language (DML) that can be run on the database. If the max_allowed_packet value for the source DB instance is larger than the max_allowed_packet value for the read replica, the replication process can throw an error and stop replication. The most common error is packet bigger than `max_allowed_packet' bytes. You can fix the error by having the source and read replica use DB parameter groups with the same max_allowed_packet parameter values.

• Writing to tables on a read replica. If you're creating indexes on a read replica, you need to have the read_only parameter set to 0 to create the indexes. If you're writing to tables on the read replica, it can break replication.
• Using a nontransactional storage engine such as MyISAM. Read replicas require a transactional storage engine. Replication is only supported for the following storage engines: InnoDB for MySQL, InnoDB for MariaDB 10.2 or higher, or XtraDB for MariaDB 10.1 or lower.

You can convert a MyISAM table to InnoDB with the following command:

```sql
alter table <schema>.<table_name> engine=innodb;
```

• Using unsafe nondeterministic queries such as `SYSDATE()`. For more information, see Determination of safe and unsafe statements in binary logging in the MySQL documentation.

The following steps can help resolve your replication error:

• If you encounter a logical error and you can safely skip the error, follow the steps described in Skipping the current replication error. Your Aurora MySQL DB instance must be running a version that includes the `mysql_rds_skip_repl_error` procedure. For more information, see `mysql_rds_skip_repl_error`.

• If you encounter a binary log (binlog) position issue, you can change the replica replay position with the `mysql_rds_next_master_log` command. Your Aurora MySQL DB instance must be running a version that supports the `mysql_rds_next_master_log` command to change the replica replay position. For version information, see `mysql_rds_next_master_log`.

• If you encounter a temporary performance issue due to high DML load, you can set the `innodb_flush_log_at_trx_commit` parameter to 2 in the DB parameter group on the read replica. Doing this can help the read replica catch up, though it temporarily reduces atomicity, consistency, isolation, and durability (ACID).

• You can delete the read replica and create an instance using the same DB instance identifier so that the endpoint remains the same as that of your old read replica.

If a replication error is fixed, the Replication State changes to replicating. For more information, see Troubleshooting a MySQL read replica problem.

### Replication stopped error

When you call the `mysql.rds_skip_repl_error` command, you might receive the following error message: Slave is down or disabled.

This error message appears because replication is stopped and can't be restarted.

If you need to skip a large number of errors, the replication lag can increase beyond the default retention period for binary log files. In this case, you might encounter a fatal error due to binary log files being purged before they have been replayed on the replica. This purge causes replication to stop, and you can no longer call the `mysql.rds_skip_repl_error` command to skip replication errors.

You can mitigate this issue by increasing the number of hours that binary log files are retained on your replication source. After you have increased the binlog retention time, you can restart replication and call the `mysql.rds_skip_repl_error` command as needed.

To set the binlog retention time, use the `mysql_rds_set_configuration` procedure. Specify a configuration parameter of 'binlog retention hours' along with the number of hours to retain binlog files on the DB cluster, up to 720 (30 days). The following example sets the retention period for binlog files to 48 hours.

```sql
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

### No space left on device

You might encounter one of the following error messages.
• From Amazon Aurora MySQL:

```sql
ERROR 3 (HY000): Error writing file '/rdsdbdata/tmp/XXXXXXXX' (Errcode: 28 - No space left on device)
```

• From Amazon Aurora PostgreSQL:

```sql
ERROR: could not write block XXXXXXXXX of temporary file: No space left on device.
```

Each DB instance in an Amazon Aurora DB cluster uses local solid state drive (SSD) storage to store temporary tables for a session. This local storage for temporary tables doesn't automatically grow like the Aurora cluster volume. Instead, the amount of local storage is limited. The limit is based on the DB instance class for DB instances in your DB cluster.

To show the amount of storage available for temporary tables and logs, you can use the CloudWatch metric FreeLocalStorage. This metric is for per-instance temporary volumes, not the cluster volume. For more information on available metrics, see Monitoring Amazon Aurora DB cluster metrics (p. 489).

In some cases, you can't modify your workload to reduce the amount temporary storage required. If so, modify your DB instances to use a DB instance class that has more local SSD storage. For more information, see DB instance classes (p. 46).

For more troubleshooting information, see What is stored in Aurora for MySQL local storage, and how can I troubleshoot local storage issues? or What is stored in Amazon Aurora for PostgreSQL storage, and how can I troubleshoot storage issues?.

Amazon RDS application programming interface (API) reference

In addition to the AWS Management Console, and the AWS Command Line Interface (AWS CLI), Amazon Relational Database Service (Amazon RDS) also provides an application programming interface (API). You can use the API to automate tasks for managing your DB instances and other objects in Amazon RDS.

- For an alphabetical list of API operations, see Actions.
- For an alphabetical list of data types, see Data types.
- For a list of common query parameters, see Common parameters.
- For descriptions of the error codes, see Common errors.

For more information about the AWS CLI, see AWS Command Line Interface reference for Amazon RDS.

**Topics**
- Using the Query API (p. 1314)
- Troubleshooting applications on Aurora (p. 1315)

**Using the Query API**

The following sections briefly discuss the parameters and request authentication used with the Query API.

For general information about how the Query API works, see Query requests in the Amazon EC2 API Reference.

**Query parameters**

HTTP Query-based requests are HTTP requests that use the HTTP verb GET or POST and a Query parameter named Action.

Each Query request must include some common parameters to handle authentication and selection of an action.

Some operations take lists of parameters. These lists are specified using the param.\(n\) notation. Values of \(n\) are integers starting from 1.

For information about Amazon RDS regions and endpoints, go to Amazon Relational Database Service (RDS) in the Regions and Endpoints section of the Amazon Web Services General Reference.

**Query request authentication**

You can only send Query requests over HTTPS, and you must include a signature in every Query request. You must use either AWS signature version 4 or signature version 2. For more information, see Signature Version 4 signing process and Signature version 2 signing process.
Amazon Aurora User Guide for Aurora
Troubleshooting applications

Troubleshooting applications on Aurora
Amazon RDS provides speciﬁc and descriptive errors to help you troubleshoot problems while interacting
with the Amazon RDS API.
Topics
• Retrieving errors (p. 1315)
• Troubleshooting tips (p. 1315)
For information about troubleshooting for Amazon RDS DB instances, see Troubleshooting for
Aurora (p. 1306).

Retrieving errors
Typically, you want your application to check whether a request generated an error before you spend any
time processing results. The easiest way to ﬁnd out if an error occurred is to look for an Error node in
the response from the Amazon RDS API.
XPath syntax provides a simple way to search for the presence of an Error node, as well as an easy way
to retrieve the error code and message. The following code snippet uses Perl and the XML::XPath module
to determine if an error occurred during a request. If an error occurred, the code prints the ﬁrst error
code and message in the response.
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"; }

Troubleshooting tips
We recommend the following processes to diagnose and resolve problems with the Amazon RDS API.
• Verify that Amazon RDS is operating normally in the AWS Region you are targeting by visiting http://
status.aws.amazon.com.
• Check the structure of your request
Each Amazon RDS operation has a reference page in the Amazon RDS API Reference. Double-check that
you are using parameters correctly. In order to give you ideas regarding what might be wrong, look at
the sample requests or user scenarios to see if those examples are doing similar operations.
• Check the forum
Amazon RDS has a development community forum where you can search for solutions to problems
others have experienced along the way. To view the forum, go to
https://forums.aws.amazon.com/

1315


## Document history

**Current API version:** 2014-10-31

The following table describes important changes to the *Amazon Aurora User Guide*. For notification about updates to this documentation, you can subscribe to an RSS feed. For information about Amazon Relational Database Service (Amazon RDS), see the *Amazon Relational Database Service User Guide*.

### Note

Before August 31, 2018, Amazon Aurora was documented in the *Amazon Relational Database Service User Guide*. For earlier Aurora document history, see Document history in the *Amazon Relational Database Service User Guide*.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services</td>
<td>The AWS JDBC Driver for MySQL (preview) is a client driver designed for the high availability of Aurora MySQL. For more information, see Connecting with the Amazon Web Services JDBC Driver for MySQL. (p. 1316)</td>
<td>January 7, 2021</td>
</tr>
<tr>
<td>JDBC Driver for MySQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(preview)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aurora supports database activity streams on secondary clusters of a global DB (p. 1316)</td>
<td>You can start a database activity stream on a primary or secondary cluster of Aurora PostgreSQL or Aurora MySQL. For supported engine versions, see Limitations of Aurora global databases.</td>
<td>December 22, 2020</td>
</tr>
<tr>
<td>Multi-master clusters with 4 DB instances (p. 1316)</td>
<td>The maximum number of DB instances in an Aurora MySQL multi-master cluster is now four. Formerly, the maximum was two DB instances. For more information, see Working with Aurora Multi-Master Clusters.</td>
<td>December 17, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 3.4.0, 2.7.0, and 1.9.0 (p. 1316)</td>
<td>New versions of Amazon Aurora with PostgreSQL compatibility include version 3.4.0 (compatible with PostgreSQL 11.9), version 2.7.0 (compatible with PostgreSQL 10.14), and version 1.9.0 (compatible with PostgreSQL 9.6.19). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>December 11, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL supports AWS Lambda functions (p. 1316)</td>
<td>You can now invoke AWS Lambda function for your Aurora PostgreSQL DB clusters. For more information, see Invoking a</td>
<td>December 11, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Aurora MySQL version 2.09.1</td>
<td>Aurora MySQL version 2.09.1 is available.</td>
<td>December 11, 2020</td>
</tr>
<tr>
<td>Amazon Aurora supports the Graviton2 DB instance classes in preview</td>
<td>You can now use the Graviton2 DB instance classes db.r6g.x in preview to create DB clusters running MySQL or PostgreSQL. For more information, see <a href="#">DB instance class types</a>.</td>
<td>December 11, 2020</td>
</tr>
<tr>
<td>Amazon Aurora Serverless v2 (preview) is now available in preview</td>
<td>Amazon Aurora Serverless v2 (preview) is available in preview. To work with Amazon Aurora Serverless v2 (preview), you must apply for access. For more information, see the <a href="#">Aurora Serverless v2 (preview) page</a>.</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL is now available for Aurora Serverless v1 in more AWS Regions.</td>
<td>Aurora PostgreSQL is now available for Aurora Serverless v1 in more AWS Regions. You can now choose to run Aurora PostgreSQL Serverless in the same AWS Regions that offer Aurora MySQL Serverless. Additional AWS Regions with Aurora Serverless v1 support include US West (N. California), Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Seoul) Asia Pacific (Mumbai) Canada (Central) Europe (London) and Europe (Paris). For a list of all Regions and supported Aurora DB engines for Aurora Serverless v1, see <a href="#">Aurora Serverless</a>. Amazon RDS Data API for Aurora Serverless v1 is also now available in these same AWS Regions. For a list of all Regions with support for the Data API for Aurora Serverless v1, see <a href="#">Data API for Aurora Serverless</a>.</td>
<td>November 24, 2020</td>
</tr>
<tr>
<td>Aurora MySQL version 1.23.1</td>
<td>Aurora MySQL version 1.23.1 is available.</td>
<td>November 24, 2020</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Amazon RDS Performance Insights introduces new dimensions</strong></td>
<td>You can group database load according to the dimension groups for database, application (PostgreSQL), and session type (PostgreSQL). Amazon RDS also supports the dimensions db.name, db.application.name (PostgreSQL), and db.session_type.name (PostgreSQL). For more information, see Top load table.</td>
<td></td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL versions 3.2.6, 2.5.6, and 1.7.6</strong></td>
<td>New versions of Amazon Aurora with PostgreSQL compatibility include version 3.2.6 (compatible with PostgreSQL 11.7), version 2.5.6 (compatible with PostgreSQL 10.12), and version 1.7.6 (compatible with PostgreSQL 9.6.17). For more information, see <strong>Database engine versions for Amazon Aurora PostgreSQL</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.08.3</strong></td>
<td>Aurora MySQL version 2.08.3 is available.</td>
<td>November 12, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.07.3</strong></td>
<td>Aurora MySQL version 2.07.3 is available.</td>
<td>November 10, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.22.3</strong></td>
<td>Aurora MySQL version 1.22.3 is available.</td>
<td>November 9, 2020</td>
</tr>
<tr>
<td><strong>Aurora Serverless v1 supports Aurora PostgreSQL version 10.12</strong></td>
<td>Aurora PostgreSQL for Aurora Serverless v1 has been upgraded to Aurora PostgreSQL version 10.12 throughout the AWS Regions where Aurora PostgreSQL for Aurora Serverless v1 is supported. For more information, see <strong>Aurora Serverless v1</strong>.</td>
<td>November 4, 2020</td>
</tr>
<tr>
<td><strong>The Data API now supports tag-based authorization</strong></td>
<td>The Data API supports tag-based authorization. If you've labeled your RDS cluster resources with tags, you can use these tags in your policy statements to control access through the Data API. For more information, see <strong>Authorizing access to the Data API</strong>.</td>
<td>October 27, 2020</td>
</tr>
<tr>
<td><strong>Amazon Aurora extends support for exporting snapshots to Amazon S3</strong></td>
<td>You can now export DB snapshot data to Amazon S3 in all commercial AWS Regions. For more information, see <strong>Exporting DB snapshot data to Amazon S3</strong>.</td>
<td>October 22, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Aurora global database supports cloning (p. 1316)</strong></td>
<td>You can now create clones of the primary and secondary DB clusters of your Aurora global databases. You can do so by using the AWS Management Console and choosing the Create clone menu option. You can also use the AWS CLI and run the restore-db-cluster-to-point-in-time command with the --restore-type copy-on-write option. Using the AWS Management Console or the AWS CLI, you can also clone DB clusters from your Aurora global databases across AWS accounts. For more information about cloning, see Cloning an Aurora DB cluster volume.</td>
<td>October 19, 2020</td>
</tr>
<tr>
<td><strong>Amazon Aurora supports dynamic resizing for the cluster volume (p. 1316)</strong></td>
<td>Starting with Aurora MySQL 1.23 and 2.09, and Aurora PostgreSQL 3.3.0 and Aurora PostgreSQL 2.6.0, Aurora reduces the size of the cluster volume after you remove data through operations such as DROP TABLE. To take advantage of this enhancement, upgrade to one of the appropriate versions depending on the database engine that your cluster uses. For information about this feature and how to check used and available storage space for an Aurora cluster, see Managing Performance and Scaling for Aurora DB Clusters.</td>
<td>October 13, 2020</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL supports the pglogical extension (p. 1316)</strong></td>
<td>Aurora PostgreSQL now supports the PostgreSQL pglogical extension version 2.2.2. For more information, see the Aurora PostgreSQL versions 3.3.0 and 2.6.0 at Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>September 22, 2020</td>
</tr>
<tr>
<td><strong>Amazon Aurora supports volume sizes up to 128 TiB (p. 1316)</strong></td>
<td>New and existing Aurora cluster volumes can now grow to a maximum size of 128 tebibytes (TiB). For more information, see How Aurora storage grows.</td>
<td>September 22, 2020</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Aurora PostgreSQL bug fix for very specific queries that use NOT EXISTS (p. 1316)</td>
<td>Fixed a bug for very specific queries that use the NOT EXISTS operator on Aurora PostgreSQL versions that were released on or after May 24, 2020. The fix is available in Aurora PostgreSQL Version 2.5.4 (compatible with PostgreSQL version 10.12), Version 2.6.1 (compatible with PostgreSQL version 10.13), Version 3.2.4 (compatible with PostgreSQL version 11.7), and Version 3.3.1 (compatible with PostgreSQL version 11.8).</td>
<td>September 17, 2020</td>
</tr>
<tr>
<td>Aurora MySQL version 2.09.0 (p. 883)</td>
<td>Aurora MySQL version 2.09.0 is available.</td>
<td>September 17, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 3.3.0, 2.6.0, and 1.8.0 (p. 1316)</td>
<td>New versions of Amazon Aurora with PostgreSQL compatibility include version 3.3.0 (compatible with PostgreSQL 11.8), version 2.6.0 (compatible with PostgreSQL 10.13), and version 1.8.0 (compatible with PostgreSQL 9.6.18). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>September 3, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL supports the db.r5 and db.t3 DB instance classes in the China (Ningxia) Region (p. 1316)</td>
<td>You can now create Aurora PostgreSQL DB clusters in the China (Ningxia) Region that use the db.r5 and db.t3 DB instance classes. For more information, see DB instance classes.</td>
<td>September 3, 2020</td>
</tr>
<tr>
<td>Aurora parallel query enhancements (p. 1316)</td>
<td>Starting with Aurora MySQL 2.09 and 1.23, you can take advantage of enhancements to the parallel query feature. Creating a parallel query cluster no longer requires a special engine mode. You can now turn parallel query on and off using the <code>aurora_parallel_query</code> configuration option for any provisioned cluster that’s running a compatible Aurora MySQL version. You can upgrade an existing cluster to a compatible Aurora MySQL version and use parallel query, instead of creating a new cluster and importing data into it. You can use Performance Insights for parallel query clusters. You can stop and start parallel query clusters. You can create Aurora parallel query clusters that are compatible with MySQL 5.7. Parallel query works for tables that use the <code>DYNAMIC</code> row format. Parallel query clusters can use AWS Identity and Access Management (IAM) authentication. Reader DB instances in parallel query clusters can take advantage of the <code>READ COMMITTED</code> isolation level. You can also now create parallel query clusters in additional AWS Regions. For more information about the parallel query feature and these enhancements, see Working with parallel query for Aurora MySQL.</td>
<td>September 2, 2020</td>
</tr>
</tbody>
</table>

| Aurora MySQL version 1.23.0 (p. 932) | Aurora MySQL version 1.23.0 is available. | September 2, 2020 |

<p>| Aurora MySQL version 2.08.2 (p. 888) | Aurora MySQL version 2.08.2 is available. | August 28, 2020 |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aurora PostgreSQL versions 3.2.3, 2.5.3, and 1.7.3 (p. 1316)</strong></td>
<td>New versions of Amazon Aurora with PostgreSQL compatibility include version 3.2.3 (compatible with PostgreSQL 11.7), version 2.5.3 (compatible with PostgreSQL 10.12), and version 1.7.3 (compatible with PostgreSQL 9.6.17). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>August 27, 2020</td>
</tr>
<tr>
<td><strong>Changes to Aurora MySQL parameter binlog_rows_query_log_events (p. 848)</strong></td>
<td>You can now change the value of the Aurora MySQL configuration parameter binlog_rows_query_log_events. Formerly, this parameter wasn't modifiable.</td>
<td>August 26, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.04.9 (p. 902)</strong></td>
<td>Aurora MySQL version 2.04.9 is available.</td>
<td>August 14, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL Serverless version 1.21.0 (p. 978)</strong></td>
<td>Aurora Serverless with MySQL 5.6 compatibility is available. The release includes features and bug fixes based on Aurora MySQL version 1.21.0. For more information about Aurora Serverless, see Using Amazon Aurora Serverless.</td>
<td>August 14, 2020</td>
</tr>
<tr>
<td><strong>Support for automatic minor version upgrades for Aurora MySQL (p. 1316)</strong></td>
<td>With Aurora MySQL, the setting Enable auto minor version upgrade now takes effect when you specify it for an Aurora MySQL DB cluster. When you enable auto minor version upgrade, Aurora automatically upgrades to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database. For Aurora MySQL, this feature applies only to Aurora MySQL version 2, which is compatible with MySQL 5.7. Initially, the automatic upgrade procedure brings Aurora MySQL DB clusters to version 2.07.2. For more information about how this feature works with Aurora MySQL, see Database Upgrades and Patches for Amazon Aurora MySQL.</td>
<td>August 3, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Aurora PostgreSQL supports major version upgrades to PostgreSQL version 11 (p. 1316)</td>
<td>With Aurora PostgreSQL, you can now upgrade the DB engine to major version 11. For more information, see Upgrading the PostgreSQL DB engine for Aurora PostgreSQL.</td>
<td>July 28, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 3.1.3, 2.4.3, and 1.6.3 (p. 1316)</td>
<td>New patch versions of Aurora PostgreSQL include version 3.1.3 (compatible with PostgreSQL 11.6), version 2.4.3 (compatible with PostgreSQL 10.11), and version 1.6.3 (compatible with PostgreSQL 9.6.16). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>July 27, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 3.2.2, 2.5.2, and 1.7.2 (p. 1316)</td>
<td>New versions of Amazon Aurora with PostgreSQL compatibility include version 3.2.2 (compatible with PostgreSQL 11.7), version 2.5.2 (compatible with PostgreSQL 10.12), and version 1.7.2 (compatible with PostgreSQL 9.6.17). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>July 9, 2020</td>
</tr>
<tr>
<td>Amazon Aurora supports AWS PrivateLink (p. 1316)</td>
<td>Amazon Aurora now supports creating Amazon VPC endpoints for Amazon RDS API calls to keep traffic between applications and Aurora in the AWS network. For more information, see Amazon Aurora and interface VPC endpoints (AWS PrivateLink).</td>
<td>July 9, 2020</td>
</tr>
<tr>
<td>RDS Proxy generally available (p. 1316)</td>
<td>RDS Proxy is now generally available. You can use RDS Proxy with RDS MySQL, Aurora MySQL, RDS PostgreSQL, and Aurora PostgreSQL for production workloads. For more information about RDS Proxy, see “Managing Connections with Amazon RDS Proxy” in the Amazon RDS User Guide, or the Aurora user guide.</td>
<td>June 30, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Aurora Serverless version 2.07.1 (p. 977)</strong></td>
<td>Aurora Serverless with MySQL 5.7 compatibility is available. The release includes features and bug fixes based on Aurora MySQL version 2.07.1. For more information about Aurora Serverless, see Using Amazon Aurora Serverless.</td>
<td>June 24, 2020</td>
</tr>
<tr>
<td><strong>Aurora global database write forwarding (p. 1316)</strong></td>
<td>You can now enable write capability on secondary clusters in a global database. With write forwarding, you issue DML statements on a secondary cluster, Aurora forwards the write to the primary cluster, and the updated data is replicated to all the secondary clusters. For more information, see Write forwarding for secondary AWS Regions with an Aurora global database.</td>
<td>June 18, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.08.1 (p. 889)</strong></td>
<td>Aurora MySQL version 2.08.1 is available.</td>
<td>June 18, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.22.2 for parallel query clusters (p. 937)</strong></td>
<td>Aurora MySQL version 1.22.2 is available when you create a parallel query cluster.</td>
<td>June 18, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.20.1 for parallel query clusters (p. 942)</strong></td>
<td>Aurora MySQL version 1.20.1 is available when you create a parallel query cluster.</td>
<td>June 11, 2020</td>
</tr>
<tr>
<td><strong>Aurora supports integration with AWS Backup (p. 1316)</strong></td>
<td>You can use AWS Backup to manage backups of Aurora DB clusters. For more information, see Overview of backing up and restoring an Aurora DB cluster.</td>
<td>June 10, 2020</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL supports db.t3.large DB instance classes (p. 1316)</strong></td>
<td>You can now create Aurora PostgreSQL DB clusters that use the db.t3.large DB instance classes. For more information, see DB instance classes.</td>
<td>June 5, 2020</td>
</tr>
<tr>
<td><strong>Aurora global database supports PostgreSQL version 11.7 and managed recovery point objective (RPO) (p. 1316)</strong></td>
<td>You can now create Aurora global databases for the PostgreSQL database engine version 11.7. You can also manage how a PostgreSQL global database recovers from a failure using a recovery point objective (RPO). For more information, see Cross-Region Disaster Recovery for Aurora global databases.</td>
<td>June 4, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL versions</strong> 3.2.1, 2.5.1, and 1.7.1 (p. 1316)</td>
<td>New versions of Amazon Aurora with PostgreSQL compatibility include version 3.2.1 (compatible with PostgreSQL 11.7), version 2.5.1 (compatible with PostgreSQL 10.12), and version 1.7.1 (compatible with PostgreSQL 9.6.17). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>June 4, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.08.0 (p. 889)</strong></td>
<td>Aurora MySQL version 2.08.0 is available.</td>
<td>June 2, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.19.6 for parallel query clusters (p. 944)</strong></td>
<td>Aurora MySQL version 1.19.6 is available when you create a parallel query cluster.</td>
<td>June 2, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL supports database monitoring with database activity streams (p. 1316)</strong></td>
<td>Aurora MySQL now includes database activity streams, which provide a near-real-time data stream of the database activity in your relational database. For more information, see Using database activity streams.</td>
<td>June 2, 2020</td>
</tr>
<tr>
<td><strong>The query editor available in additional AWS Regions (p. 1316)</strong></td>
<td>The query editor for Aurora Serverless is now available in additional AWS Regions. For more information, see Availability of the query editor.</td>
<td>May 28, 2020</td>
</tr>
<tr>
<td><strong>The Data API available in additional AWS Regions (p. 1316)</strong></td>
<td>The Data API is now available in additional AWS Regions. For more information, see Availability of the Data API.</td>
<td>May 28, 2020</td>
</tr>
<tr>
<td><strong>RDS Proxy available in Canada (Central) Region (p. 1316)</strong></td>
<td>You can now use the RDS Proxy preview in the Canada (Central) Region. For more information about RDS Proxy, see Managing connections with Amazon RDS proxy (preview).</td>
<td>May 28, 2020</td>
</tr>
<tr>
<td><strong>Aurora global database and cross-Region read replicas (p. 1316)</strong></td>
<td>For an Aurora global database, you can now create an Aurora MySQL cross-Region read replica from the primary cluster in the same region as a secondary cluster. For more information about Aurora Global Database and cross-Region read replicas, see Working with Amazon Aurora global database and Replicating Amazon Aurora MySQL DB.</td>
<td>May 18, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>RDS Proxy available in more AWS Regions (p. 1316)</td>
<td>You can now use the RDS Proxy preview in the US West (N. California) Region, the Europe (London) Region, the Europe (Frankfurt) Region, the Asia Pacific (Seoul) Region, the Asia Pacific (Mumbai) Region, the Asia Pacific (Singapore) Region, and the Asia Pacific (Sydney) Region. For more information about RDS Proxy, see Managing connections with Amazon RDS proxy (preview).</td>
<td>May 13, 2020</td>
</tr>
<tr>
<td>Aurora with PostgreSQL compatibility supports on-premises or self-hosted Microsoft active directory (p. 1316)</td>
<td>You can now use an on-premises or self-hosted Active Directory for Kerberos authentication of users when they connect to your Aurora PostgreSQL DB clusters. For more information, see Using Kerberos authentication with Aurora PostgreSQL.</td>
<td>May 7, 2020</td>
</tr>
<tr>
<td>Aurora MySQL multi-master clusters available in more AWS Regions (p. 1316)</td>
<td>You can now create Aurora multi-master clusters in the Asia Pacific (Seoul) Region, the Asia Pacific (Tokyo) Region, the Asia Pacific (Mumbai) Region, and the Europe (Frankfurt) Region. For more information about multi-master clusters, see Working with Aurora multi-master clusters.</td>
<td>May 7, 2020</td>
</tr>
<tr>
<td>Performance Insights supports analyzing statistics of running Aurora MySQL queries (p. 1316)</td>
<td>You can now analyze statistics of running queries with Performance Insights for Aurora MySQL DB instances. For more information, see Analyzing statistics of running queries.</td>
<td>May 5, 2020</td>
</tr>
<tr>
<td>Java client library for Data API generally available (p. 1316)</td>
<td>The Java client library for the Data API is now generally available. You can download and use a Java client library for Data API. It enables you to map your client-side classes to requests and responses of the Data API. For more information, see Using the Java client library for Data API.</td>
<td>April 30, 2020</td>
</tr>
<tr>
<td>Amazon Aurora available in the Europe (Milan) Region (p. 1316)</td>
<td>Aurora is now available in the Europe (Milan) Region. For more information, see Regions and Availability Zones.</td>
<td>April 28, 2020</td>
</tr>
<tr>
<td>Amazon Aurora available in the Europe (Milan) Region (p. 1316)</td>
<td>Aurora is now available in the Europe (Milan) Region. For more information, see Regions and Availability Zones.</td>
<td>April 27, 2020</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Amazon Aurora available in the Africa (Cape Town) Region (p. 1316)</td>
<td>Aurora is now available in the Africa (Cape Town) Region. For more information, see Regions and Availability Zones.</td>
<td>April 22, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 3.1.2, 2.4.2, and 1.6.2 (p. 1316)</td>
<td>New patch versions of Aurora PostgreSQL include version 3.1.2 (compatible with PostgreSQL 11.6), version 2.4.2 (compatible with PostgreSQL 10.11), and version 1.6.2 (compatible with PostgreSQL 9.6.16). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>April 17, 2020</td>
</tr>
<tr>
<td>Aurora MySQL version 2.07.2 (p. 894)</td>
<td>Aurora MySQL version 2.07.2 is available.</td>
<td>April 17, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 3.1.1, 2.4.1, and 1.6.1 (p. 1316)</td>
<td>New patch versions of Aurora PostgreSQL include version 3.1.1 (compatible with PostgreSQL 11.6), version 2.4.1 (compatible with PostgreSQL 10.11), and version 1.6.1 (compatible with PostgreSQL 9.6.16). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>April 16, 2020</td>
</tr>
<tr>
<td>Aurora PostgreSQL now supports db.r5.16xlarge and db.r5.8xlarge DB instance classes (p. 1316)</td>
<td>You can now create Aurora PostgreSQL DB clusters running PostgreSQL that use the db.r5.16xlarge and db.r5.8xlarge DB instance classes. For more information, see Hardware specifications for DB instance classes for Aurora.</td>
<td>April 8, 2020</td>
</tr>
<tr>
<td>Amazon RDS proxy for PostgreSQL (p. 1316)</td>
<td>Amazon RDS Proxy is now available for PostgreSQL. You can use RDS Proxy to reduce the overhead of connection management on your cluster and also the chance of “too many connections” errors. The RDS Proxy is currently in public preview for PostgreSQL. For more information, see Managing connections with Amazon RDS proxy (preview).</td>
<td>April 8, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Aurora global databases now support Aurora PostgreSQL</strong> (p. 1316)</td>
<td>You can now create Aurora global databases for the PostgreSQL database engine. An Aurora global database spans multiple AWS Regions, enabling low latency global reads and disaster recovery from region-wide outages. For more information, see Working with Amazon Aurora global database.</td>
<td>March 10, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.22.2 (p. 937)</strong></td>
<td>Aurora MySQL version 1.22.2 is available.</td>
<td>March 5, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.20.1 (p. 942)</strong></td>
<td>Aurora MySQL version 1.20.1 is available.</td>
<td>March 5, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.19.6 (p. 944)</strong></td>
<td>Aurora MySQL version 1.19.6 is available.</td>
<td>March 5, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.17.9 (p. 949)</strong></td>
<td>Aurora MySQL version 1.17.9 is available.</td>
<td>March 5, 2020</td>
</tr>
<tr>
<td><strong>Support for major version upgrades for Aurora PostgreSQL</strong> (p. 1316)</td>
<td>With Aurora PostgreSQL, you can now upgrade the DB engine to a major version. By doing so, you can skip ahead to a newer major version when you upgrade select PostgreSQL engine versions. For more information, see Upgrading the PostgreSQL DB engine for Aurora PostgreSQL.</td>
<td>March 4, 2020</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL supports Kerberos authentication</strong> (p. 1316)</td>
<td>You can now use Kerberos authentication to authenticate users when they connect to your Aurora PostgreSQL DB clusters. For more information, see Using Kerberos authentication with Aurora PostgreSQL.</td>
<td>February 28, 2020</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL versions 3.1, 2.4, and 1.6 (p. 1316)</strong></td>
<td>New versions of Amazon Aurora with PostgreSQL compatibility include version 3.1 (compatible with PostgreSQL 11.6), version 2.4 (compatible with PostgreSQL 10.11), and version 1.6 (compatible with PostgreSQL 9.6.16). For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>February 11, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>The Data API supports AWS PrivateLink (p. 1316)</strong></td>
<td>The Data API now supports creating Amazon VPC endpoints for Data API calls to keep traffic between applications and the Data API in the AWS network. For more information, see Creating an Amazon VPC endpoint (AWS PrivateLink) for the Data API.</td>
<td>February 6, 2020</td>
</tr>
<tr>
<td><strong>Aurora machine learning support in Aurora PostgreSQL (p. 1316)</strong></td>
<td>The aws_ml Aurora PostgreSQL extension provides functions you use in your database queries to call Amazon Comprehend for sentiment analysis and SageMaker to run your own machine learning models. For more information, see Using machine learning (ML) capabilities with Aurora.</td>
<td>February 5, 2020</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL supports exporting data to Amazon S3 (p. 1316)</strong></td>
<td>You can query data from an Aurora PostgreSQL DB cluster and export it directly into files stored in an Amazon S3 bucket. For more information, see Exporting data from an Aurora PostgreSQL DB cluster to Amazon S3.</td>
<td>February 5, 2020</td>
</tr>
<tr>
<td><strong>Support for exporting DB snapshot data to Amazon S3 (p. 1316)</strong></td>
<td>Amazon Aurora supports exporting DB snapshot data to Amazon S3 for MySQL and PostgreSQL. For more information, see Exporting DB snapshot data to Amazon S3.</td>
<td>January 9, 2020</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.07.1 (p. 895)</strong></td>
<td>Aurora MySQL version 2.07.1 is available.</td>
<td>December 23, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.22.1 (p. 937)</strong></td>
<td>Aurora MySQL version 1.22.1 is available.</td>
<td>December 23, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL release notes in document history (p. 1316)</strong></td>
<td>This section now includes history entries for Aurora with MySQL compatibility release notes for versions released after August 31, 2018. For the full release notes for a specific version, choose the link in the first column of the history entry.</td>
<td>December 13, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Amazon RDS proxy (p. 1316)</strong></td>
<td>You can reduce the overhead of connection management on your cluster, and reduce the chance of &quot;too many connections&quot; errors, by using the Amazon RDS Proxy. You associate each proxy with an RDS DB instance or Aurora DB cluster. Then you use the proxy endpoint in the connection string for your application. The Amazon RDS Proxy is currently in a public preview state. It supports the Aurora MySQL database engine. For more information, see Managing connections with Amazon RDS proxy (preview).</td>
<td>December 3, 2019</td>
</tr>
<tr>
<td><strong>Data API for Aurora Serverless supports data type mapping hints (p. 1316)</strong></td>
<td>You can now use a hint to instruct the Data API for Aurora Serverless to send a String value to the database as a different type. For more information, see Calling the data API.</td>
<td>November 26, 2019</td>
</tr>
<tr>
<td><strong>Data API for Aurora Serverless supports a Java client library (preview) (p. 1316)</strong></td>
<td>You can download and use a Java client library for Data API. It enables you to map your client-side classes to requests and responses of the Data API. For more information, see Using the Java client library for Data API.</td>
<td>November 26, 2019</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL version 3.0 (p. 1316)</strong></td>
<td>Amazon Aurora PostgreSQL version 3.0 is available and compatible with PostgreSQL 11.4. Supported AWS Regions include us-east-1, us-east-2, us-west-2, eu-west-1, ap-northeast-1, and ap-northeast-2. For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>November 26, 2019</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL is FedRAMP HIGH eligible (p. 1316)</strong></td>
<td>Aurora PostgreSQL is FedRAMP HIGH eligible. For details about AWS and compliance efforts, see AWS services in scope by compliance program.</td>
<td>November 26, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>READ COMMITTED isolation level enabled for Amazon Aurora MySQL replicas (p. 1316)</strong></td>
<td>You can now enable the READ COMMITTED isolation level on Aurora MySQL Replicas. Doing so requires enabling the <code>aurora_read_replica_read_committed_isolation_enabled</code> configuration setting at the session level. Using the READ COMMITTED isolation level for long-running queries on OLTP clusters can help address issues with history list length. Before enabling this setting, be sure to understand how the isolation behavior on Aurora Replicas differs from the usual MySQL implementation of READ COMMITTED. For more information, see Aurora MySQL isolation levels.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>Performance Insights supports analyzing statistics of running Aurora PostgreSQL queries (p. 1316)</strong></td>
<td>You can now analyze statistics of running queries with Performance Insights for Aurora PostgreSQL DB instances. For more information, see Analyzing statistics of running queries.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>More clusters in an Aurora global database (p. 1316)</strong></td>
<td>You can now add multiple secondary regions to an Aurora global database. You can take advantage of low latency global reads and disaster recovery across a wider geographic area. For more information about Aurora global databases, see Working with Amazon Aurora global databases.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>Aurora machine learning support in Aurora MySQL (p. 1316)</strong></td>
<td>In Aurora MySQL 2.07 and higher, you can call Amazon Comprehend for sentiment analysis and SageMaker for a wide variety of machine learning algorithms. You use the results directly in your database application by embedding calls to stored functions in your queries. For more information, see Using machine learning (ML) capabilities with Aurora.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td>Feature Description</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Aurora global database no longer requires engine mode setting (p. 1316)</strong></td>
<td>You no longer need to specify <code>--engine-mode=global</code> when creating a cluster that is intended to be part of an Aurora global database. All Aurora clusters that meet the compatibility requirements are eligible to be part of a global database. For example, the cluster currently must use Aurora MySQL version 1 with MySQL 5.6 compatibility. For information about Aurora global databases, see Working with Amazon Aurora global databases.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>Aurora global database is available for Aurora MySQL version 2 (p. 1316)</strong></td>
<td>Starting in Aurora MySQL 2.07, you can create an Aurora global database with MySQL 5.7 compatibility. You don't need to specify the global engine mode for the primary or secondary clusters. You can add any new provisioned cluster with Aurora MySQL 2.07 or higher to an Aurora Global Database. For information about Aurora Global Database, see Working with Amazon Aurora global database.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.07.0 (p. 895)</strong></td>
<td>Aurora MySQL version 2.07.0 is available.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.22.0 (p. 938)</strong></td>
<td>Aurora MySQL version 1.22.0 is available.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.21.0 (p. 941)</strong></td>
<td>Aurora MySQL version 1.21.0 is available.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.06.0 (p. 898)</strong></td>
<td>Aurora MySQL version 2.06.0 is available.</td>
<td>November 22, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.04.8 (p. 905)</strong></td>
<td>Aurora MySQL version 2.04.8 is available.</td>
<td>November 20, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL hot row contention optimization available without lab mode (p. 1316)</strong></td>
<td>The hot row contention optimization is now generally available for Aurora MySQL and does not require the Aurora lab mode setting to be ON. This feature substantially improves throughput for workloads with many transactions contending for rows on the same page. The improvement involves changing the lock release algorithm used by Aurora MySQL.</td>
<td>November 19, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Aurora MySQL hash joins available without lab mode (p. 1316)</strong></td>
<td>The hash join feature is now generally available for Aurora MySQL and does not require the Aurora lab mode setting to be ON. This feature can improve query performance when you need to join a large amount of data by using an equi-join. For more information about using this feature, see Working with hash joins in Aurora MySQL.</td>
<td>November 19, 2019</td>
</tr>
<tr>
<td><em><em>Aurora MySQL 2.</em> support for more db.r5 instance classes (p. 1316)</em>*</td>
<td>Aurora MySQL clusters now support the instance types db.r5.8xlarge, db.r5.16xlarge, and db.r5.24xlarge. For more information about instance types for Aurora MySQL clusters, see Choosing the DB instance class.</td>
<td>November 19, 2019</td>
</tr>
<tr>
<td><em><em>Aurora MySQL 2.</em> support for backtracking (p. 1316)</em>*</td>
<td>Aurora MySQL 2.* versions now offer a quick way to recover from user errors, such as dropping the wrong table or deleting the wrong row. Backtrack allows you to move your database to a prior point in time without needing to restore from a backup, and it completes within seconds, even for large databases. For details, see Backtracking an Aurora DB cluster.</td>
<td>November 19, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.04.7 (p. 907)</strong></td>
<td>Aurora MySQL version 2.04.7 is available.</td>
<td>November 14, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.05.0 (p. 900)</strong></td>
<td>Aurora MySQL version 2.05.0 is available.</td>
<td>November 11, 2019</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.20.0 (p. 943)</strong></td>
<td>Aurora MySQL version 1.20.0 is available.</td>
<td>November 11, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Billing tag support for Aurora (p. 1316)</td>
<td>You can now use tags to keep track of cost allocation for resources such as Aurora clusters, DB instances within Aurora clusters, I/O, backups, snapshots, and so on. You can see costs associated with each tag using AWS Cost Explorer. For more information about using tags with Aurora, see Tagging Amazon RDS resources. For general information about tags and ways to use them for cost analysis, see Using cost allocation tags and User-defined cost allocation tags.</td>
<td>October 23, 2019</td>
</tr>
<tr>
<td>Data API for Aurora PostgreSQL (p. 1316)</td>
<td>Aurora PostgreSQL now supports using the Data API with Amazon Aurora Serverless DB clusters. For more information, see Using the Data API for Aurora Serverless.</td>
<td>September 23, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 2.04.6 (p. 909)</td>
<td>Aurora MySQL version 2.04.6 is available.</td>
<td>September 19, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 1.19.5 (p. 945)</td>
<td>Aurora MySQL version 1.19.5 is available.</td>
<td>September 19, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL supports uploading database logs to CloudWatch logs (p. 1316)</td>
<td>You can configure your Aurora PostgreSQL DB cluster to publish log data to a log group in Amazon CloudWatch Logs. With CloudWatch Logs, you can perform real-time analysis of the log data, and use CloudWatch to create alarms and view metrics. You can use CloudWatch Logs to store your log records in highly durable storage. For more information, see Publishing Aurora PostgreSQL logs to Amazon CloudWatch Logs.</td>
<td>August 9, 2019</td>
</tr>
<tr>
<td>Multi-master clusters for Aurora MySQL (p. 1316)</td>
<td>You can set up Aurora MySQL multi-master clusters. In these clusters, each DB instance has read/write capability. For more information, see Working with Aurora multi-master clusters.</td>
<td>August 8, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Aurora PostgreSQL supports Aurora Serverless (p. 1316)</td>
<td>You can now use Amazon Aurora Serverless with Aurora PostgreSQL. An Aurora Serverless DB cluster automatically starts up, shuts down, and scales up or down its compute capacity based on your application's needs. For more information, see Using Amazon Aurora Serverless.</td>
<td>July 9, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 2.04.5 (p. 910)</td>
<td>Aurora MySQL version 2.04.5 is available.</td>
<td>July 8, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 2.3.3 and 1.5.2 (p. 1316)</td>
<td>Amazon Aurora with PostgreSQL compatibility version 2.3.3 is available and compatible with PostgreSQL 10.7. Amazon Aurora with PostgreSQL compatibility version 1.5.2 is available and compatible with PostgreSQL 9.6.12. For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>July 3, 2019</td>
</tr>
<tr>
<td>Cross-account cloning for Aurora MySQL (p. 1316)</td>
<td>You can now clone the cluster volume for an Aurora MySQL DB cluster between AWS accounts. You authorize the sharing through AWS Resource Access Manager (AWS RAM). The cloned cluster volume uses a copy-on-write mechanism, which only requires additional storage for new or changed data. For more information about cloning for Aurora, see Cloning databases in an Aurora DB cluster.</td>
<td>July 2, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 2.3.1 and 1.5.1 (p. 1316)</td>
<td>Amazon Aurora with PostgreSQL compatibility version 2.3.1 is available and compatible with PostgreSQL 10.7. Amazon Aurora with PostgreSQL compatibility version 1.5.1 is available and compatible with PostgreSQL 9.6.12. For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>July 2, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL supports db.t3 DB instance classes (p. 1316)</td>
<td>You can now create Aurora PostgreSQL DB clusters that use the db.t3 DB instance classes. For more information, see DB instance class.</td>
<td>June 20, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Support for importing data from Amazon S3 for Aurora PostgreSQL (p. 1316)</td>
<td>You can now import data from an Amazon S3 file into a table in an Aurora PostgreSQL DB cluster. For more information, see Importing Amazon S3 data into an Aurora PostgreSQL DB cluster.</td>
<td>June 19, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL now provides fast failover recovery with cluster cache management (p. 1316)</td>
<td>Aurora PostgreSQL now provides cluster cache management to ensure fast recovery of the primary DB instance in the event of a failover. For more information, see Fast recovery after failover with cluster cache management.</td>
<td>June 11, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 1.19.2 (p. 946)</td>
<td>Aurora MySQL version 1.19.2 is available.</td>
<td>June 5, 2019</td>
</tr>
<tr>
<td>Data API for Aurora Serverless generally available (p. 1316)</td>
<td>You can access Aurora Serverless clusters with web services-based applications using the Data API. For more information, see Using the Data API for Aurora Serverless.</td>
<td>May 30, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL version 2.3 (p. 1316)</td>
<td>Version 2.3 of Amazon Aurora with PostgreSQL compatibility is available and compatible with PostgreSQL 10.7. For more information, see Version 2.3.</td>
<td>May 30, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL supports database monitoring with database activity streams (p. 1316)</td>
<td>Aurora PostgreSQL now includes database activity streams, which provide a near real-time data stream of the database activity in your relational database. For more information, see Using database activity streams.</td>
<td>May 30, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 2.04.4 (p. 912)</td>
<td>Aurora MySQL version 2.04.4 is available.</td>
<td>May 29, 2019</td>
</tr>
<tr>
<td>Amazon Aurora recommendations (p. 1316)</td>
<td>Amazon Aurora now provides automated recommendations for Aurora resources. For more information, see Using Amazon Aurora recommendations.</td>
<td>May 22, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL versions 1.2.2, 1.3.2, 2.0.1, 2.1.1, 2.2.1 (p. 1316)</td>
<td>The following patch versions for Amazon Aurora with PostgreSQL compatibility are now available and include versions 1.2.2, 1.3.2, 2.0.1, 2.1.1, and 2.2.1. For more information, see Database engine versions for Amazon Aurora PostgreSQL.</td>
<td>May 21, 2019</td>
</tr>
<tr>
<td>变更内容</td>
<td>描述</td>
<td>日期</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Performance Insights支持Aurora全局数据库 (p. 1316)</td>
<td>您现在可以使用Performance Insights与Aurora全局数据库一起使用。有关Performance Insights的更多信息，请参见Using Amazon RDS performance insights。有关Aurora全局数据库的信息，请参见Working with Aurora global database。</td>
<td>May 13, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL版本1.4 (p. 1316)</td>
<td>Version 1.4 of Amazon Aurora with PostgreSQL compatibility is available and compatible with PostgreSQL 9.6.11. For more information, see Version 1.4.</td>
<td>May 9, 2019</td>
</tr>
<tr>
<td>Aurora MySQL版本2.04.3 (p. 913)</td>
<td>Aurora MySQL version 2.04.3 is available.</td>
<td>May 9, 2019</td>
</tr>
<tr>
<td>Aurora MySQL版本1.19.1 (p. 946)</td>
<td>Aurora MySQL version 1.19.1 is available.</td>
<td>May 9, 2019</td>
</tr>
<tr>
<td>Performance Insights可用Aurora MySQL 5.7 (p. 1316)</td>
<td>Amazon RDS Performance Insights is now available for Aurora MySQL 2.x versions, which are compatible with MySQL 5.7. For more information, see Using Amazon RDS performance insights.</td>
<td>May 3, 2019</td>
</tr>
<tr>
<td>Aurora MySQL版本2.04.2 (p. 914)</td>
<td>Aurora MySQL version 2.04.2 is available.</td>
<td>May 2, 2019</td>
</tr>
<tr>
<td>Aurora全局数据库在更多AWS区域可用 (p. 1316)</td>
<td>您现在可以在大多数AWS区域创建Aurora全局数据库。有关Aurora全局数据库的信息，请参见Working with Amazon Aurora global databases。</td>
<td>April 30, 2019</td>
</tr>
<tr>
<td>最小容量为1 for Aurora Serverless (p. 1316)</td>
<td>The minimum capacity setting you can use for an Aurora Serverless cluster is 1. Formerly, the minimum was 2. For information about specifying Aurora Serverless capacity values, see Setting the capacity of an Aurora Serverless DB cluster.</td>
<td>April 29, 2019</td>
</tr>
<tr>
<td>Aurora Serverless超时动作 (p. 1316)</td>
<td>You can now specify the action to take when an Aurora Serverless capacity change times out. For more information, see Timeout action for capacity changes.</td>
<td>April 29, 2019</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Per-second billing (p. 1316)</td>
<td>Amazon RDS is now billed in 1-second increments in all AWS Regions except AWS GovCloud (US) for on-demand instances. For more information, see DB instance billing for Aurora.</td>
<td>April 25, 2019</td>
</tr>
<tr>
<td>Sharing Aurora Serverless snapshots across AWS Regions (p. 1316)</td>
<td>With Aurora Serverless, snapshots are always encrypted. If you encrypt the snapshot with your own AWS Key Management Service customer master key (CMK), you can now copy or share the snapshot across AWS Regions. For information about snapshots of Aurora Serverless DB clusters, see Aurora Serverless and snapshots.</td>
<td>April 17, 2019</td>
</tr>
<tr>
<td>Restore MySQL 5.7 backups from Amazon S3 (p. 1316)</td>
<td>You can now create a backup of your MySQL version 5.7 database, store it on Amazon S3, and then restore the backup file onto a new Aurora MySQL DB cluster. For more information, see Migrating data from an external MySQL database to an Aurora MySQL DB cluster.</td>
<td>April 17, 2019</td>
</tr>
<tr>
<td>Sharing Aurora Serverless snapshots across regions (p. 1316)</td>
<td>With Aurora Serverless, snapshots are always encrypted. If you encrypt the snapshot with your own AWS Key Management Service customer master key (CMK), you can now copy or share the snapshot across regions. For information about snapshots of Aurora Serverless DB clusters, see Aurora Serverless and snapshots.</td>
<td>April 16, 2019</td>
</tr>
<tr>
<td>Aurora proof-of-concept tutorial (p. 1316)</td>
<td>You can learn how to perform a proof of concept to try your application and workload with Aurora. For the full tutorial, see Performing an Aurora proof of concept.</td>
<td>April 16, 2019</td>
</tr>
<tr>
<td>Aurora Serverless supports restoring from an Amazon S3 backup (p. 1316)</td>
<td>You can now import backups from Amazon S3 to an Aurora Serverless cluster. For details about that procedure, see Migrating data from MySQL by using an Amazon S3 bucket.</td>
<td>April 16, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>New modifiable parameters for Aurora Serverless (p. 1316)</td>
<td>You can now modify the following DB parameters for an Aurora Serverless cluster: 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, and tx_isolation. For more information about configuration parameters for Aurora Serverless clusters, see Aurora Serverless and parameter groups.</td>
<td>April 4, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL supports db.r5 DB instance classes (p. 1316)</td>
<td>You can now create Aurora PostgreSQL DB clusters that use the db.r5 DB instance classes. For more information, see DB instance class.</td>
<td>April 4, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL logical replication (p. 1316)</td>
<td>You can now use PostgreSQL logical replication to replicate parts of a database for an Aurora PostgreSQL DB cluster. For more information, see Using PostgreSQL logical replication.</td>
<td>March 28, 2019</td>
</tr>
<tr>
<td>GTID support for Aurora MySQL 2.04 (p. 1316)</td>
<td>You can now use replication with the global transaction ID (GTID) feature of MySQL 5.7. This feature simplifies performing binary log (binlog) replication between Aurora MySQL and an external MySQL 5.7-compatible database. The replication can use the Aurora MySQL cluster as the source or the destination. This feature is available for Aurora MySQL 2.04 and higher. For more information about GTID-based replication and Aurora MySQL, see Using GTID-based replication for Aurora MySQL.</td>
<td>March 25, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 2.04.1 (p. 916)</td>
<td>Aurora MySQL version 2.04.1 is available.</td>
<td>March 25, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Aurora MySQL version 2.04 (p. 916)</td>
<td>Aurora MySQL version 2.04 is available.</td>
<td>March 25, 2019</td>
</tr>
<tr>
<td>Uploading Aurora Serverless logs to Amazon CloudWatch (p. 1316)</td>
<td>You can now have Aurora upload database logs to CloudWatch for an Aurora Serverless cluster. For more information, see Viewing Aurora Serverless DB clusters. As part of this enhancement, you can now define values for instance-level parameters in a DB cluster parameter group, and those values apply to all DB instances in the cluster unless you override them in the DB parameter group. For more information, see Working with DB parameter groups and DB cluster parameter groups.</td>
<td>February 25, 2019</td>
</tr>
<tr>
<td>Aurora MySQL supports db.t3 DB instance classes (p. 1316)</td>
<td>You can now create Aurora MySQL DB clusters that use the db.t3 DB instance classes. For more information, see DB instance class.</td>
<td>February 25, 2019</td>
</tr>
<tr>
<td>Aurora MySQL supports db.r5 DB instance classes (p. 1316)</td>
<td>You can now create Aurora MySQL DB clusters that use the db.r5 DB instance classes. For more information, see DB instance class.</td>
<td>February 25, 2019</td>
</tr>
<tr>
<td>Performance Insights counters for Aurora MySQL (p. 1316)</td>
<td>You can now add performance counters to your Performance Insights charts for Aurora MySQL DB instances. For more information, see Performance Insights dashboard components.</td>
<td>February 19, 2019</td>
</tr>
<tr>
<td>Aurora PostgreSQL version 2.2.0 (p. 1316)</td>
<td>Version 2.2.0 of Aurora PostgreSQL is available and compatible with PostgreSQL 10.6. For more information, see Version 2.2.0.</td>
<td>February 13, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 2.03.4 (p. 917)</td>
<td>Aurora MySQL version 2.03.4 is available.</td>
<td>February 7, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 1.19.0 (p. 947)</td>
<td>Aurora MySQL version 1.19.0 is available.</td>
<td>February 7, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Details</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Amazon RDS Performance Insights supports viewing more SQL text for Aurora MySQL (p. 1316)</td>
<td>Amazon RDS Performance Insights now supports viewing more SQL text in the Performance Insights dashboard for Aurora MySQL DB instances. For more information, see Viewing more SQL text in the Performance Insights dashboard.</td>
<td>February 6, 2019</td>
</tr>
<tr>
<td>Amazon RDS Performance Insights supports viewing more SQL text for Aurora PostgreSQL (p. 1316)</td>
<td>Amazon RDS Performance Insights now supports viewing more SQL text in the Performance Insights dashboard for Aurora PostgreSQL DB instances. For more information, see Viewing more SQL text in the Performance Insights dashboard.</td>
<td>January 24, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 2.03.3 (p. 918)</td>
<td>Aurora MySQL version 2.03.3 is available.</td>
<td>January 18, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 1.17.8 (p. 949)</td>
<td>Aurora MySQL version 1.17.8 is available.</td>
<td>January 17, 2019</td>
</tr>
<tr>
<td>Aurora MySQL version 2.03.2 (p. 919)</td>
<td>Aurora MySQL version 2.03.2 is available.</td>
<td>January 9, 2019</td>
</tr>
<tr>
<td>Aurora backup billing (p. 1316)</td>
<td>You can use the Amazon CloudWatch metrics TotalBackupStorageBilled, SnapshotStorageUsed, and BackupRetentionPeriodStorageUsed to monitor the space usage of your Aurora backups. For more information about how to use CloudWatch metrics, see Overview of monitoring. For more information about how to manage storage for backup data, see Understanding Aurora backup storage usage.</td>
<td>January 3, 2019</td>
</tr>
<tr>
<td>Performance Insights counters (p. 1316)</td>
<td>You can now add performance counters to your Performance Insights charts. For more information, see Performance Insights dashboard components.</td>
<td>December 6, 2018</td>
</tr>
<tr>
<td>Aurora global database (p. 1316)</td>
<td>You can now create Aurora global databases. An Aurora global database spans multiple AWS Regions, enabling low latency global reads and disaster recovery from region-wide outages. For more information, see Working with Amazon Aurora global database.</td>
<td>November 28, 2018</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Query plan management in Aurora PostgreSQL (p. 1316)</td>
<td>Aurora PostgreSQL now provides query plan management that you can use to manage PostgreSQL query execution plans. For more information, see Managing query execution plans for Aurora PostgreSQL.</td>
<td>November 20, 2018</td>
</tr>
<tr>
<td>Query editor for Aurora Serverless (beta) (p. 1316)</td>
<td>You can run SQL statements in the Amazon RDS console on Aurora Serverless clusters. For more information, see Using the query editor for Aurora Serverless.</td>
<td>November 20, 2018</td>
</tr>
<tr>
<td>Data API for Aurora Serverless (beta) (p. 1316)</td>
<td>You can access Aurora Serverless clusters with web services-based applications using the Data API. For more information, see Using the Data API for Aurora Serverless.</td>
<td>November 20, 2018</td>
</tr>
<tr>
<td>Aurora PostgreSQL version 2.1 (p. 1316)</td>
<td>Aurora PostgreSQL version 2.1 is available and compatible with PostgreSQL 10.5. For more information, see Version 2.1.</td>
<td>November 20, 2018</td>
</tr>
<tr>
<td>TLS support for Aurora Serverless (p. 1316)</td>
<td>Aurora Serverless clusters support TLS/SSL encryption. For more information, see TLS/SSL for Aurora Serverless.</td>
<td>November 19, 2018</td>
</tr>
<tr>
<td>Custom endpoints (p. 1316)</td>
<td>You can now create endpoints that are associated with an arbitrary set of DB instances. This feature helps with load balancing and high availability for Aurora clusters where some DB instances have different capacity or configuration than others. You can use custom endpoints instead of connecting to a specific DB instance through its instance endpoint. For more information, see Amazon Aurora connection management.</td>
<td>November 12, 2018</td>
</tr>
<tr>
<td>IAM authentication support in Aurora PostgreSQL (p. 1316)</td>
<td>Aurora PostgreSQL now supports IAM authentication. For more information see IAM database authentication.</td>
<td>November 8, 2018</td>
</tr>
<tr>
<td>Aurora MySQL version 2.03.1 (p. 919)</td>
<td>Aurora MySQL version 2.03.1 is available.</td>
<td>October 24, 2018</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Custom parameter groups for restore and point in time recovery</strong> (p. 1316)</td>
<td>You can now specify a custom parameter group when you restore a snapshot or perform a point in time recovery operation. For more information, see Restoring from a DB cluster snapshot and Restoring a DB cluster to a specified time.</td>
<td>October 15, 2018</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.03</strong> (p. 920)</td>
<td>Aurora MySQL version 2.03 is available.</td>
<td>October 11, 2018</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.02.5</strong> (p. 920)</td>
<td>Aurora MySQL version 2.02.5 is available.</td>
<td>October 8, 2018</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.17.7</strong> (p. 950)</td>
<td>Aurora MySQL version 1.17.7 is available.</td>
<td>October 8, 2018</td>
</tr>
<tr>
<td><strong>Deletion protection for Aurora DB clusters</strong> (p. 1316)</td>
<td>When you enable deletion protection for a DB cluster, the database cannot be deleted by any user. For more information, see Deleting a DB instance in a DB cluster.</td>
<td>September 26, 2018</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL version 2.0</strong> (p. 1316)</td>
<td>Aurora PostgreSQL version 2.0 is available and compatible with PostgreSQL 10.4. For more information, see Version 2.0.</td>
<td>September 25, 2018</td>
</tr>
<tr>
<td><strong>Stop/Start feature</strong> Aurora (p. 1316)</td>
<td>You can now stop or start an entire Aurora cluster with a single operation. For more information, see Stopping and starting an Aurora cluster.</td>
<td>September 24, 2018</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 2.02.4</strong> (p. 921)</td>
<td>Aurora MySQL version 2.02.4 is available.</td>
<td>September 21, 2018</td>
</tr>
<tr>
<td><strong>Parallel query feature for Aurora MySQL</strong> (p. 1316)</td>
<td>Aurora MySQL now offers an option to parallelize I/O work for queries across the Aurora storage infrastructure. This feature speeds up data-intensive analytic queries, which are often the most time-consuming operations in a workload. For more information, see Working with parallel query for Aurora MySQL.</td>
<td>September 20, 2018</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.18.0</strong> (p. 948)</td>
<td>Aurora MySQL version 1.18.0 is available.</td>
<td>September 20, 2018</td>
</tr>
<tr>
<td><strong>Aurora PostgreSQL version 1.3</strong> (p. 1316)</td>
<td>Aurora PostgreSQL version 1.3 is now available and is compatible with PostgreSQL 9.6.9. For more information, see Version 1.3.</td>
<td>September 11, 2018</td>
</tr>
<tr>
<td><strong>Aurora MySQL version 1.17.6</strong> (p. 951)</td>
<td>Aurora MySQL version 1.17.6 is available.</td>
<td>September 6, 2018</td>
</tr>
<tr>
<td><strong>New guide (p. 1316)</strong></td>
<td>This is the first release of the <em>Amazon Aurora User Guide</em>.</td>
<td>August 31, 2018</td>
</tr>
</tbody>
</table>
AWS glossary

For the latest AWS terminology, see the AWS glossary in the AWS General Reference.