

# Relational Database Service

## User Guide

**Issue** 01  
**Date** 2024-04-15



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

---

# Contents

---

<b>1 Introduction.....</b>	<b>1</b>
1.1 What Is RDS?.....	1
1.2 Basic Concepts.....	2
1.3 Advantages.....	3
1.3.1 Easy Management.....	3
1.3.2 High Security.....	4
1.3.3 High Reliability.....	5
1.3.4 Comparison Between RDS and Self-Built Databases.....	5
1.4 Product Series.....	6
1.4.1 DB Instance Introduction.....	6
1.4.2 Function Comparison.....	7
1.5 DB Instance Description.....	9
1.5.1 DB Instance Types.....	9
1.5.2 DB Instance Classes.....	10
1.5.3 DB Engines and Versions.....	12
1.5.4 DB Instance Statuses.....	13
1.6 Typical Applications.....	14
1.6.1 Read/Write Splitting.....	14
1.7 Permissions Management.....	14
1.8 Constraints.....	21
1.8.1 RDS for MySQL Constraints.....	21
1.8.2 RDS for PostgreSQL Constraints.....	27
1.9 Related Services.....	28
<b>2 Getting Started with RDS for MySQL.....</b>	<b>30</b>
2.1 Operation Guide.....	30
2.2 Step 1: Create a DB Instance.....	31
2.3 Step 2: Connect to a DB Instance.....	35
2.3.1 Connecting to a DB Instance.....	35
2.3.2 Connecting to an RDS for MySQL DB Instance Through a Private Network.....	37
2.3.2.1 Connecting to a DB Instance Through a Private Network.....	37
2.3.2.2 Configuring Security Group Rules.....	39
2.3.2.3 Connecting to a DB Instance Through a Private Network.....	40
2.3.3 Connecting to an RDS for MySQL DB Instance Through a Public Network.....	44

2.3.3.1 Connecting to a DB Instance Through a Public Network.....	44
2.3.3.2 Binding an EIP.....	45
2.3.3.3 Configuring Security Group Rules.....	46
2.3.3.4 Connecting to a DB Instance Through a Public Network.....	47
<b>3 Getting Started with RDS for PostgreSQL.....</b>	<b>52</b>
3.1 Operation Guide.....	52
3.2 Step 1: Create a DB Instance.....	53
3.3 Step 2: Connect to a DB Instance.....	57
3.3.1 Connecting to a DB Instance.....	57
3.3.2 Connecting to a DB Instance Through a Private Network.....	59
3.3.2.1 Connecting to a DB Instance Through a Private Network.....	59
3.3.2.2 Configuring Security Group Rules.....	60
3.3.2.3 Connecting to a DB Instance Through psql.....	62
3.3.3 Connecting to a DB Instance Through a Public Network.....	64
3.3.3.1 Connecting to a DB Instance Through a Public Network.....	64
3.3.3.2 Binding an EIP.....	65
3.3.3.3 Configuring Security Group Rules.....	65
3.3.3.4 Connecting to a DB Instance Through psql.....	66
<b>4 Working with RDS for MySQL.....</b>	<b>69</b>
4.1 Database Migration.....	69
4.1.1 Migrating Data to RDS for MySQL Using mysqldump.....	69
4.1.2 Migrating Data to RDS for MySQL Using the Export and Import Functions of DAS.....	72
4.2 Parameter Tuning.....	74
4.2.1 Suggestions on RDS for MySQL Parameter Tuning.....	74
4.3 Permissions Management.....	76
4.3.1 Creating a User and Granting Permissions.....	76
4.3.2 RDS Custom Policies.....	78
4.4 Instance Lifecycle.....	78
4.4.1 Creating a Same DB Instance as an Existing DB Instance.....	78
4.4.2 Rebooting DB Instances or Read Replicas.....	79
4.4.3 Selecting Displayed Items.....	80
4.4.4 Exporting DB Instance Information.....	81
4.4.5 Deleting a DB Instance or Read Replica.....	82
4.5 Instance Modifications.....	83
4.5.1 Changing a DB Instance Name.....	83
4.5.2 Changing the Failover Priority.....	83
4.5.3 Changing a DB Instance Class.....	84
4.5.4 Scaling up Storage Space.....	85
4.5.5 Changing the Maintenance Window.....	87
4.5.6 Changing a DB Instance Type from Single to Primary/Standby.....	88
4.5.7 Promoting a Read Replica Into a Single DB Instance.....	89
4.5.8 Manually Switching Between Primary and Standby DB Instances.....	90

4.5.9 Migrating a Standby DB Instance.....	91
4.6 Read Replicas.....	91
4.6.1 Introducing Read Replicas.....	92
4.6.2 Creating a Read Replica.....	93
4.6.3 Managing a Read Replica.....	95
4.7 Backups and Restorations.....	96
4.7.1 Working with Backups.....	96
4.7.2 Configuring an Automated Backup Policy.....	96
4.7.3 Setting a Cross-Region Backup Policy.....	97
4.7.4 Creating a Manual Backup.....	99
4.7.5 Downloading a Backup File.....	100
4.7.6 Downloading a Binlog Backup File.....	102
4.7.7 Restoring from Backup Files to DB Instances.....	103
4.7.8 Restoring a DB Instance to a Point in Time.....	105
4.7.9 Restoring a Table to a Point in Time.....	107
4.7.10 Replicating a Backup.....	108
4.7.11 Deleting a Manual Backup.....	109
4.8 Parameter Template Management.....	110
4.8.1 Creating a Parameter Template.....	110
4.8.2 Modifying Parameters.....	111
4.8.3 Exporting a Parameter Template.....	114
4.8.4 Comparing Parameter Templates.....	115
4.8.5 Viewing Parameter Change History.....	116
4.8.6 Replicating a Parameter Template.....	117
4.8.7 Resetting a Parameter Template.....	118
4.8.8 Applying a Parameter Template.....	119
4.8.9 Viewing Application Records of a Parameter Template.....	120
4.8.10 Modifying a Parameter Template Description.....	120
4.8.11 Deleting a Parameter Template.....	121
4.9 Connection Management.....	121
4.9.1 Configuring and Changing a Floating IP Address.....	121
4.9.2 Binding and Unbinding an EIP.....	122
4.9.3 Changing a Database Port.....	123
4.9.4 Configuring a Security Group Rule.....	125
4.10 Database Proxy (Read/Write Splitting).....	126
4.10.1 Introducing Read/Write Splitting.....	126
4.10.2 Best Practices for Database Proxy.....	127
4.10.3 Enabling Read/Write Splitting.....	129
4.10.4 Configuring Delay Threshold and Distributing Read Weight.....	130
4.10.5 Changing the Read/Write Splitting Address.....	132
4.10.6 Changing the Instance Class of a DB Proxy Instance.....	133
4.10.7 Upgrading the Kernel Version of Database Proxy.....	134

4.10.8 Enabling or Disabling Access Control.....	135
4.10.9 Disabling Read/Write Splitting.....	136
4.10.10 Rules for Distributing Weights.....	136
4.10.11 Testing Read/Write Splitting Performance.....	137
4.11 Data Security.....	137
4.11.1 Resetting the Administrator Password.....	137
4.11.2 Changing a Security Group.....	139
4.12 Metrics and Alarms.....	139
4.12.1 Configuring Displayed Metrics.....	140
4.12.2 Setting Alarm Rules.....	146
4.12.3 Viewing Monitoring Metrics.....	146
4.13 Log Management.....	147
4.13.1 Viewing and Downloading Error Logs.....	147
4.13.2 Viewing and Downloading Slow Query Logs.....	148
4.13.3 Viewing Failover/Switchover Logs.....	150
4.13.4 Enabling the SQL Audit Function.....	150
4.13.5 Downloading SQL Audit Logs.....	151
4.14 Task Center.....	153
4.14.1 Viewing a Task.....	153
4.14.2 Deleting a Task Record.....	154
<b>5 Working with RDS for PostgreSQL.....</b>	<b>155</b>
5.1 Database Migration.....	155
5.1.1 Migrating Data to RDS for PostgreSQL Using psql.....	155
5.1.2 Migrating Data to RDS for PostgreSQL Using the Export and Import Functions of DAS.....	157
5.2 Parameter Tuning.....	159
5.2.1 Suggestions on RDS for PostgreSQL Parameter Tuning.....	159
5.3 Permissions Management.....	160
5.3.1 Creating a User and Granting Permissions.....	160
5.3.2 RDS Custom Policies.....	161
5.4 Instance Lifecycle.....	162
5.4.1 Creating a Same DB Instance as an Existing DB Instance.....	162
5.4.2 Rebooting DB Instances or Read Replicas.....	163
5.4.3 Selecting Displayed Items.....	164
5.4.4 Exporting DB Instance Information.....	164
5.4.5 Deleting a DB Instance or Read Replica.....	165
5.5 Instance Modifications.....	166
5.5.1 Changing a DB Instance Name.....	167
5.5.2 Changing the Failover Priority.....	167
5.5.3 Changing a DB Instance Class.....	168
5.5.4 Scaling up Storage Space.....	169
5.5.5 Changing the Maintenance Window.....	171
5.5.6 Changing a DB Instance Type from Single to Primary/Standby.....	172

5.5.7 Manually Switching Between Primary and Standby DB Instances.....	173
5.5.8 Migrating a Standby DB Instance.....	174
5.6 Read Replicas.....	174
5.6.1 Introducing Read Replicas.....	175
5.6.2 Creating a Read Replica.....	176
5.6.3 Managing a Read Replica.....	178
5.7 Backups and Restorations.....	179
5.7.1 Working with Backups.....	179
5.7.2 Configuring an Automated Backup Policy.....	179
5.7.3 Set a Cross-Region Backup Policy.....	180
5.7.4 Creating a Manual Backup.....	182
5.7.5 Downloading a Full Backup File.....	183
5.7.6 Downloading an Incremental Backup File.....	185
5.7.7 Restoring from Backup Files to RDS for PostgreSQL.....	186
5.7.8 Restoring a DB Instance to a Point in Time.....	188
5.7.9 Replicating a Backup.....	190
5.7.10 Deleting a Manual Backup.....	191
5.8 Parameter Template Management.....	191
5.8.1 Creating a Parameter Template.....	191
5.8.2 Modifying Instance Parameters.....	193
5.8.3 Exporting a Parameter Template.....	195
5.8.4 Comparing Parameter Templates.....	196
5.8.5 Viewing Parameter Change History.....	197
5.8.6 Replicating a Parameter Template.....	198
5.8.7 Resetting a Parameter Template.....	198
5.8.8 Applying a Parameter Template.....	199
5.8.9 Viewing Application Records of a Parameter Template.....	200
5.8.10 Modifying a Parameter Template Description.....	200
5.8.11 Deleting a Parameter Template.....	201
5.9 Connection Management.....	201
5.9.1 Configuring and Changing a Floating IP Address.....	201
5.9.2 Binding and Unbinding an EIP.....	202
5.9.3 Changing a Database Port.....	204
5.9.4 Connecting to a DB Instance Through pgAdmin.....	204
5.10 Plugin Management.....	207
5.10.1 Creating or Deleting a Plugin.....	207
5.10.2 Supported Plugins.....	209
5.10.3 Using pg_repack.....	214
5.11 Tablespace Management.....	215
5.12 Data Security.....	217
5.12.1 Resetting the Administrator Password.....	217
5.12.2 Changing a Security Group.....	218

5.13 Metrics and Alarms.....	219
5.13.1 Configuring Displayed Metrics.....	219
5.13.2 Setting Alarm Rules.....	222
5.13.3 Viewing Monitoring Metrics.....	223
5.14 Log Management.....	224
5.14.1 Viewing Error Logs.....	224
5.14.2 Viewing Slow Query Logs.....	225
5.15 Task Center.....	227
5.15.1 Viewing a Task.....	227
5.15.2 Deleting a Task Record.....	227
<b>6 FAQs.....</b>	<b>229</b>
6.1 Product Consulting.....	229
6.1.1 What Should I Pay Attention to When Using RDS?.....	229
6.1.2 What Is the Availability of RDS DB Instances?.....	229
6.1.3 Does RDS Support Cross-AZ High Availability?.....	229
6.1.4 What Can I Do About Slow Responses of Websites When They Use RDS?.....	230
6.1.5 Can I Change the Replication Mode Between Primary DB Instances and Read Replicas?.....	230
6.1.6 What Is the Time Delay for Primary/Standby Replication?.....	230
6.1.7 What Are the Restrictions on MySQL DB Instances After GTID Is Enabled?.....	231
6.1.8 How Many Databases Can Run on an RDS DB Instance?.....	231
6.1.9 What Is the Maximum Size Allowed for a Single Table in MySQL Instances?.....	231
6.2 Resource and Disk Management.....	232
6.2.1 How Long Does It Take to Create a DB Instance?.....	232
6.2.2 Which Types of Logs and Files Occupy RDS Storage Space?.....	232
6.2.3 Which Items Occupy the Storage Space of My RDS DB Instances?.....	233
6.2.4 How Much Storage Space Is Required for DDL Operations?.....	233
6.3 Database Connection.....	233
6.3.1 What Should I Do If I Can't Connect to My RDS DB Instance?.....	233
6.3.2 Can an External Server Access the RDS Database?.....	237
6.3.3 What Do I Do If the Number of RDS Database Connections Reaches the Upper Limit?.....	237
6.3.4 What Is the Maximum Number of Connections to an RDS DB Instance?.....	238
6.3.5 How Can I Create and Connect to an ECS?.....	240
6.3.6 What Should I Do If an ECS Cannot Connect to an RDS DB Instance Through a Private Network?.....	240
6.3.7 What Should I Do If a Database Client Problem Causes a Connection Failure?.....	240
6.3.8 What Should I Do If an RDS Database Problem Causes a Connection Failure?.....	241
6.3.9 Do Applications Need to Support Reconnecting to the RDS DB Instance Automatically?.....	241
6.3.10 How Can I Connect to an RDS for PostgreSQL Database Through JDBC?.....	242
6.3.11 Why Cannot I Ping My EIP After It Is Bound to a DB Instance?.....	245
6.3.12 How Can I Obtain the IP Address of an Application?.....	245
6.3.13 Can I Access an RDS DB Instance Over an Intranet Connection Across Regions?.....	246
6.3.14 Why Did the New Password Not Take Effect After I Reset the Administrator Password?.....	247
6.3.15 How Do I Set the Encoding Format of the MySQL 8.0 Character Set?.....	247



6.3.16 What Should I Do If the ECS and RDS Are Deployed in Different VPCs and They Cannot Communicate with Each Other?.....	247
6.3.17 How Do I View All IP Addresses Connected to a Database?.....	247
6.3.18 Can I Access Standby RDS DB Instances?.....	248
6.3.19 How Do I Check the Connections to an RDS for MySQL Instance?.....	248
6.4 Database Migration.....	248
6.4.1 Why Do I Need to Use the mysqldump or pg_dump Tools for Migration?.....	248
6.4.2 What Should I Do When a Large Number of Binlog Files Cause Storage Space Insufficiency During an RDS MySQL Instance Migration?.....	249
6.4.3 What Types of DB Engines Does RDS Support for Importing Data?.....	249
6.5 Database Permission.....	249
6.5.1 Why Does the Root User Not Have the Super Permissions?.....	249
6.5.2 RDS for MySQL Built-in Accounts.....	250
6.5.3 Does RDS for MySQL Support Multiple Accounts?.....	250
6.5.4 How Do I View Authorized Databases After a Local Client Is Connected to a DB Instance?.....	250
6.6 Database Storage.....	251
6.6.1 What Storage Engines Does RDS for MySQL Support?.....	251
6.6.2 What Types of Storage Does RDS Use?.....	252
6.6.3 Does RDS for MySQL Support Stored Procedures and Functions?.....	252
6.6.4 What Should I Do If My Data Exceeds the Available Storage of an RDS for MySQL Instance?.....	252
6.6.5 How Do I View the Storage Usage of My RDS Instance?.....	253
6.7 Client Installation.....	253
6.7.1 How Can I Install the MySQL Client?.....	253
6.7.2 How Can I Install a PostgreSQL Client?.....	254
6.8 Database Usage.....	256
6.8.1 Does MySQL 8.0 Support Full-Text Search?.....	256
6.8.2 How Do I Use the mysqlbinlog Tool?.....	256
6.8.3 How Do I View Session IDs and Login and Logout Time of a Database?.....	257
6.8.4 Does the OPTIMIZE TABLE Operation Lock Tables on an RDS DB Instance?.....	257
6.9 Backup and Restoration.....	257
6.9.1 How Long Does RDS Store Backup Data For?.....	258
6.9.2 How Do I Clear RDS Backup Space?.....	258
6.9.3 Can My Database Be Used in the Backup Window?.....	258
6.9.4 How Do I View My Backup Storage Usage?.....	258
6.9.5 How Can I Back Up an RDS Database to an ECS?.....	259
6.9.6 Will Backups Be Retained After My RDS Instance Is Deleted?.....	259
6.9.7 Why Has My Automated Backup Failed?.....	259
6.9.8 Why Is a Table or Data Missing from My Database?.....	260
6.9.9 How Do I Restore a Local Database Backup to RDS?.....	260
6.9.10 Does RDS for PostgreSQL Support Table PITR?.....	261
6.9.11 Can I Dump Backup Files to OBS Buckets?.....	261
6.9.12 Does RDS for MySQL Support Table-Level Backup to a Specified OBS Bucket?.....	261
6.9.13 Can I Delete the RDS for MySQL Backup Policy?.....	261

6.10 Database Monitoring.....	261
6.10.1 Which DB Instance Monitoring Metrics Do I Need to Pay Attention To?.....	261
6.10.2 How Can I Calculate the Memory Usage of an RDS DB Instance?.....	262
6.10.3 How Do I Set an Alarm Rule for the Replication Delay Between Primary and Standby DB Instances?.....	262
6.11 Capacity Expansion and Specification Change.....	262
6.11.1 Are My RDS DB Instances Still Available During Storage Scale-up and Instance Class Change?....	262
6.11.2 Why Does the DB Instance Become Faulty After the Original Database Port Is Changed?.....	263
6.11.3 Can I Change the VPC that My RDS DB Instance Belongs To?.....	263
6.12 Database Parameter Modification.....	263
6.12.1 What Inappropriate Parameter Settings Cause Unavailability of the RDS for PostgreSQL Database? .....	263
6.12.2 How Can I Change the Time Zone?.....	264
6.12.3 How Do I Configure a Password Expiration Policy for RDS for MySQL DB Instances?.....	265
6.12.4 How Do I Change the RDS Transaction Isolation Level?.....	266
6.12.5 Does RDS for PostgreSQL Support the test_decoding Plugin?.....	267
6.12.6 How Do I Use the utf8mb4 Character Set to Store Emojis in an RDS for MySQL DB Instance?.....	267
6.12.7 Can I Use SQL Commands to Modify Global Parameters?.....	268
6.12.8 How Do I Set Case Sensitivity for RDS for MySQL Table Names?.....	269
6.12.9 Can I Enable Query Caching for My RDS for MySQL Instance?.....	269
6.13 Network Security.....	269
6.13.1 What Security Protection Policies Does RDS Have?.....	270
6.13.2 How Can Data Security Be Ensured During Transmission When I Access RDS Through an EIP?.....	270
6.13.3 How Can I Prevent Untrusted Source IP Addresses from Accessing RDS?.....	270
6.13.4 How Do I Configure a Security Group to Enable Access to RDS DB Instances?.....	270
6.13.5 How Can I Import the Root Certificate to a Windows or Linux OS?.....	271
6.13.6 How Can I Identify the Validity Period of an SSL Root Certificate?.....	272
6.13.7 What Are the Possible Causes for Data Corruption?.....	272
6.14 Version Upgrade.....	272
6.14.1 Does RDS for MySQL Support Version Upgrades?.....	272
6.14.2 Does RDS for MySQL Support Version Downgrades?.....	273
<b>A Change History.....</b>	<b>274</b>

# 1 Introduction

---

## 1.1 What Is RDS?

RDS is a reliable and scalable cloud database service that is easy to manage. RDS supports the following DB engines:

- [MySQL](#)
- [PostgreSQL](#)

RDS includes a comprehensive performance monitoring system, multi-level security measures, and a professional database management platform, allowing you to easily set up and scale up a relational database. On the RDS console, you can perform almost all necessary tasks and no programming is required. The console simplifies operations and reduces routine O&M workloads, so you can stay focused on application and service development.

### MySQL

MySQL is one of the world's most popular open-source relational databases. It works with the Linux, Apache, and Perl/PHP/Python to establish a LAMP model for efficient web solutions. RDS for MySQL is reliable, secure, scalable, inexpensive, and easy to manage.

- It supports various web applications and is cost-effective, preferred by small- and medium-sized enterprises.
- A web-based console provides comprehensive visualized monitoring for easier operations.
- You can flexibly scale resources based on your service requirements and pay for only what you use.

For details about the versions supported by RDS for MySQL, see [DB Engines and Versions](#).

For more information, see the official documentation at <https://dev.mysql.com/doc/>.

## PostgreSQL

PostgreSQL is an open-source object-relational database management system that focuses on extensibility and standards compliance. It is known as the most advanced open-source database available. RDS for PostgreSQL excels in processing complex online transaction processing (OLTP) transactions and supports NoSQL (JSON, XML, or hstore) and geographic information system (GIS) data types. It has earned a reputation for reliability and data integrity, and is widely used for websites, location-based applications, and complex data object processing.

- RDS for PostgreSQL supports the postgis plugin and provides excellent spatial performance.
- RDS for PostgreSQL is a good cost-effective solution for many different scenarios. You can flexibly scale resources based on your service requirements and pay for only what you use.

For details about the versions supported by RDS for PostgreSQL, see [DB Engines and Versions](#).

For more information, see the official documentation at <https://www.postgresql.org/docs/>.

## 1.2 Basic Concepts

### DB Instances

The smallest management unit of RDS is the DB instance. A DB instance is an isolated database environment on the cloud. Each DB instance runs a DB engine. For details about DB instance types, specifications, engines, versions, and statuses, see [DB Instance Description](#).

### DB Engines

RDS supports the following DB engines:

- MySQL
- PostgreSQL

For details about the supported versions, see [DB Engines and Versions](#).

### DB Instance Types

RDS DB instances are classified into the following types: single and primary/standby.

For details about DB instance types, see [DB Instance Introduction](#) and [Function Comparison](#).

### DB Instance Classes

The DB instance class determines the compute (vCPUs) and memory capacity (memory size) of a DB instance. For details, see [DB Instance Classes](#).

## Automated Backups

When you create a DB instance, an automated backup policy is enabled by default. After the DB instance is created, you can modify the policy. RDS will automatically create full backups for DB instances based on your settings.

## Manual Backups

Manual backups are user-initiated full backups of DB instances. They are retained until you delete them manually.

## Regions and AZs

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are defined by their geographical location and network latency. Each region is completely independent, improving fault tolerance and stability. After a resource is created, its region cannot be changed.
- An AZ is a physical location using independent power supplies and networks. Faults in an AZ do not affect other AZs. A region can contain multiple AZs, which are physically isolated but interconnected through internal networks. This ensures the independence of AZs and provides low-cost and low-latency network connections.

**Figure 1-1** shows the relationship between regions and AZs.

**Figure 1-1** Regions and AZs



## 1.3 Advantages

### 1.3.1 Easy Management

#### Quick Setup

You can create a DB instance on the management console within minutes and access RDS from an ECS to reduce the application response time and avoid paying for the traffic that would be generated by regular public access.

## Elastic Scaling

Cloud Eye monitors changes in the load on your database and storage capacity. You can flexibly scale resources accordingly and pay for only what you use.

## High Compatibility

You use RDS database engines (DB engines) the same way as you would use a native engine. RDS is compatible with existing programs and tools.

## Easy O&M

Routine RDS maintenance and management operations, including hardware and software fault handling and database patch updates, are easy to perform. With the web-based console, you can reboot DB instances, reset passwords, modify parameters, view error or slow query logs, and restore data. Additionally, the system helps you monitor DB instances in real time and generates alarms if errors occur. You can check DB instance information at any time, including CPU usage, IOPS, database connections, and storage space usage.

## 1.3.2 High Security

### Network Isolation

RDS uses Virtual Private Cloud (VPC) and network security groups to isolate and secure your DB instances. VPCs allow you to define what IP address range can access RDS. You can configure subnets and security groups to control access to DB instances.

### Access Control

RDS controls access through the domain/IAM user and security groups. When you create an RDS DB instance, a domain is automatically created. To separate out specific permissions, you can create IAM users and assign permissions to them as needed. VPC security groups have rules that govern both inbound and outbound traffic for DB instances.

### Transmission Encryption

RDS uses Transport Layer Security (TLS) and Secure Sockets Layer (SSL) to encrypt transmission. You can download a Certificate Agency (CA) certificate from the RDS console and upload it when connecting to a database for authentication.

### Data Deletion

When you delete an RDS DB instance, its attached disks, storage space its automated backups occupy, and all data it stores will be deleted. You can restore a deleted DB instance using a manual backup.

### Anti-DDoS

When you connect to an RDS DB instance through a public network, there may be risks of a distributed denial-of-service (DDoS) attack. If the RDS security system

detects a DDoS attack, it will enable the anti-DDoS function. If the function cannot defend against the attack or the attack reaches the black hole threshold, black hole processing is triggered to ensure availability of the RDS service.

## Security Protection

RDS is protected by multiple layers of firewalls to defend against various malicious attacks, such as DDoS attacks and SQL injections. For security reasons, you are advised to access RDS through a private network.

### 1.3.3 High Reliability

#### Dual-Host Hot Standby

RDS uses the hot standby architecture, in which failover upon fault occurrence takes only some seconds.

#### Data Backup

RDS automatically backs up data every day and transfers backup files to Object Storage Service (OBS). The backup files can be stored for 732 days and can be restored with just a few clicks. You can set a custom backup policy and create manual backups at any time.

#### Data Restoration

You can restore data from backups to any point in time during the backup retention period. In most scenarios, you can use backup files to restore data to a new DB instance at any time point within 732 days. After the data is verified, data can be migrated back to the primary DB instance.

### 1.3.4 Comparison Between RDS and Self-Built Databases

#### Performance

Item	Cloud Database RDS	Self-Built Database Service
Service availability	For details, see the <i>Elastic Cloud Server User Guide</i> .	Requires device procurement, primary/standby relationship setup, and RAID setup.
Data reliability	For more information, see the <i>Elastic Volume Service User Guide</i> .	Requires device procurement, primary/standby relationship setup, and RAID setup.
System security	Defends against DDoS attacks and promptly repairs database security vulnerabilities.	Requires procurement of expensive devices and software, as well as manual detection and repair of security vulnerabilities.

Item	Cloud Database RDS	Self-Built Database Service
Database backup	Supports automated backups, manual backups, and custom backup retention periods.	Requires device procurement, setup, and maintenance.
Hardware and software investment	Supports on-demand pricing and scaling without requiring hardware and software investment.	Requires large investment in database servers.
System hosting	Not required.	Requires two servers for primary/standby DB instances.
Maintenance cost	Not required.	Requires large manpower investment and professional database administrator (DBA) for maintenance.
Deployment and scaling	Supports elastic scaling, fast upgrade, and on-demand enabling.	Requires procurement, deployment, and coordination of hardware that matches original devices.
Resource utilization	Bills users based on the resources actually used, resulting in 100% resource utilization.	Considers peak traffic, resulting in low resource utilization.

## 1.4 Product Series

### 1.4.1 DB Instance Introduction

Currently, RDS DB instances are classified into the following types:

- Single
- Primary/Standby

Different series support different DB engines and instance specifications.



**Table 1-1** DB instance types

DB Instance Type	Description	Notes	Scenarios
Single	Uses a single-node architecture. More cost-effective than the mainstream primary/standby DB instances.	If a fault occurs on a single instance, the instance cannot recover in a timely manner.	<ul style="list-style-type: none"> <li>• Personal learning</li> <li>• Microsites</li> <li>• Development and testing environment of small- and medium-sized enterprises</li> </ul>
Primary/Standby	Uses an HA architecture. A pair of primary and standby DB instances shares the same IP address and can be deployed in different AZs.	<ul style="list-style-type: none"> <li>• When a primary instance is being created, a standby instance is provisioned synchronously to provide data redundancy. The standby instance is invisible to you after being created.</li> <li>• If a failover occurs due to a primary instance failure, your database client will be disconnected for a short period of time. You need to reconnect the client to the instance.</li> </ul>	<ul style="list-style-type: none"> <li>• Production databases of large- and medium-sized enterprises</li> <li>• Applications for the Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other industries</li> </ul>

## 1.4.2 Function Comparison

Single DB instances use a single-node architecture. Different from the primary/standby DB instances, a single DB instance contains only one node and has no slave node for fault recovery.

### Advantage Comparison

- Single DB instances: support the creation of read replicas and support the queries of error logs and slow query logs. Different from primary/standby DB instances that have two database nodes, a single DB instance has only one node. If the node fails, the restoration will take a long time. Therefore, single

DB instances are not recommended for sensitive services that have high requirements on database availability.

- Primary/Standby DB instances: use the slave database node only for failover and restoration. The slave database node does not provide services. The performance of single DB instances is similar to or even higher than the primary/standby DB instances.

**Table 1-2** Function comparisons

Function	Single	Primary/Standby
Number of nodes	1	2
Specifications	vCPUs: a maximum of 32 Memory: a maximum of 128 GB Storage: a maximum of 4,000 GB	vCPUs: a maximum of 32 Memory: a maximum of 128 GB Storage: a maximum of 4,000 GB
Monitoring and alarms	Supported	Supported
Security group	Supported	Supported
Backups and restorations	Supported	Supported
Parameter settings	Supported	Supported
SSL	Supported	Supported
Log management	Supported	Supported
Read replicas (need to be created)	Supported	Supported
High-frequency monitoring	Supported	Supported
Primary/standby switchover or failover	Not supported	Supported
Standby DB instance migration	Not supported	Supported
Manual primary/standby switchover	Not supported	Supported

Function	Single	Primary/Standby
Instance class change	Supported	Supported

## 1.5 DB Instance Description

### 1.5.1 DB Instance Types

The smallest management unit of RDS is the DB instance. A DB instance is an isolated database environment on the cloud. Each DB instance can contain multiple user-created databases, and you can access a DB instance using the same tools and applications that you use with a stand-alone DB instance. You can create and modify DB instances using the management console or APIs. RDS does not have limits on the number of running DB instances. Each DB instance has a DB instance identifier.

DB instances are classified into the following types.

**Table 1-3** DB instance types

DB Instance Type	Description	Notes
Single	Uses a single-node architecture. More cost-effective than primary/standby DB instances.	If a fault occurs on a single instance, the instance cannot recover in a timely manner.
Primary/Standby	Uses an HA architecture. A pair of primary and standby instances has the same instance class.	<ul style="list-style-type: none"> <li>When a primary instance is being created, a standby instance is provisioned synchronously to provide data redundancy. The standby instance is invisible to you after being created.</li> <li>If a failover occurs due to a primary instance failure, your database client will be disconnected for a short period of time. You need to reconnect the client to the instance.</li> </ul>

DB Instance Type	Description	Notes
Read replica	Uses a single-node architecture (without a standby node).	<ul style="list-style-type: none"> <li>• A read replica is a single-node instance. If the physical server hosting a read replica is faulty or database replication between the read replica and its primary instance is abnormal, it takes a long time to rebuild and restore the read replica (depending on the data volume).</li> <li>• Database proxy is recommended for read-intensive workloads. Before using database proxy, ensure that you have purchased more than one read replica. If a single read replica is faulty, database proxy can distribute traffic to other read replicas.</li> </ul>

You can use RDS to create and manage DB instances running various DB engines.

For details about differences and function comparison between different instance types, see [DB Instance Introduction](#) and [Function Comparison](#).

## 1.5.2 DB Instance Classes

General-enhanced and general-enhanced II instance classes provide robust and stable performance. They use latest-generation network acceleration engines and Data Plane Development Kit (DPDK) to provide higher network performance, meeting requirements in different scenarios.

- General-enhanced DB instances use Intel® Xeon® Scalable processors and feature high and stable computing performance. Working in high-performance networks, general-enhanced DB instances provide higher performance and stability, meeting enterprise-class application requirements.
- General-enhanced II DB instances use second-generation Intel® Xeon® Scalable processors with technologies optimized and 25GE high-speed intelligent NICs to offer powerful and stable computing performance, including ultra-high network bandwidth and PPS.

**Table 1-4** DB instance classes

Instance Class	vCPUs	Memory (GB)	Supported DB Engine
General-enhanced	2	4	<ul style="list-style-type: none"> <li>• MySQL</li> <li>• PostgreSQL</li> </ul>

Instance Class	vCPUs	Memory (GB)	Supported DB Engine
	2	8	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	4	8	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	4	16	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	8	16	MySQL
	8	32	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	16	32	MySQL
	16	64	MySQL
	32	64	MySQL
	32	128	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	60	128	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	60	256	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
General-enhanced II	2	4	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	2	8	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	2	16	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	4	8	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	4	16	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	4	32	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	8	16	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>

Instance Class	vCPUs	Memory (GB)	Supported DB Engine
	8	32	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	8	64	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	16	32	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	16	64	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	16	128	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	32	64	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	32	128	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	64	128	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	64	256	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>
	64	512	<ul style="list-style-type: none"> <li>MySQL</li> <li>PostgreSQL</li> </ul>

The DB instance specifications vary according to site requirements.

### 1.5.3 DB Engines and Versions

**Table 1-5** lists the DB engines and versions supported by RDS.

For new applications, you are advised to use the latest major version of the DB engine, for example, MySQL 8.0. When you create a DB instance, you can select a major DB engine version only (such as MySQL 8.0). The system will automatically select an appropriate minor version (such as 8.0.17) for you. After the DB instance is created, you can view the minor version in the **DB Engine Version** column on the **Instance Management** page. The DB engine and version vary according to site requirements.

**Table 1-5** DB engines and versions

DB Engine	Single	Primary/Standby	Cluster
MySQL	<ul style="list-style-type: none"> <li>• 8.0</li> <li>• 5.7</li> <li>• 5.6</li> </ul>	<ul style="list-style-type: none"> <li>• 8.0</li> <li>• 5.7</li> <li>• 5.6</li> </ul>	Not supported
PostgreSQL	<ul style="list-style-type: none"> <li>• 14</li> <li>• 13</li> <li>• 12</li> <li>• 11</li> <li>• 10</li> <li>• 9.6</li> </ul>	<ul style="list-style-type: none"> <li>• 14</li> <li>• 13</li> <li>• 12</li> <li>• 11</li> <li>• 10</li> <li>• 9.6</li> </ul>	Not supported

## 1.5.4 DB Instance Statuses

### DB Instance Statuses

The status of a DB instance indicates the health of the DB instance. You can use the management console or API to view the status of a DB instance.

**Table 1-6** DB instance statuses

Status	Description
Available	A DB instance is available.
Abnormal	A DB instance is abnormal.
Creating	A DB instance is being created.
Creation failed	A DB instance has failed to be created.
Switchover in progress	A standby DB instance is being switched over to the primary DB instance.
Changing type to primary/standby	A single DB instance is being changed to primary/standby DB instances.
Rebooting	A DB instance is being rebooted.
Changing port	A DB instance port is being changed.
Changing instance class	The CPU or memory of a DB instance is being modified.
Changing proxy instance class	The CPU or memory of a DB proxy instance is being modified.
Scaling up	Storage space of a DB instance is being scaled up.

Status	Description
Backing up	A DB instance is being backed up.
Restoring	A DB instance is in the process of being restored from a backup.
Restore failed	A DB instance fails to be restored.
Storage full	Storage space of a DB instance is full. Data cannot be written to databases.
Deleted	A DB instance has been deleted and will not be displayed in the instance list.
Parameter change. Pending reboot	A modification to a database parameter is waiting for an instance reboot before it can take effect.

## 1.6 Typical Applications

### 1.6.1 Read/Write Splitting

For RDS for MySQL and RDS for PostgreSQL, the primary DB instances and read replicas have independent connection addresses. A maximum of five read replicas can be created for each RDS for MySQL or RDS for PostgreSQL DB instance. For details about how to create a read replica, see [Creating a Read Replica](#) and [Managing a Read Replica](#).

To offload read pressure on the primary DB instance, you can create one or more read replicas in the same region as the primary instance. These read replicas can process a large number of read requests and increase application throughput. You need to separately configure connection addresses for the primary DB instance and each read replica on your applications so that all read requests can be sent to read replicas and write requests to the primary DB instance.

## 1.7 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your RDS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use RDS resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using RDS resources.



If your account does not need individual IAM users for permissions management, you may skip over this chapter.

IAM can be used free of charge. You pay only for the resources in your account.

## RDS Permissions

RDS is a project-level service deployed and accessed in specific physical regions. To assign RDS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing RDS, users need to switch to a region where they have been authorized to use RDS.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you need to also assign other roles on which the permissions depend to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control.

[Table 1-7](#) lists all the system-defined roles and policies supported by RDS.

**Table 1-7** System policy summary

Policy Name/ System Role	Description	Category	Dependencies
RDS FullAccess	Full permissions for Relational Database Service	System-defined policy	N/A
RDS ReadOnlyAccesses	Read-only permissions for Relational Database Service	System-defined policy	N/A
RDS Administrator	Administrator permissions for RDS	System-defined role	The <b>Tenant Guest</b> and <b>Server Administrator</b> roles need to be assigned in the same project.

[Table 1-8](#) lists the common operations supported by each system policy of RDS. Please choose proper system policies according to this table.

**Table 1-8** Common operations supported by the RDS system policies

Operation	RDS FullAccess	RDS ReadOnlyAccess	RDS Administrator
Creating an RDS DB instance	√	x	√
Deleting an RDS DB instance	√	x	√
Querying an RDS DB instance list	√	√	√

**Table 1-9** Common operations and supported actions

Operation	Actions	Remarks
Creating a DB instance	rds:instance:create rds:param:list	To select a VPC, subnet, and security group, configure the following actions: vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get
Changing DB instance specifications	rds:instance:modifySpec	N/A
Scaling up storage space	rds:instance:extendSpace	N/A
Changing a DB instance type from single to primary/standby	rds:instance:singleToHa	N/A
Rebooting a DB instance	rds:instance:restart	N/A
Deleting a DB instance	rds:instance:delete	N/A
Querying a DB instance list	rds:instance:list	N/A

Operation	Actions	Remarks
Querying DB instance details	rds:instance:list	If the VPC, subnet, and security group are displayed in the DB instance list, you need to configure vpc:*:get and vpc:*:list.
Changing a DB instance password	rds:password:update	N/A
Changing a database port	rds:instance:modifyPort	N/A
Changing a floating IP address	rds:instance:modifyIp	To query the list of unused IP addresses, configure the following actions: vpc:subnets:get vpc:ports:get
Changing a DB instance name	rds:instance:modify	N/A
Changing a maintenance window	rds:instance:modify	N/A
Performing a manual switchover	rds:instance:switchover	N/A
Changing the replication mode	rds:instance:modifySynchronizeModel	N/A
Changing the failover priority	rds:instance:modifyStrategy	N/A
Changing a security group	rds:instance:modifySecurityGroup	N/A
Binding or unbinding an EIP	rds:instance:modifyPublicAccess	To query public IP addresses, configure the following actions: vpc:publicips:get vpc:publicips:list
Modifying the recycling policy	rds:instance:setRecycleBin	N/A
Querying the recycling policy	rds:instance:list	N/A
Enabling or disabling SSL	rds:instance:modifySSL	N/A

Operation	Actions	Remarks
Enabling or disabling event scheduler	rds:instance:modifyEvent	N/A
Configuring read/write splitting	rds:instance:modifyProxy	N/A
Applying for a private domain name	rds:instance:createDns	N/A
Migrating a standby DB instance to another AZ	rds:instance:create	N/A
Restoring tables to a specified point in time	rds:instance:tableRestore	N/A
Changing host permission	rds:instance:modifyHost	N/A
Querying hosts of the corresponding database account	rds:instance:list	N/A
Obtaining a parameter template list	rds:param:list	N/A
Creating a parameter template	rds:param:create	N/A
Modifying parameters in a parameter template	rds:param:modify	N/A
Applying a parameter template	rds:param:apply	N/A
Modifying parameters of a specified DB instance	rds:param:modify	N/A
Obtaining the parameter template of a specified DB instance	rds:param:list	N/A
Obtaining parameters of a specified parameter template	rds:param:list	N/A
Deleting a parameter template	rds:param:delete	N/A

Operation	Actions	Remarks
Resetting a parameter template	rds:param:reset	N/A
Comparing parameter templates	rds:param:list	N/A
Saving parameters in a parameter template	rds:param:save	N/A
Querying a parameter template type	rds:param:list	N/A
Setting an automated backup policy	rds:instance:modifyBackupPolicy	N/A
Querying an automated backup policy	rds:instance:list	N/A
Creating a manual backup	rds:backup:create	N/A
Obtaining a backup list	rds:backup:list	N/A
Obtaining the link for downloading a backup file	rds:backup:download	N/A
Deleting a manual backup	rds:backup:delete	N/A
Replicating a backup	rds:backup:create	N/A
Querying the restoration time range	rds:instance:list	N/A
Restoring data to a new DB instance	rds:instance:create	To select a VPC, subnet, and security group, configure the following actions: vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get
Restoring data to an existing or original DB instance	rds:instance:restoreInPlace	N/A

Operation	Actions	Remarks
Obtaining the binlog clearing policy	rds:binlog:get	N/A
Merging binlog files	rds:binlog:merge	N/A
Downloading a binlog file	rds:binlog:download	N/A
Deleting a binlog file	rds:binlog:delete	N/A
Configuring a binlog clearing policy	rds:binlog:setPolicy	N/A
Obtaining a database backup file list	rds:backup:list	N/A
Obtaining a backup database list at a specified time point	rds:backup:list	N/A
Querying a database error log	rds:log:list	N/A
Querying a database slow log	rds:log:list	N/A
Downloading a database error log	rds:log:download	N/A
Downloading a database slow log	rds:log:download	N/A
Enabling or disabling the audit log function	rds:auditlog:operate	N/A
Obtaining an audit log list	rds:auditlog:list	N/A
Querying the audit log policy	rds:auditlog:list	N/A
Obtaining the link for downloading an audit log	rds:auditlog:download	N/A
Obtaining a switchover log	rds:log:list	N/A
Creating a database	rds:database:create	N/A
Querying details about databases	rds:database:list	N/A

Operation	Actions	Remarks
Querying authorized databases of a specified user	rds:database:list	N/A
Dropping a database	rds:database:drop	N/A
Creating a database account	rds:databaseUser:create	N/A
Querying details about database accounts	rds:databaseUser:list	N/A
Querying authorized accounts of a specified database	rds:databaseUser:list	N/A
Deleting a database account	rds:databaseUser:drop	N/A
Authorizing a database account	rds:databasePrivilege:grant	N/A
Revoking permissions of a database account	rds:databasePrivilege:revoke	N/A
Viewing a task center list	rds:task:list	N/A
Deleting a task from the task center	rds:task:delete	N/A
Adding nodes	rds:instance:expandCluster	N/A

## 1.8 Constraints

### 1.8.1 RDS for MySQL Constraints

The following tables show the constraints designed to ensure the stability and security of RDS for MySQL.

#### Specifications

**Table 1-10** Specifications

Item	Constraints
Storage space	<ul style="list-style-type: none"> <li>Cloud SSD: 40 GB to 4,000 GB</li> <li>Extreme SSD: 40 GB to 4,000 GB</li> </ul>

Item	Constraints
Connections	A maximum of 100,000
IOPS	<ul style="list-style-type: none"> <li>• Cloud SSD: a maximum of 50,000</li> <li>• Extreme SSD: a maximum of 128,000</li> </ul>

## Naming

**Table 1-11** Naming

Item	Constraints
Instance name	<ul style="list-style-type: none"> <li>• 4 to 64 characters long.</li> <li>• Must start with a letter. Only letters (case sensitive), digits, hyphens (-), and underscores (_) are allowed.</li> </ul>
Database name	<ul style="list-style-type: none"> <li>• 1 to 64 characters long</li> <li>• Only letters, digits, hyphens (-), underscores (_), and dollar signs (\$) are allowed. The total number of hyphens (-) and dollar signs (\$) cannot exceed 10. (RDS for MySQL 8.0 does not support dollar signs (\$).)</li> </ul>
Account name	<ul style="list-style-type: none"> <li>• RDS for MySQL 5.6: The account name must be 1 to 16 characters long. Only letters, digits, hyphens (-), and underscores (_) are allowed.</li> <li>• RDS for MySQL 5.7 and 8.0: The account name must be 1 to 32 characters long. Only letters, digits, hyphens (-), and underscores (_) are allowed.</li> </ul>
Backup name	<ul style="list-style-type: none"> <li>• 4 to 64 characters long</li> <li>• Must start with a letter. Only letters (case sensitive), digits, hyphens (-), and underscores (_) are allowed.</li> </ul>
Parameter template name	<ul style="list-style-type: none"> <li>• 1 to 64 characters long</li> <li>• Only letters (case sensitive), digits, hyphens (-), underscores (_), and periods (.) are allowed.</li> </ul>



## Security

**Table 1-12** Security

Item	Constraints
root permissions	<p>Only the administrator account <b>root</b> is provided on the instance creation page. For details about the supported permissions, see <a href="#">root Permissions</a>.</p> <p><b>NOTE</b> Running <b>revoke</b>, <b>drop user</b>, or <b>rename user</b> on <b>root</b> may cause service interruption. Exercise caution when running any of these statements.</p>
root password	<ul style="list-style-type: none"> <li>• 8 to 32 characters long</li> <li>• Must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@\$#%^*_-=+?,()&amp;).</li> </ul> <p>For more information, see <a href="#">Resetting the Administrator Password</a>.</p>
Database port	<p>1024 to 65535 (excluding 12017 and 33071, which are occupied by the RDS system)</p> <p>For more information, see <a href="#">Changing a Database Port</a>.</p>
VPC	<p>The VPC where a DB instance is located cannot be changed after the instance is created.</p>
Security group	<ul style="list-style-type: none"> <li>• By default, you can create a maximum of 100 security groups in your cloud account.</li> <li>• By default, you can add up to 50 security group rules to a security group. For more information, see <a href="#">Configuring Security Group Rules</a>.</li> <li>• One RDS DB instance can be associated with multiple security groups, and one security group can be associated with multiple RDS DB instances.</li> <li>• When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. For more information, see <a href="#">Changing a Security Group</a>.</li> </ul>

Item	Constraints
System account	<p>To provide O&amp;M services, the system automatically creates system accounts when you create RDS for MySQL DB instances. These system accounts are unavailable to you.</p> <ul style="list-style-type: none"> <li>● <b>rdsAdmin</b>: a management account with the highest permission. It is used to query and modify instance information, rectify faults, migrate data, and restore data.</li> <li>● <b>rdsRepl</b>: a replication account, used to synchronize data from the primary instance to the standby instance or read replicas.</li> <li>● <b>rdsBackup</b>: a backup account, used for backend backup.</li> <li>● <b>rdsMetric</b>: a metric monitoring account used by watchdog to collect database status data.</li> <li>● <b>rdsProxy</b>: a database proxy account, used for authentication when the database is connected through the read/write splitting address. This account is automatically created when you enable read/write splitting.</li> </ul>
Instance parameter	<p>To ensure the optimal performance of RDS, you can modify parameters in the parameter template you created as needed.</p>

## Instance Operations

**Table 1-13** Instance operations

Item	Constraints
RDS for MySQL storage engine	<p>Only the InnoDB storage engine is supported. MyISAM, FEDERATED, and MEMORY are not supported.</p>
Instance deployment	<p>s where DB instances are deployed are not directly visible to you. You can only access the DB instances through IP addresses and database ports.</p>

Item	Constraints
Data migration	<p>You can migrate data from DDM, GaussDB, GaussDB(for MySQL), self-managed MySQL databases, self-managed Oracle databases, or MySQL databases built on other clouds to RDS for MySQL, or from one RDS for MySQL instance to another RDS for MySQL instance.</p> <p>Data migration tools include Data Replication Service (DRS), mysqldump, and Data Admin Service (DAS). You are advised to use DRS because it is easy to use and can complete a migration task in minutes. DRS facilitates data transfer between databases, helping you reduce DBA labor costs and hardware costs.</p> <p>For more information, see <a href="#">Migrating Data to RDS for MySQL Using mysqldump</a>.</p>
Primary/Standby replication	<p>RDS for MySQL uses a primary/standby dual-node replication cluster. You do not need to set up replication additionally. The standby DB instance is not visible to you and therefore you cannot access it directly.</p>
High CPU usage	<p>If the CPU usage is high or close to 100%, data read/write and database access will become slow, and an error will be reported during data deletion.</p>
Full storage	<p>There is not enough storage available for a DB instance and the instance becomes read-only, so applications cannot write any data to the instance.</p>
Number of tables	<p>RDS for MySQL supports a maximum of 500,000 tables. If there are more than 500,000 tables, database backup or a minor version upgrade may fail.</p>
Rebooting a DB instance	<p>DB instances cannot be rebooted through commands. They must be rebooted through the RDS console.</p>
Viewing backups	<p>You can download automated and manual backups for local storage. To download a backup, you can use OBS Browser+, the current browser, or the download URL.</p> <p>For more information, see <a href="#">Downloading a Backup File</a>.</p>
Log management	<ul style="list-style-type: none"> <li>• RDS for MySQL logging is enabled by default and cannot be disabled.</li> <li>• Binary logging is enabled for RDS for MySQL by default and uses row-based logging.</li> <li>• Read replicas do not provide binlogs.</li> </ul>
Recycle bin	<p>RDS allows you to move deleted pay-per-use DB instances to the recycle bin. You can rebuild a DB instance that was deleted up to 7 days ago from the recycle bin.</p>

## root Permissions

**Table 1-14** root permissions

Permission	Level	Description	Supported
Select	Table	Query permissions	Yes
Insert	Table	Insert permissions	
Update	Table	Update permissions	
Delete	Table	Delete permissions	
Create	Database, table, or index	Permissions of creating databases, tables, or indexes	
Drop	Database or table	Permissions of deleting databases or tables	
Reload	Server management	Permissions of running the following commands: flush-hosts, flush-logs, flush-privileges, flush-status, flush-tables, flush-threads, refresh, and reload	
Process	Server management	Permissions of viewing processes	
Grant	Database, table, or stored program	Permissions of granting access control	
References	Database or table	Foreign key operation permissions	
Index	Table	Index permissions	
Alter	Table	Permissions of altering tables, such as adding fields or indexes	
Show_db	Server management	Permissions of viewing database connections	
Create_tmp_table	Server management	Permissions of creating temporary tables	
Lock_tables	Server management	Permissions of locking tables	

Permission	Level	Description	Supported
Execute	Stored procedure	Permissions of executing storage procedures	
Repl_slave	Server management	Replication permissions	
Repl_client	Server management	Replication permissions	
Create_view	View	Permissions of creating views	
Show_view	View	Permissions of viewing views	
Create_routine	Stored procedure	Permissions of creating storage procedures	
Alter_routine	Stored procedure	Permissions of altering storage procedures	
Create_user	Server management	Permissions of creating users	
Event	Database	Event triggers	
Trigger	Database	Triggers	
Super	Server management	Permissions of killing threads	No
File	File on the server	Permissions of accessing files on database server nodes	No
Shutdown	Server management	Permissions of shutting down databases	
Create_tablespace	Server management	Permissions of creating tablespaces	

## 1.8.2 RDS for PostgreSQL Constraints

**Table 1-15** shows the constraints designed to ensure the stability and security of RDS for PostgreSQL.

**Table 1-15** Function constraints

Function Item	Constraints
Database access	<ul style="list-style-type: none"> <li>If public accessibility is not enabled, the RDS DB instance must be in the same VPC as the ECS.</li> <li>RDS read replicas must be created in the same subnet as the primary DB instance.</li> <li>The security group must allow access from the ECS. By default, RDS cannot be accessed through an ECS in a different security group. You need to add an inbound rule to the RDS security group.</li> <li>The default port of RDS for PostgreSQL instances is <b>5432</b>. You can change it if you want to access an instance through another port.</li> </ul>
Deployment	EC2s in which DB instances are deployed are not visible to users. You can access the DB instances only through an IP address and a port number.
Database root permissions	Only the <b>root</b> user permissions are provided on the instance creation page.
Database parameter modification	Most parameters can be modified on the RDS console.
Data migration	Use <code>psql</code> to import data by referring to <a href="#">Migrating Data to RDS for PostgreSQL Using psql</a> .
Database replication setup	RDS for PostgreSQL uses a primary/standby dual-node replication cluster. You do not need to set up replication additionally. The standby DB instance is not visible to users and therefore you cannot access it directly.
DB instance reboot	DB instances cannot be rebooted through commands. They must be rebooted through the RDS console.
RDS backup files	For details, see <a href="#">Downloading a Full Backup File</a> .

## 1.9 Related Services

**Table 1-16** Related services

Service Name	Description
Elastic Cloud Server (ECS)	Enables you to access RDS DB instances through an internal network. You can then access applications faster and you do not need to pay for public network traffic.

Service Name	Description
Virtual Private Cloud (VPC)	Isolates your networks and controls access to your RDS DB instances.
Object Storage Service (OBS)	Stores automated and manual backups of your RDS DB instances.
Cloud Eye	Monitors RDS resources in real time and reports alarms and warnings promptly.

# 2 Getting Started with RDS for MySQL

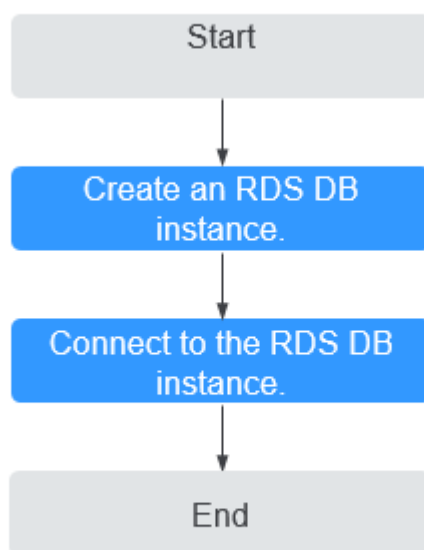
---

## 2.1 Operation Guide

You can create and connect to DB instances on the RDS console.

### Flowchart

Figure 2-1 Flowchart





## Procedure

**Table 2-1** Related operations and references

Operation	Reference
Creating an RDS DB instance	<a href="#">Step 1: Create a DB Instance</a>
Connecting to an RDS DB Instance	<a href="#">Step 2: Connect to a DB Instance</a>


## 2.2 Step 1: Create a DB Instance

### Scenarios

This section describes how to create a DB instance on the management console.

RDS allows you to tailor your computing resources and storage space to your business needs.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click **Create DB Instance**.
- Step 5** On the displayed page, configure information about your DB instance. Then, click **Create Now**.
  - Basic information

**Table 2-2** Basic information

Parameter	Description
Region	Region where the tenant is located. You can select a region from the drop-down list box. <b>NOTE</b> Products in different regions cannot communicate with each other through a private network. After a DB instance is created, the region cannot be changed. Therefore, exercise caution when selecting a region.
DB Instance Name	Must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.

Parameter	Description
DB Engine	Set to <b>MySQL</b> .
DB Engine Version	<p>For details, see <a href="#">DB Engines and Versions</a>.</p> <p>Different DB engine versions are supported in different regions.</p> <p>You are advised to select the latest available version because it is more stable, reliable, and secure.</p>
DB Instance Type	<ul style="list-style-type: none"> <li>- <b>Primary/Standby</b>: uses an HA architecture with a primary DB instance and a synchronous standby DB instance. It is suitable for production databases of large- and medium-sized enterprises in Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other sectors. The standby DB instance improves instance reliability and is invisible to you after being created. An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. You can deploy primary and standby DB instances in a single AZ or across AZs to achieve failover and high availability.</li> <li>- <b>Single</b>: uses a single-node architecture, which is more cost-effective than primary/standby DB instances. It is suitable for development and testing of microsites, and small and medium enterprises, or for learning about RDS.</li> </ul>
Time Zone	You need to select a time zone for your instance based on the region hosting your instance. You can select a time zone during instance creation and change it after the instance is created.

- DB instance specifications

**Table 2-3** Instance specifications

Parameter	Description
Instance Class	<p>Refers to the CPU and memory of a DB instance. Different instance classes have different numbers of database connections and different maximum IOPS.</p> <p>For details about instance classes, see section <a href="#">DB Instance Classes</a>.</p> <p>After a DB instance is created, you can change its instance class. For details, see section <a href="#">Changing a DB Instance Class</a>.</p>

Parameter	Description
Storage Type	<p>Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be.</p> <ul style="list-style-type: none"> <li>- <b>Common I/O:</b> uses the SATA disk type, with a maximum throughput of 90 MB/s.</li> <li>- <b>Ultra-high I/O:</b> uses the SSD disk type that supports a maximum throughput of 350 MB/s.</li> </ul>
Storage Space (GB)	<p>Contains the file system overhead required for inode, reserved block, and database operation.</p> <p>After a DB instance is created, you can scale up its storage space. For details, see section <a href="#">Scaling up Storage Space</a>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- Storage space can range in size from 40 GB to 4,000 GB and can be scaled up only by a multiple of 10 GB.</li> </ul>

- Network and database configuration

**Table 2-4** Network

Parameter	Description
VPC	<p>A dedicated virtual network in which your RDS DB instances are located. A VPC can isolate networks for different workloads. You can select an existing VPC or create a VPC. For details on how to create a VPC, see the "Creating a VPC" section in the <i>Virtual Private Cloud User Guide</i>.</p> <p>If no VPC is available, RDS allocates a VPC to you by default.</p> <p><b>NOTICE</b></p> <p>After the DB instance is created, the VPC cannot be changed.</p>
Subnet	<p>Improves network security by providing dedicated network resources that are logically isolated from other networks. Subnets take effect only within an AZ. The Dynamic Host Configuration Protocol (DHCP) function is enabled by default for subnets in which you plan to create RDS DB instances and cannot be disabled.</p> <p>A floating IP address is automatically assigned when you create a DB instance. You can also enter an unused floating IP address in the subnet CIDR block. After the DB instance is created, you can change the floating IP address.</p>

Parameter	Description
Security Group	Enhances security by controlling access to RDS from other services. You need to add inbound rules to a security group so that you can connect to your DB instance.  If no security group is available or has been created, RDS allocates a security group to you by default.

**Table 2-5** Database configuration

Parameter	Description
Administrator	The default login name for the database is <b>root</b> .
Administrator Password	Must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@#\$\$%^*_+=+?,). Enter a strong password and periodically change it for security reasons.  Keep this password secure. The system cannot retrieve it.  After a DB instance is created, you can reset this password. For details, see section <a href="#">Resetting the Administrator Password</a> .
Confirm Password	Must be the same as <b>Administrator Password</b> .
Parameter Template	Contains engine configuration values that can be applied to one or more DB instances. If you intend to create primary/standby DB instances, they use the same parameter template.  <b>NOTICE</b> If you use a custom parameter template when creating a DB instance, the following specification-related parameters in the custom template are not delivered. Instead, the default values are used.  <ul style="list-style-type: none"> <li>- <b>back_log</b></li> <li>- <b>innodb_io_capacity_max</b></li> <li>- <b>max_connections</b></li> <li>- <b>innodb_io_capacity</b></li> <li>- <b>innodb_buffer_pool_size</b></li> <li>- <b>innodb_buffer_pool_instances</b></li> </ul> You can modify the instance parameters as required after the DB instance is created. For details, see section <a href="#">Modifying Parameters</a> .

- Batch creation

**Table 2-6** Batch creation

Parameter	Description
Quantity	<p>RDS supports DB instance creation in batches. If you choose to create primary/standby DB instances and set <b>Quantity</b> to <b>1</b>, a primary DB instance and a standby DB instance will be created synchronously.</p> <p>If you create multiple DB instances at a time, they will be named with four digits appended to the DB instance name. For example, if you enter <b>instance</b>, the first instance will be named instance-0001, the second instance-0002, and so on.</p>

 **NOTE**

The performance of your DB instance depends on its configurations. Hardware configuration items include the instance specifications, storage type, and storage space.

**Step 6** Confirm the specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

**Step 7** To view and manage your DB instance, go to the **Instance Management** page.

- When your DB instance is being created, the status is **Creating**. The status changes to **Available** after the instance is created. To view the detailed progress and result of the creation, go to the **Task Center** page.
- The automated backup policy is enabled by default. You can change it after the DB instance is created. An automated full backup is immediately triggered once your DB instance is created.
- The default database port is **3306**. You can change it after a DB instance is created.

For details, see section [Changing a Database Port](#).

----End

## 2.3 Step 2: Connect to a DB Instance

### 2.3.1 Connecting to a DB Instance

An RDS DB instance can be connected through a private network or a public network.

**Table 2-7** RDS connection methods

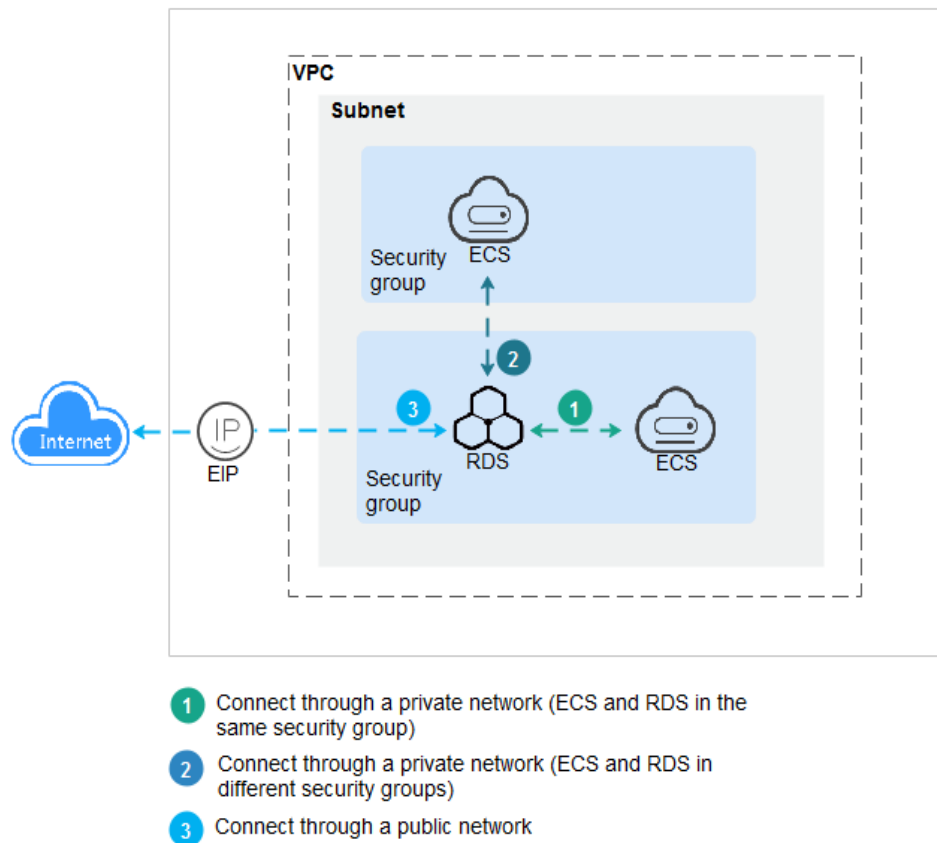
Connect Through	IP Address	Scenarios	Description
<b>Private network</b>	Floating IP	<p>RDS provides a floating IP address by default.</p> <p>When your applications are deployed on an ECS that is in the same region and VPC as RDS, you are advised to use a floating IP address to connect to the RDS DB instance through the ECS.</p>	<ul style="list-style-type: none"> <li>• Secure and excellent performance</li> <li>• Recommended</li> </ul>
<b>Public network</b>	EIP	<p>If you cannot access an RDS DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance to the ECS through the EIP.</p>	<ul style="list-style-type: none"> <li>• A relatively lower level of security compared to other connection methods</li> <li>• To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance.</li> </ul>

 **NOTE**

- VPC: indicates the Virtual Private Cloud.
- ECS: indicates the Elastic Cloud Server.
- If the ECS is in the same VPC as your RDS DB instance, you do not need to apply for an EIP.

**Figure 2-2** illustrates the connection over a private network or a public network.

**Figure 2-2** DB instance connection



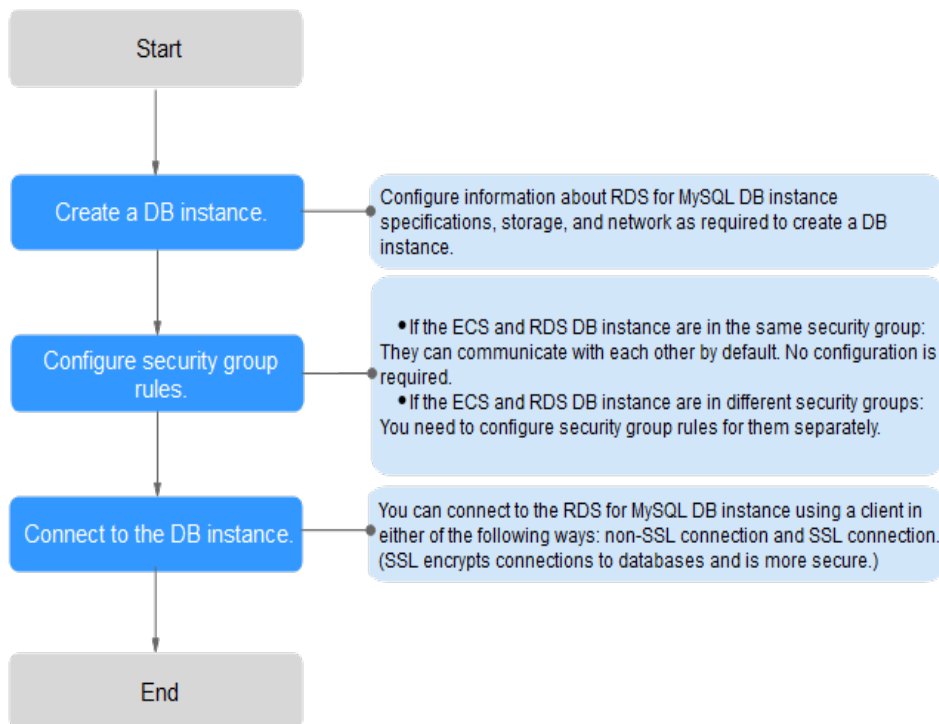
## 2.3.2 Connecting to an RDS for MySQL DB Instance Through a Private Network

### 2.3.2.1 Connecting to a DB Instance Through a Private Network

#### Process

**Figure 2-3** illustrates the process of connecting to an RDS for MySQL DB instance through a private network.

**Figure 2-3** Connecting to a DB instance through a private network



- **Step 1: Create a DB instance.** Confirm the specifications, storage, network, and database account configurations of the RDS for MySQL DB instances based on service requirements.
- **Step 2: Configure security group rules.**
  - If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to [Connecting to a DB Instance Through a Private Network](#).
  - If the ECS and RDS DB instance are in different security groups, you need to configure security group rules for them, separately.
    - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
    - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.
- **Step 3: Connect to a DB instance through a private network.** You can connect to a DB instance through a non-SSL connection or an SSL connection. The SSL connection encrypts data and is more secure.



## 2.3.2.2 Configuring Security Group Rules

### Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted in a VPC.

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS instance.

First check whether the ECS and RDS DB instance are in the same security group.

- If they are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to [Connecting to a DB Instance Through a Private Network](#).
- If they are in different security groups, configure security group rules for them, separately.
  - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
  - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

### Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated only with one security group, but a security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

#### NOTE

If you use **0.0.0.0/0**, RDS DB instances in the security group can be accessed from any IP address.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Under **Network**, click **Virtual Private Cloud**.

**Step 3** In the navigation pane on the left, choose **Access Control > Security Groups**.

**Step 4** On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column.

**Step 5** On the displayed page, click **Add Rule**.

**Step 6** In the displayed dialog box, set required parameters to add an inbound rule.

**Step 7** Click **OK**.

----End

### 2.3.2.3 Connecting to a DB Instance Through a Private Network

You can connect to a DB instance through a non-SSL connection or an SSL connection. The SSL connection encrypts data and is more secure.

#### Prerequisites

1. You have logged in to an ECS.
  - To connect to a DB instance through an ECS, you must ensure that:
    - The ECS and DB instance must be in the same VPC.
    - The ECS must be allowed by the security group to access the DB instance.
      - If the security group with which the target DB instance is associated is the default security group, you do not need to configure security group rules.
      - If the security group with which the target DB instance is associated is not the default security group, check whether the security group rules allow the ECS to connect to the DB instance. For details, see section [Configuring Security Group Rules](#).  
If the security group rules allow the access from the ECS, the ECS can connect to the DB instance.  
If the security group rules do not allow the access from the ECS, you need to add a security group rule. The ECS must be allowed by the security group to access the DB instance.
2. You have installed a database client to connect to DB instances.

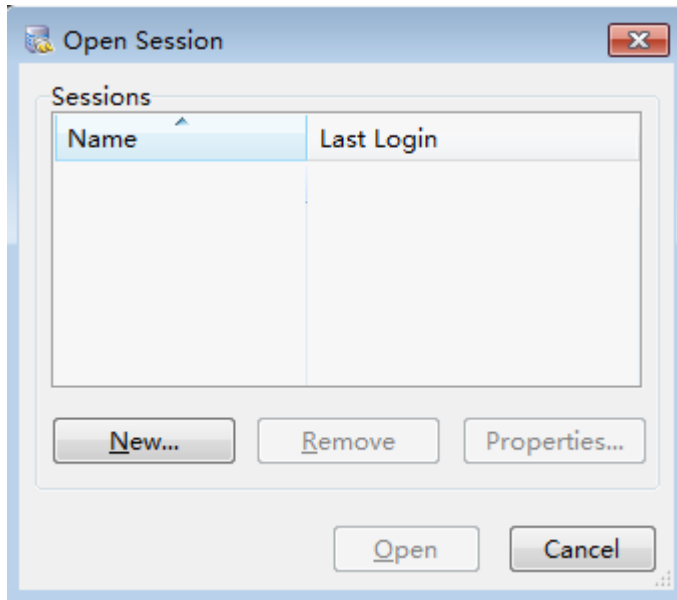
You can use a database client to connect to the target DB instance in the Linux or Windows OS.

  - In the Linux OS, install the MySQL client on the device that can access RDS. It is recommended that you download a MySQL client running a version later than that of the DB instance.  
For details about how to obtain and install the MySQL client, see section [How Can I Install the MySQL Client?](#)
  - In the Windows OS, you can use any common database client to connect to the target DB instance in a similar way.  
The database client MySQL-Front is used as an example in [Using MySQL-Front to Connect to a DB Instance](#).

## Using MySQL-Front to Connect to a DB Instance

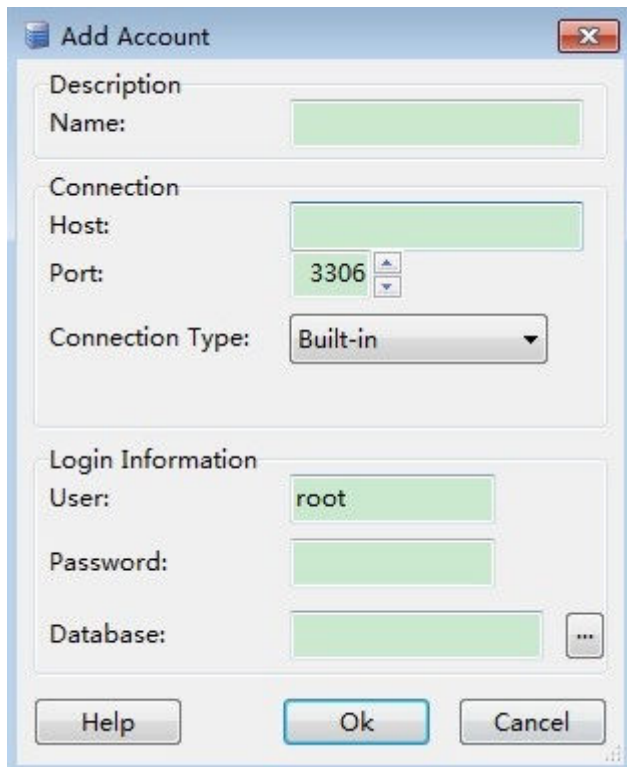
- Step 1** Start MySQL-Front.
- Step 2** In the displayed dialog box, click **New**.

Figure 2-4 Connection management



- Step 3** Enter the information of the DB instance to be connected and click **Ok**, as shown in [Figure 2-5](#).

Figure 2-5 Adding an account

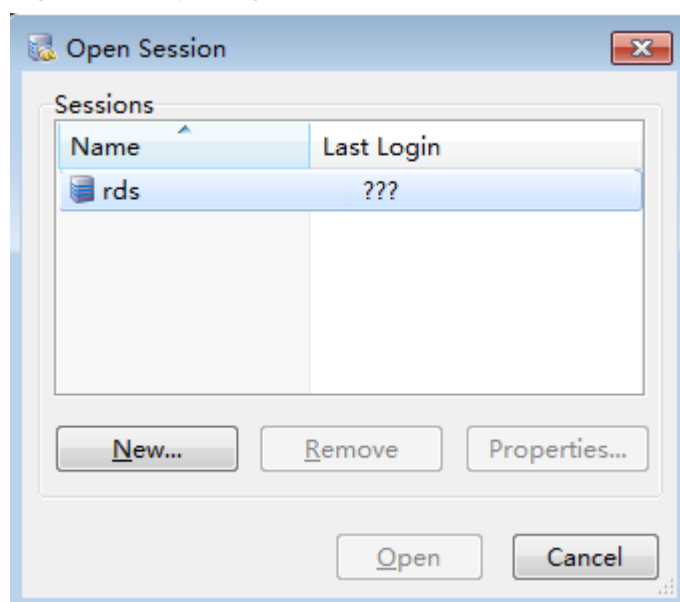


**Table 2-8** Parameter description

Parameter	Description
Name	Name of the database connection task. If you do not set this parameter, it will be the same as the <b>Host</b> value by default.
Host	Floating IP address of the DB instance to be connected. To view the floating IP address and port of the DB instance, perform the following steps: <ol style="list-style-type: none"> <li>1. Log in to the RDS console.</li> <li>2. Select the region in which the DB instance is located.</li> <li>3. Click the target DB instance to enter the <b>Basic Information</b> page.</li> <li>4. In the <b>Connection Information</b> area, view the floating IP address and database port.</li> </ol>
Port	Database port of the DB instance.
User	Name of the user who will access the DB instance. The default user is <b>root</b> .
Password	Password of the RDS database account.

**Step 4** In the displayed window, select the connection that you have created in [Step 3](#) and click **Open**. If the connection information is correct, the DB instance is successfully connected.

**Figure 2-6** Opening a session



 NOTE

If the connection fails, see [What Should I Do If an ECS Cannot Connect to an RDS DB Instance Through a Private Network?](#)

----End

## SSL Connection


**Step 1** Log in to the management console.


**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the instance name to go to the **Basic Information** page.

**Step 5** In the **DB Information** area, check whether SSL is enabled.

- If yes, go to [Step 6](#).
- If no, click . In the displayed dialog box, click **Yes**. Then go to [Step 6](#).

**Step 6** Click  next to **SSL** to download the root certificate or certificate bundle.

**Step 7** Import the root certificate to the Windows or Linux OS on the ECS. For details, see [How Can I Import the Root Certificate to a Windows or Linux OS?](#)

 NOTE

- Since April 2017, RDS has offered a new root certificate that has a 20-year validation period. The new certificate takes effect after DB instances are rebooted. Replace the old certificate before it expires to improve system security.

For details, see section [How Can I Identify the Validity Period of an SSL Root Certificate?](#)

- You can also download the certificate bundle, which contains both the new certificate provided since April 2017 and the old certificate.

**Step 8** Connect to the RDS DB instance. The Linux OS is used as an example.

- Method 1  
`mysql -h <host> -P <port> -u <userName> -p --ssl-ca=<caName>`
- Method 2  
`mysql -h <host> -P <port> -u <userName> -p --ssl-capath=<caPath>`

**Table 2-9** Parameter description

Parameter	Description
<host>	Floating IP address. To obtain this parameter, go to the <b>Basic Information</b> page of the DB instance and view the floating IP address in the <b>Connection Information</b> area.

Parameter	Description
<code>&lt;port&gt;</code>	Database port. By default, the value is <b>3306</b> . To obtain this parameter, go to the <b>Basic Information</b> page of the DB instance and view the database port in the <b>Connection Information</b> area.
<code>&lt;userName&gt;</code>	Username of the RDS database account. The default administrator is <b>root</b> .
<code>&lt;caName&gt;</code>	Name of the CA certificate. The certificate should be stored in the directory where the command is executed.
<code>&lt;caPath&gt;</code>	Path of the CA certificate.

For example, to connect to a DB instance through an SSL connection as user **root**, run the following command:

```
mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=ca.pem
```

Enter the password of the database account if the following information is displayed:

Enter password:

 **NOTE**

If the connection fails, see [What Should I Do If an ECS Cannot Connect to an RDS DB Instance Through a Private Network?](#)

----End

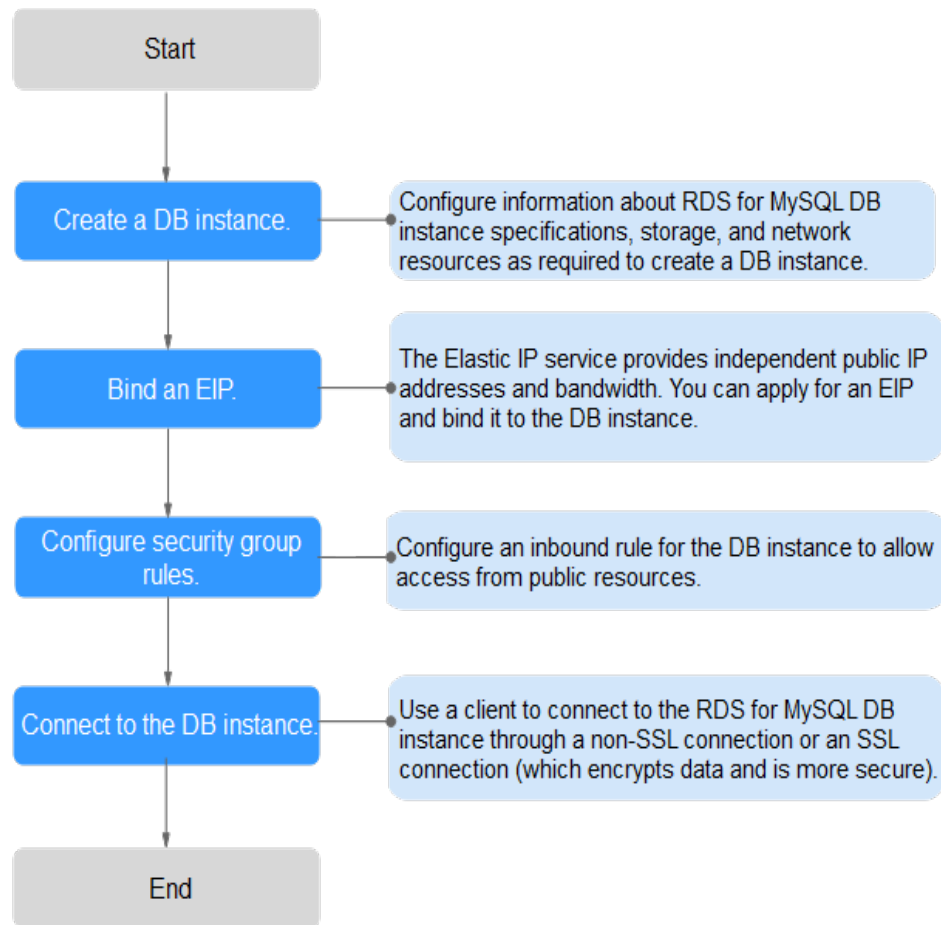
## 2.3.3 Connecting to an RDS for MySQL DB Instance Through a Public Network

### 2.3.3.1 Connecting to a DB Instance Through a Public Network

#### Process

**Figure 2-7** illustrates the process of connecting to an RDS for MySQL DB instance through a public network.

**Figure 2-7** Connecting to a DB instance through a public network



- **Step 1: Create a DB instance.** Confirm the specifications, storage, network, and database account configurations of the RDS for MySQL DB instances based on service requirements.
- **Step 2: Bind an EIP.** The EIP provides independent public IP addresses and bandwidth for Internet access. You can apply for an EIP on the VPC console and bind the EIP to the RDS DB instance.
- **Step 3: Configure security group rules.** To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.
- **Step 4: Connect to a DB instance through a public network.** You can connect to a DB instance through a non-SSL connection or an SSL connection. The SSL connection encrypts data and is more secure.

### 2.3.3.2 Binding an EIP

#### Scenarios

By default, a DB instance is not publicly accessible (not bound with an EIP) after being created. You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

## Precautions

- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, you need to add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see section [Configuring Security Group Rules](#).
- Public accessibility reduces the security of DB instances. Therefore, exercise caution when enabling this function. To achieve a higher transmission rate and security level, you are advised to migrate your applications to the ECS that is in the same region as RDS.

## Binding an EIP

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **EIPs**. On the displayed page, click **Bind EIP**.

**Step 6** In the displayed dialog box, select an EIP and click **OK**.

**Step 7** On the **EIPs** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

----End

### 2.3.3.3 Configuring Security Group Rules

#### Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted in a VPC.

This section describes how to create a security group to enable specific IP addresses and ports to access RDS.

When you attempt to connect to an RDS DB instance through an EIP, you need to configure an **inbound rule** for the security group associated with the DB instance.

#### Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.



- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated only with one security group, but a security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

 **NOTE**

If you use **0.0.0.0/0**, RDS DB instances in the security group can be accessed from any IP address.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Under **Network**, click **Virtual Private Cloud**.
- Step 3** In the navigation pane on the left, choose **Access Control > Security Groups**.
- Step 4** On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- Step 5** On the displayed page, click **Add Rule**.
- Step 6** In the displayed dialog box, set required parameters to add an inbound rule.
- Step 7** Click **OK**.

----End

### 2.3.3.4 Connecting to a DB Instance Through a Public Network

You can connect to a DB instance through a non-SSL connection or an SSL connection. The SSL connection encrypts data and is more secure.

## Prerequisites

1. An EIP has been bound to the target DB instance and security group rules have been configured.
  - a. Bind an EIP to the target DB instance.  
For details about how to bind an EIP, see section [Binding an EIP](#).
  - b. Obtain the IP address of the local device.
  - c. Configure security group rules.  
Add the IP address obtained in **1.b** and the instance port to the inbound rule of the security group.  
For details about how to configure a security group rule, see section [Configuring Security Group Rules](#).

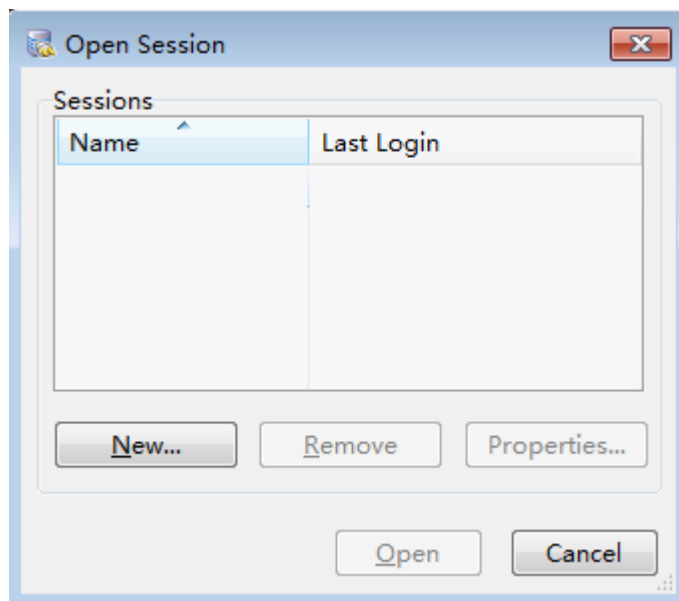
- d. Run the **ping** command to check the connectivity between the local device and the EIP that has been bound to the DB instance in **1.a**.
2. You have installed a database client to connect to DB instances.  
You can use a database client to connect to the target DB instance in the Linux or Windows operating system (OS).
  - In the Linux OS, you need to install a MySQL client on the ECS. It is recommended that you download a MySQL client running a version later than that of the DB instance.  
For details about how to obtain and install the MySQL client, see section [How Can I Install the MySQL Client?](#)
  - In the Windows OS, you can use any common database client to connect to the target DB instance in a similar way.  
The database client MySQL-Front is used as an example in [Using MySQL-Front to Connect to a DB Instance](#).

## Using MySQL-Front to Connect to a DB Instance

**Step 1** Start MySQL-Front.

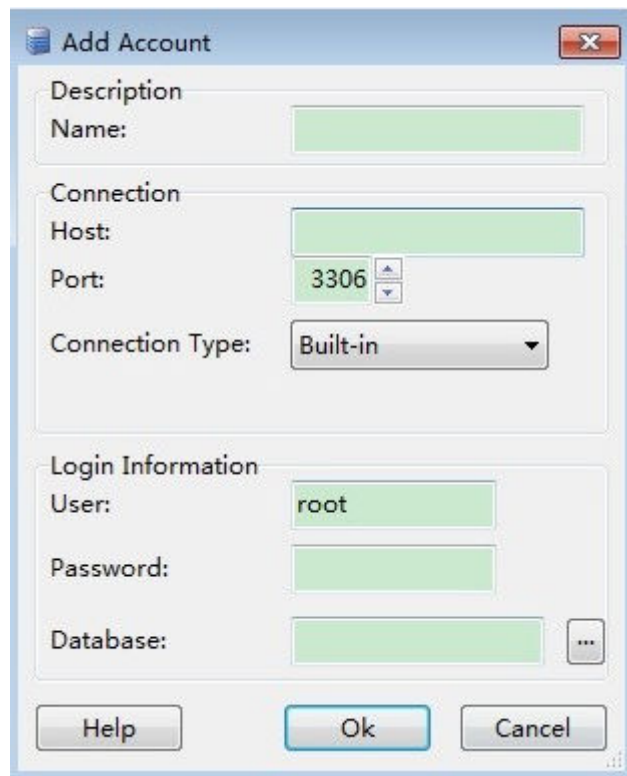
**Step 2** In the displayed dialog box, click **New**.

**Figure 2-8** Connection management



**Step 3** Enter the information of the DB instance to be connected and click **Ok**, as shown in [Figure 2-9](#).

**Figure 2-9** Adding an account



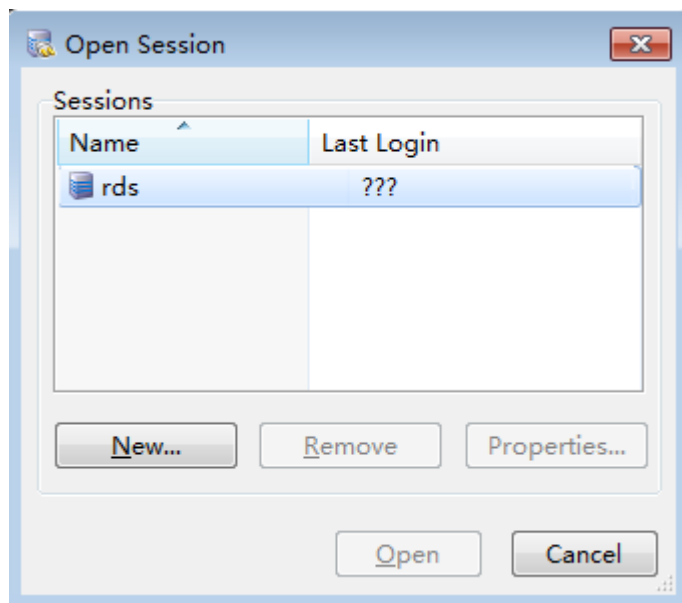
**Table 2-10** Parameter description

Parameter	Description
Name	Name of the database connection task. If you do not set this parameter, it will be the same as the <b>Host</b> value by default.
Host	EIP of the DB instance to be connected. For details about how to bind an EIP, see <a href="#">Binding an EIP</a> .
Port	Database port of the DB instance.
User	Name of the user who will access the DB instance. The default user is <b>root</b> .
Password	Password of the RDS database account.

**Step 4** In the displayed window, select the connection that you have created in [Figure 2-10](#) and click **Open**.

If the connection information is correct, the DB instance is successfully connected.

**Figure 2-10** Opening a session






**NOTE**

If the connection fails, ensure that preparations have been correctly made in [Prerequisites](#) and try again.

----End

## Using SSL to Connect to a DB Instance

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the instance name to go to the **Basic Information** page.
- Step 5** In the **DB Information** area, check whether SSL is enabled.
  - If yes, go to [Step 6](#).
  - If no, click . In the displayed dialog box, click **Yes**. Then go to [Step 6](#).
- Step 6** Click  next to **SSL** to download the root certificate or certificate bundle.
- Step 7** Import the root certificate to the Windows or Linux OS on the ECS. For details, see [How Can I Import the Root Certificate to a Windows or Linux OS?](#)

 **NOTE**

- Since April 2017, RDS has offered a new root certificate that has a 20-year validation period. The new certificate takes effect after DB instances are rebooted. Replace the old certificate before it expires to improve system security.

For details, see section [How Can I Identify the Validity Period of an SSL Root Certificate?](#)

- You can also download the certificate bundle, which contains both the new certificate provided since April 2017 and the old certificate.

**Step 8** Connect to an RDS DB instance. The Linux OS is used as an example.

- Method 1

```
mysql -h <host> -P <port> -u <userName> -p --ssl-ca=<caName>
```

- Method 2

```
mysql -h <host> -P <port> -u <userName> -p --ssl-capath=<caPath>
```

**Table 2-11** Parameter description

Parameter	Description
<host>	EIP of the DB instance to be connected.
<port>	Port of the DB instance to be connected.
<userName>	Username of the RDS database account. The default administrator is <b>root</b> .
<caName>	Name of the CA certificate. The certificate should be stored in the directory where the command is executed.
<caPath>	Path of the CA certificate.

For example, to connect to a DB instance through an SSL connection as user **root**, run the following command:

```
mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=ca.pem
```

Enter the password of the database account if the following information is displayed:

Enter password:

 **NOTE**

If the connection fails, ensure that preparations have been correctly made in [Prerequisites](#) and try again.

----End

# 3 Getting Started with RDS for PostgreSQL

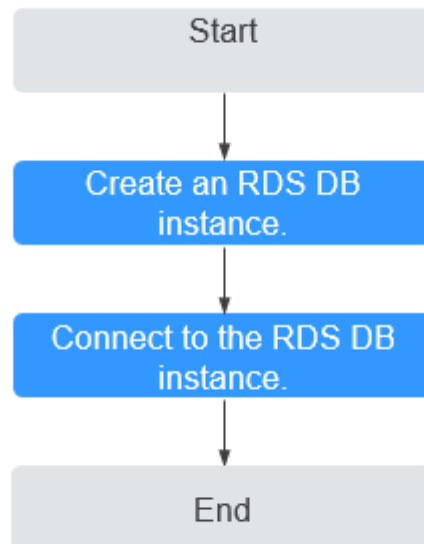
---

## 3.1 Operation Guide

You can create and connect to DB instances on the RDS console.

### Flowchart

Figure 3-1 Flowchart



## Procedure

**Table 3-1** Related operations and references

Operation	Reference
Creating an RDS DB instance	<a href="#">Step 1: Create a DB Instance</a>
Connecting to an RDS DB Instance	<a href="#">Step 2: Connect to a DB Instance</a>


## 3.2 Step 1: Create a DB Instance

### Scenarios

This section describes how to create a DB instance on the RDS console.

RDS allows you to tailor your computing resources and storage space to your business needs.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click **Create DB Instance**.
- Step 5** On the displayed page, configure information about your DB instance. Then, click **Create Now**.

**Table 3-2** Basic information

Parameter	Description
Region	Region where the tenant is located. <b>NOTE</b> Products in different regions cannot communicate with each other through a private network and you cannot change the region of a DB instance after creating the instance. Therefore, exercise caution when selecting a region.
DB Instance Name	Different DB instances can have the same name. The instance name must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.
DB Engine	Set to <b>PostgreSQL</b> .

Parameter	Description
DB Engine Version	<p>For details, see <a href="#">DB Engines and Versions</a>.</p> <p>Different DB engine versions are supported in different regions.</p> <p>You are advised to select the latest available version because it is more stable, reliable, and secure.</p>
DB Instance Type	<ul style="list-style-type: none"> <li> <b>Primary/Standby:</b> uses an HA architecture with a primary DB instance and a synchronous standby DB instance. It is suitable for production databases of large- and medium-sized enterprises in Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other sectors. The standby DB instance improves instance reliability and is invisible to you after being created.                     </li> </ul> <p>An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network.</p> <p>You can deploy primary and standby DB instances in a single AZ or across AZs to achieve failover and high availability.</p> <ul style="list-style-type: none"> <li> <b>Single:</b> uses a single-node architecture, which is more cost-effective than primary/standby DB instances. It is suitable for development and testing of microsites, and small- and medium-sized enterprises, or for learning about RDS.                     </li> </ul>
Time Zone	<p>You need to select a time zone for your instance based on the region hosting your instance. You can select a time zone during instance creation and change it later.</p>

**Table 3-3** Instance specifications

Parameter	Description
Instance Class	<p>Refers to the CPU and memory of a DB instance. Different instance classes have different numbers of database connections and different maximum IOPS.</p> <p>For details about instance classes, see <a href="#">DB Instance Classes</a>.</p> <p>After a DB instance is created, you can change its CPU and memory. For details, see <a href="#">Changing a DB Instance Class</a>.</p>



Parameter	Description
Storage Type	<p>Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be.</p> <ul style="list-style-type: none"> <li>• <b>Common I/O:</b> uses the SATA disk type, with a maximum throughput of 90 MB/s.</li> <li>• <b>Ultra-high I/O:</b> uses the SSD disk type that supports a maximum throughput of 350 MB/s.</li> </ul>
Storage Space (GB)	<p>Contains the file system overhead required for inode, reserved block, and database operation. Storage space can range in size from 40 GB to 4,000 GB and can be scaled up only by a multiple of 10 GB.</p> <p>After a DB instance is created, you can scale up its storage space. For details, see <a href="#">Scaling up Storage Space</a>.</p>

**Table 3-4** Network

Parameter	Description
VPC	<p>A dedicated virtual network in which your RDS DB instances are located. A VPC can isolate networks for different services. You can select an existing VPC or create a VPC. For details on how to create a VPC, see the "Creating a VPC" section in the <i>Virtual Private Cloud User Guide</i>.</p> <p>If no VPC is available, RDS allocates a VPC to you by default.</p> <p><b>NOTICE</b> After the DB instance is created, the VPC cannot be changed.</p>
Subnet	<p>Improves network security by providing dedicated network resources that are logically isolated from other networks. Subnets take effect only within an AZ. The Dynamic Host Configuration Protocol (DHCP) function is enabled by default for subnets in which you plan to create RDS DB instances and cannot be disabled.</p> <p>A floating IP address is automatically assigned when you create a DB instance. You can also enter an unused floating IP address in the subnet CIDR block. After the DB instance is created, you can change the floating IP address.</p>
Security Group	<p>Controls the access that traffic has in and out of a DB instance. By default, the security group associated with the DB instance is authorized.</p> <p>Enhances security by controlling access to RDS from other services. You need to add inbound rules to a security group so that you can connect to your DB instance.</p> <p>If no security group is available, RDS allocates a security group to you by default.</p>

**Table 3-5** Database configuration

Parameter	Description
Administrator	The default login name for the database is <b>root</b> .
Administrator Password	<p>Must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@#%^*_-=+?,). Enter a strong password and periodically change it for security reasons. Keep this password secure. The system cannot retrieve it.</p> <p>After a DB instance is created, you can reset this password. For details, see section <a href="#">Resetting the Administrator Password</a>.</p>
Confirm Password	Must be the same as <b>Administrator Password</b> .
Parameter Template	<p>Contains engine configuration values that can be applied to one or more DB instances. If you intend to create primary/standby DB instances, they use the same parameter template.</p> <p><b>NOTICE</b> If you use a custom parameter template when creating a DB instance, the following specification-related parameters in the custom template are not delivered. Instead, the default values are used.</p> <ul style="list-style-type: none"> <li>• <b>maintenance_work_mem</b></li> <li>• <b>shared_buffers</b></li> <li>• <b>max_connections</b></li> <li>• <b>effective_cache_size</b></li> </ul> <p>You can modify the instance parameters as required after the DB instance is created. For details, see <a href="#">Modifying Instance Parameters</a>.</p>

**Table 3-6** Batch creation

Parameter	Description
Quantity	<p>RDS supports DB instance creation in batches. If you choose to create primary/standby DB instances and set <b>Quantity</b> to <b>1</b>, a primary DB instance and a standby DB instance will be created synchronously.</p> <p>If you create multiple DB instances at a time, they will be named with four digits appended to the DB instance name. For example, if you enter <b>instance</b>, the first instance will be named instance-0001, the second instance-0002, and so on.</p>

 **NOTE**

The performance of your DB instance depends on its configurations. Hardware configuration items include the instance specifications, storage type, and storage space.

**Step 6** Confirm the specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

**Step 7** To view and manage the DB instance, go to the **Instance Management** page.

- During the creation process, the DB instance status is **Creating**. When the creation process is complete, the instance status will change to **Available**.
- The automated backup policy is enabled by default. After the DB instance is created, you can modify the policy as needed. An automated full backup is immediately triggered after a DB instance is created.
- The default database port is **5432**. After a DB instance is created, you can change the database port.

For details, see [Changing a Database Port](#).

----End

## 3.3 Step 2: Connect to a DB Instance

### 3.3.1 Connecting to a DB Instance

An RDS DB instance can be connected through a private network or a public network.

**Table 3-7** RDS connection methods

Connect Through	IP Address	Scenarios	Description
<a href="#">Private network</a>	Floating IP	RDS provides a floating IP address by default. When your applications are deployed on an ECS that is in the same region and VPC as RDS, you are advised to use a floating IP address to connect to the RDS DB instance through the ECS.	<ul style="list-style-type: none"> <li>• Secure and excellent performance</li> <li>• Recommended</li> </ul>

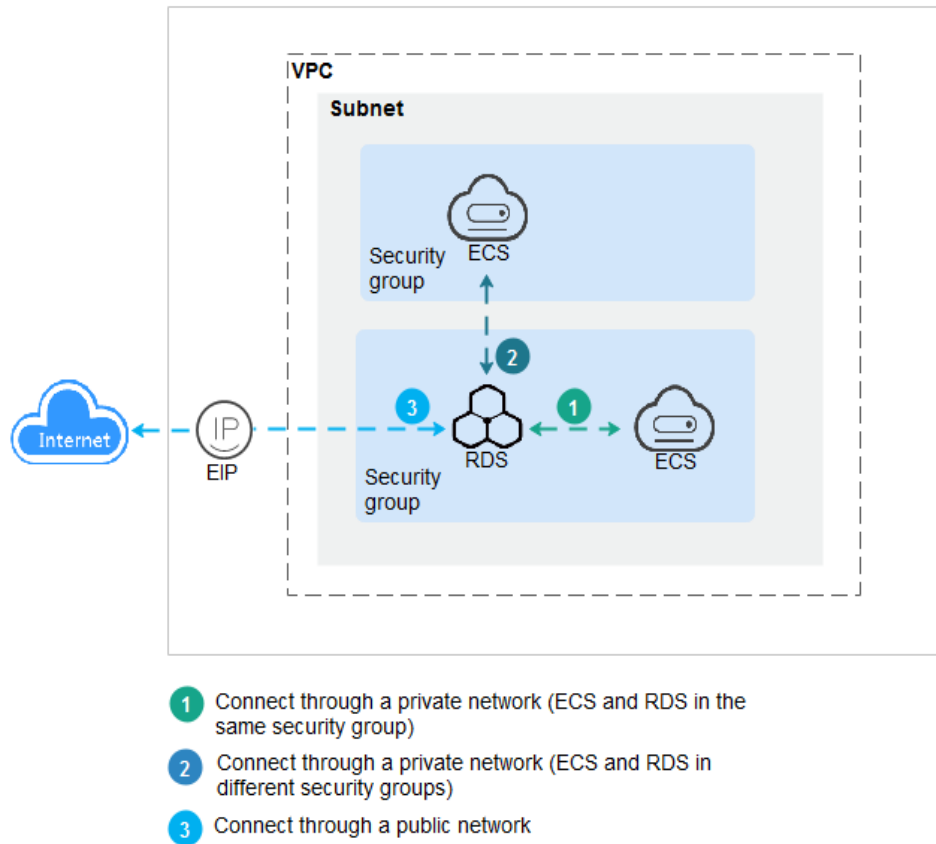
Connect Through	IP Address	Scenarios	Description
Public network	EIP	If you cannot access an RDS DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance to the ECS through the EIP.	<ul style="list-style-type: none"> <li>• A relatively lower level of security compared to other connection methods</li> <li>• To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance.</li> </ul>

 **NOTE**

- VPC: indicates the Virtual Private Cloud.
- ECS: indicates the Elastic Cloud Server.
- If the ECS is in the same VPC as your RDS DB instance, you do not need to apply for an EIP.

**Figure 3-2** illustrates the connection over a private network or a public network.

Figure 3-2 DB instance connection



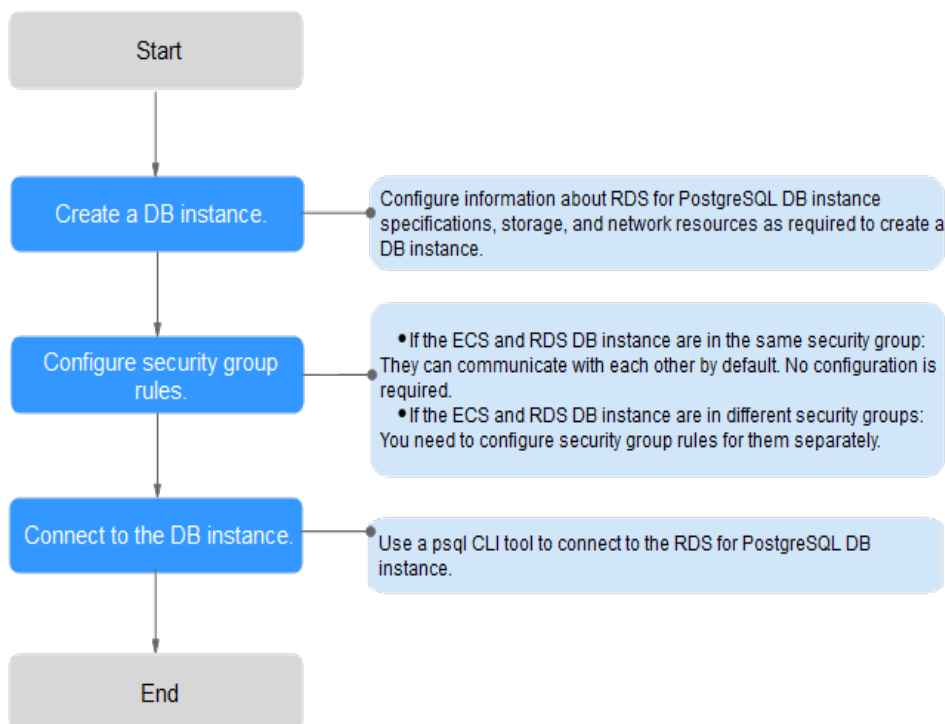
## 3.3.2 Connecting to a DB Instance Through a Private Network

### 3.3.2.1 Connecting to a DB Instance Through a Private Network

#### Process

Figure 3-3 illustrates the process of connecting to an RDS for PostgreSQL DB instance through a private network.

**Figure 3-3** Connecting to a DB instance through a private network



- **Step 1: Create a DB instance.** Confirm the specifications, storage, network, and database account configurations of the RDS for PostgreSQL DB instances based on service requirements.
- **Step 2: Configure security group rules.**
  - If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to [Connecting to a DB Instance Through psql](#).
  - If the ECS and RDS DB instance are in different security groups, you need to configure security group rules for them, separately.
    - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
    - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.
- **Step 3: Connect to a DB instance through a private network.** The CLI tool psql is used as an example to describe the connection method.

### 3.3.2.2 Configuring Security Group Rules

#### Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted in a VPC.

This section describes how to create a security group to enable specific IP addresses and ports to access RDS.

First check whether the ECS and RDS DB instance are in the same security group.

- If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to [Connecting to a DB Instance Through psql](#).
- If the ECS and RDS DB instance are in different security groups, you need to configure security group rules for them, separately.
  - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
  - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

## Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are deployed in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS DB instance can be associated only with one security group.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for each security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

### NOTE

If you use **0.0.0.0/0**, RDS DB instances in the security group can be accessed from any IP address.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Under **Network**, click **Virtual Private Cloud**.
- Step 3** In the navigation pane on the left, choose **Access Control > Security Groups**.
- Step 4** On the displayed page, locate the target security group and click **Manage Rule** in the **Operation** column.
- Step 5** On the displayed page, click **Add Rule**.
- Step 6** In the displayed dialog box, set required parameters to add an inbound rule.

**Step 7** Click **OK**.

----End

### 3.3.2.3 Connecting to a DB Instance Through psql

You can use a PostgreSQL client to connect to an instance through an SSL connection. The SSL connection is encrypted and therefore more secure.

SSL is enabled by default when you create an RDS for PostgreSQL DB instance and cannot be disabled after the instance is created.

#### Prerequisites

1. You have logged in to the ECS.
  - To connect to a DB instance through an ECS, make sure that:
    - The ECS and DB instance must be in the same VPC.
    - The ECS must be allowed by the security group to access RDS DB instances.
      - If the security group with which the target DB instance is associated is the default security group, you do not need to configure security group rules.
      - If the security group with which the target DB instance is associated is not the default security group, check whether the security group rules allow the ECS to connect to the DB instance. For details, see [Configuring Security Group Rules](#).


If the security group rules allow the access from the ECS, the ECS can connect to the DB instance.

If the security group rules do not allow the access from the ECS, you need to add a security group rule. The ECS must be allowed by the security group to access DB instances.
2. You have installed a database client to connect to DB instances.

For details, see [How Can I Install a PostgreSQL Client?](#)


#### SSL Connection

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the instance name to go to the **Basic Information** page.

**Step 5** Click  next to SSL to download the root certificate or certificate bundle.

**Step 6** Upload the root certificate to the ECS or save it to the device to be connected to the DB instance.



For details about how to import the root certificate to the Linux OS on the ECS, see [How Can I Import the Root Certificate to a Windows or Linux OS?](#)

**Step 7** Connect to an RDS DB instance. The Linux OS is used as an example.

```
psql --no-readline -h <host> -p <port> "dbname=<database> user=<user>
sslmode=verify-ca sslrootcert=<ca-file-directory>"
```

**Table 3-8** Parameter description

Parameter	Description
<host>	IP address of the primary DB instance. To obtain this parameter value, go to the <b>Basic Information</b> page of the DB instance and view the floating IP address in the <b>Connection Information</b> area (if the DB instance is to be accessed through an ECS).
<port>	Database port in use. The default value is <b>5432</b> . To obtain this parameter value, go to the <b>Basic Information</b> page of the DB instance. The port number can be found in the <b>Database Port</b> field in the <b>Connection Information</b> area.
<database>	Name of the database (the default database name is <b>postgres</b> ).
<user>	Username of the RDS database account. The default administrator is <b>root</b> .
<ca-file-directory>	Directory of the CA certificate for the SSL connection. The certificate should be stored in the directory where the command is executed.
sslmode	SSL connection mode. Set it to <b>verify-ca</b> to use a CA to check whether the service is trusted.

Enter the password of the database account if the following information is displayed:

Password:

For example, to connect to a DB instance through an SSL connection as user **root**, run the following command:

```
psql --no-readline -h 192.168.0.44 -p 5432 "dbname=postgres user=root
sslmode=verify-ca sslrootcert=/root/ca.pem"
```

Password:

**Step 8** The SSL connection is established if information similar to the following is displayed after you log in to the database:

```
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
```

----End

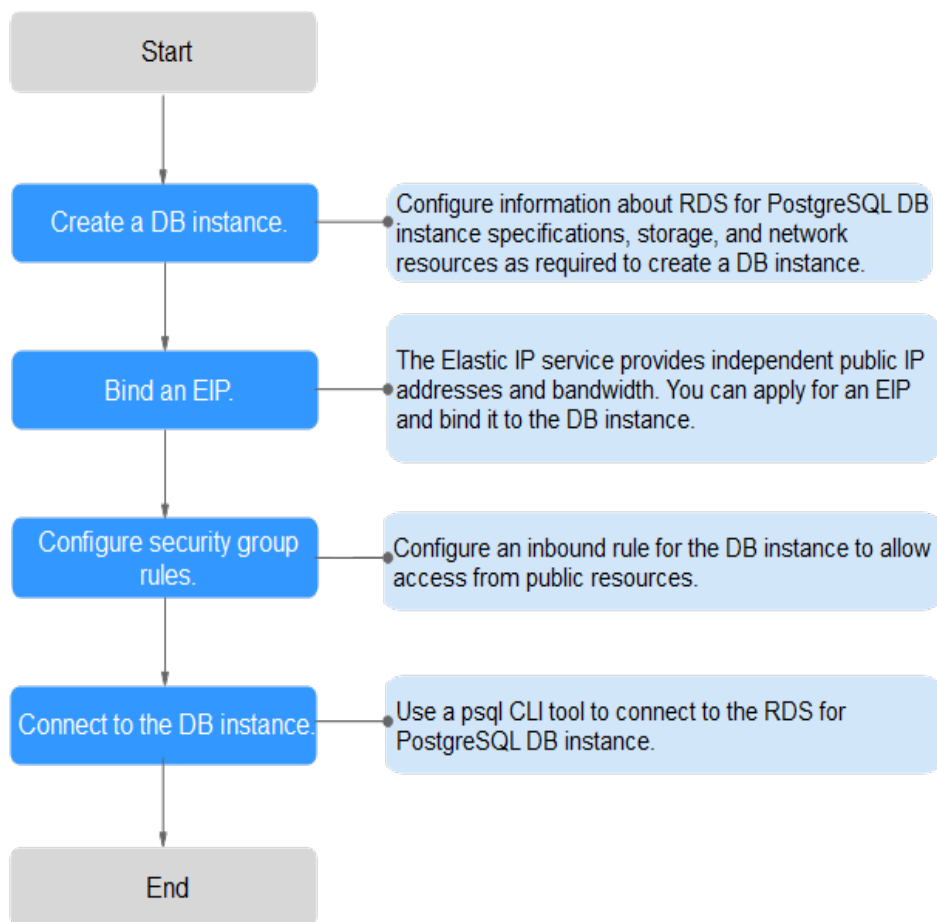
## 3.3.3 Connecting to a DB Instance Through a Public Network

### 3.3.3.1 Connecting to a DB Instance Through a Public Network

#### Process

**Figure 3-4** illustrates the process of connecting to an RDS for PostgreSQL DB instance through a public network.

**Figure 3-4** Connecting to a DB instance through a public network



- **Step 1: Create a DB instance.** Confirm the specifications, storage, network, and database account configurations of the RDS for PostgreSQL DB instances based on service requirements.
- **Step 2: Bind an EIP.** The EIP provides independent public IP addresses and bandwidth for Internet access. You can apply for an EIP on the VPC console and bind the EIP to the RDS DB instance.
- **Step 3: Configure security group rules.** To enable access to a DB instance from resources outside the security group, you need to configure an inbound rule for the security group associated with the DB instance.
- **Step 4: Connect to a DB instance through psql.** The CLI tool psql is used as an example to describe the connection method.

### 3.3.3.2 Binding an EIP

#### Scenarios

By default, a DB instance is not publicly accessible (not bound with an EIP) after being created. You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

#### Precautions

- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, you need to add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see section [Configuring Security Group Rules](#).
- Public accessibility reduces the security of DB instances. Therefore, exercise caution when deciding to connect to DB instances through a public network. To achieve a higher transmission rate and security level, you are advised to migrate your applications to the ECS that is in the same region as RDS.

#### Binding an EIP

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **EIPs**. On the displayed page, click **Bind EIP**.

**Step 6** In the displayed dialog box, select an EIP and click **OK**.

If no available EIPs are displayed, click **View EIP** to obtain an EIP.

**Step 7** On the **EIPs** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

----End

### 3.3.3.3 Configuring Security Group Rules

#### Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted in a VPC.

This section describes how to create a security group to enable specific IP addresses and ports to access RDS.

When you attempt to connect to an RDS DB instance through an EIP, you need to configure an **inbound rule** for the security group associated with the DB instance.

## Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are deployed in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS DB instance can be associated only with one security group.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for each security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

### NOTE

If you use **0.0.0.0/0**, RDS DB instances in the security group can be accessed from any IP address.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Under **Network**, click **Virtual Private Cloud**.
- Step 3** In the navigation pane on the left, choose **Access Control > Security Groups**.
- Step 4** On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- Step 5** On the displayed page, click **Add Rule**.
- Step 6** In the displayed dialog box, set required parameters to add an inbound rule.
- Step 7** Click **OK**.

----End

### 3.3.3.4 Connecting to a DB Instance Through psql

You can use a PostgreSQL client to connect to an instance through an SSL connection. The SSL connection is encrypted and therefore more secure.

SSL is enabled by default when you create an RDS for PostgreSQL DB instance and cannot be disabled after the instance is created.

## Prerequisites

1. An EIP has been bound to the target DB instance and security group rules have been configured.

- a. Bind an EIP to the target DB instance.  
For details about how to bind an EIP, see [Binding an EIP](#).
  - b. Obtain the IP address of a local device.
  - c. Configure security group rules.  
Add the IP address obtained in [1.b](#) and the instance port to the inbound rule of the security group.  
For details about how to configure security group rules, see [Configuring Security Group Rules](#).
  - d. Run the **ping** command to ping the EIP bound in [1.a](#).
2. You have installed a database client to connect to DB instances.  
For details, see [How Can I Install a PostgreSQL Client?](#)


## SSL Connection

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the instance name to go to the **Basic Information** page.

**Step 5** Click  next to **SSL** to download the root certificate or certificate bundle.

**Step 6** Upload the root certificate to the ECS or save it to the device to be connected to the DB instance.

For details about how to import the root certificate to the Linux OS on the ECS, see [How Can I Import the Root Certificate to a Windows or Linux OS?](#)

**Step 7** Connect to an RDS DB instance. The Linux OS is used as an example.

```
psql --no-readline -h <host> -p <port> "dbname=<database> user=<user>
sslmode=verify-ca sslrootcert=<ca-file-directory>"
```

**Table 3-9** Parameter description

Parameter	Description
<host>	EIP of the DB instance to be connected.
<port>	Database port in use. The default value is <b>5432</b> . To obtain this parameter, go to the <b>Basic Information</b> page of the DB instance. The port number can be found in the <b>Database Port</b> field in the <b>Connection Information</b> area.
<database>	Name of the database (the default database name is <b>postgres</b> ).
<user>	Username of the RDS database account. The default administrator is <b>root</b> .

Parameter	Description
<i>&lt;ca-file-directory&gt;</i>	Directory of the CA certificate for the SSL connection. The certificate should be stored in the directory where the command is executed.
sslmode	SSL connection mode. Set it to <b>verify-ca</b> to use a CA to check whether the service is trusted.

Enter the password of the database account if the following information is displayed:

Password:

For example, to connect to a DB instance through an SSL connection as user **root**, run the following command:

```
psql --no-readline -h 192.168.0.44 -p 5432 "dbname=postgres user=root sslmode=verify-ca sslrootcert=/root/ca.pem"
```

**Password:**

**Step 8** The SSL connection is established if information similar to the following is displayed after you log in to the database:

```
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
```

**----End**

# 4 Working with RDS for MySQL

---

## 4.1 Database Migration

### 4.1.1 Migrating Data to RDS for MySQL Using mysqldump

#### Preparing for Data Migration

You can access RDS DB instances through an EIP or through an ECS.

1. Prepare an ECS for accessing DB instances in the same VPC or prepare a device for accessing RDS through an EIP.
  - To connect to a DB instance through an ECS, you need to create an ECS first.  
For details about how to create and connect to an ECS, see [How Can I Create and Connect to an ECS?](#)
  - To connect to a DB instance through an EIP, you must:
    - i. Bind an EIP to a DB instance. For details, see [Binding an EIP](#).
    - ii. Ensure that the local device can access the EIP.
2. Install the MySQL client on the prepared ECS or device.

For details, see [How Can I Install the MySQL Client?](#)

#### NOTE

The MySQL client version must be the same as the version of RDS for MySQL. The MySQL database or client will provide mysqldump and mysql.

After data is migrated to RDS, you may need to change the IP address. For details, see [Configuring and Changing a Floating IP Address](#).

#### Exporting Data

Before migrating data to RDS, you need to export data first.

### NOTICE

- The export tool must match the DB engine version.
- Database migration is performed offline. Before the migration, you must stop any applications using the source database.

**Step 1** Log in to the ECS or the device that can access RDS.

**Step 2** Use the mysqldump tool to export metadata into an SQL file.

### NOTICE

The MySQL database is required for RDS management. When exporting metadata, do not specify **--all-database**. Otherwise, the MySQL database will be unavailable.

```
mysqldump --databases <DB_NAME> --single-transaction --order-by-primary
--hex-blob --no-data --routines --events --set-gtid-purged=OFF -u <DB_USER>
-p -h <DB_ADDRESS> -P <DB_PORT> |sed -e 's/DEFINER[ ]*=[ ]*[^\]*\*/' -e 's/
DEFINER[ ]*.*FUNCTION/FUNCTION/' -e 's/DEFINER[ ]*.*PROCEDURE/
PROCEDURE/' -e 's/DEFINER[ ]*.*TRIGGER/TRIGGER/' -e 's/
DEFINER[ ]*.*EVENT/EVENT/' > <BACKUP_FILE>
```

- *DB\_NAME* indicates the name of the database to be migrated.
- *DB\_USER* indicates the database username.
- *DB\_ADDRESS* indicates the database address.
- *DB\_PORT* indicates the database port.
- *BACKUP\_FILE* indicates the name of the file to which the data will be exported.

Enter the database password when prompted.

Example:

```
mysqldump --databases rdsdb --single-transaction --order-by-primary --hex-
blob --no-data --routines --events --set-gtid-purged=OFF -u root -p -h
192.168.151.18 -P 3306 |sed -e 's/DEFINER[ ]*=[ ]*[^\]*\*/' -e 's/
DEFINER[ ]*.*FUNCTION/FUNCTION/' -e 's/DEFINER[ ]*.*PROCEDURE/
PROCEDURE/' -e 's/DEFINER[ ]*.*TRIGGER/TRIGGER/' -e 's/
DEFINER[ ]*.*EVENT/EVENT/' > dump-defs.sql
```

Enter password:

### NOTE

If you use mysqldump with a version earlier than 5.6, remove **--set-gtid-purged=OFF** before running this command.

After this command is executed, a **dump-defs.sql** file will be generated as follows:

```
[rds@localhost ~]$ ll dump-defs.sql
-rw-r-----. 1 rds rds 2714 Sep 21 08:23 dump-defs.sql
```

**Step 3** Use the mysqldump tool to export data into an SQL file.



**NOTICE**

The MySQL database is required for RDS management. When exporting metadata, do not specify **--all-database**. Otherwise, the MySQL database will be unavailable.

```
mysqldump --databases <DB_NAME> --single-transaction --hex-blob --set-gtid-purged=OFF --no-create-info --skip-triggers -u <DB_USER> -p -h <DB_ADDRESS> -P <DB_PORT> -r <BACKUP_FILE>
```

For details on the parameters in the preceding command, see [Step 2](#).

Enter the database password when prompted.

Example:

```
mysqldump --databases rdsdb --single-transaction --hex-blob --set-gtid-purged=OFF --no-create-info --skip-triggers -u root -p -h 192.168.151.18 -P 8635 -r dump-data.sql
```

 **NOTE**

If you use `mysqldump` with a version earlier than 5.6, remove **--set-gtid-purged=OFF** before running this command.

After this command is executed, a **dump-data.sql** file will be generated as follows:

```
[rds@localhost ~]$ ll dump-data.sql  
-rw-r-----. 1 rds rds 2714 Sep 21 08:23 dump-data.sql
```

----End

## Importing Data

You can connect your client to RDS and import exported SQL files into RDS.

**NOTICE**

If the source database calls triggers, stored procedures, functions, or events, you must set **log\_bin\_trust\_function\_creators** to **ON** on the destination database before importing data.

**Step 1** Log in to the ECS or the device that can access RDS.

**Step 2** Import metadata into RDS.

```
# mysql -f -h <RDS_ADDRESS> -P <DB_PORT> -u root -p < <BACKUP_DIR>/  
dump-defs.sql
```

- *RDS\_ADDRESS*: indicates the IP address of the RDS DB instance.
- *DB\_PORT* indicates the RDS DB instance port.
- *BACKUP\_DIR* indicates the directory where **dump-defs.sql** is stored.

Example:

```
# mysql -f -h 172.16.66.198 -P 3306 -u root -p < dump-defs.sql
```

**Enter password:**

 **NOTE**

If you intend to import SQL statements of a table to RDS, you are advised to specify a database. Otherwise, the error message "No database selected" may be displayed. For example, if you intend to import SQL statements of a table to database **mydb**, run the following command:

```
# mysql -f -h 172.16.66.198 -P 3306 -u root -p mydb < dump-defs.sql
```

**Enter password:**

**Step 3** Import data into RDS.

```
# mysql -f -h <RDS_ADDRESS> -P <DB_PORT> -u root -p < <BACKUP_DIR>/dump-data.sql
```

- *RDS\_ADDRESS*: indicates the IP address of the RDS DB instance.
- *DB\_PORT* indicates the RDS DB instance port.
- *BACKUP\_DIR* indicates the directory where **dump-data.sql** is stored.

Example:

```
# mysql -f -h 172.16.66.198 -P 3306 -u root -p < dump-data.sql
```

**Enter password:**

 **NOTE**

If you intend to import SQL statements of a table to RDS, you are advised to specify a database. Otherwise, the error message "No database selected" may be displayed. For example, if you intend to import SQL statements of a table to database **mydb**, run the following command:

```
# mysql -f -h 172.16.66.198 -P 3306 -u root -p mydb < dump-defs.sql
```

**Enter password:**

**Step 4** View the import result.

```
mysql> show databases;
```

The following result indicates that database **rdsdb** has been imported.

```
mysql> show databases;
+-----+
| Database          |
+-----+
| information_schema |
| rdsdb              |
| mysql              |
| performance_schema |
+-----+
4 rows in set (0.00 sec)
```

----End

## 4.1.2 Migrating Data to RDS for MySQL Using the Export and Import Functions of DAS

### Scenarios

Data Admin Service (DAS) is a one-stop management platform that allows you to manage databases on a web console. It offers database development, O&M,

intelligent diagnosis, and enterprise-level DevOps, making it easy to use and maintain databases.

To back up or migrate data, you can use DAS to export data from the source database first and then import the data to from your local PC or OBS bucket to the destination database.

## Constraints

- Only one file that is no larger than 1 GB can be imported at a time.
- Only data files in the CSV or SQL format can be imported.
- Binary fields such as BINARY, VARBINARY, TINYBLOB, BLOB, MEDIUMBLOB, and LONGBLOB are not supported.
- Data cannot be exported or imported using cross-region OBS buckets.

## Exporting Data

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Databases**, click **Relational Database Service**.

**Step 4** On the **Instances** page, locate the DB instance and click **Log In** in the **Operation** column.

**Step 5** On the displayed login page, enter the username and password and click **Log In**.

**Step 6** On the top menu bar, choose **Import and Export > Export**.

**Step 7** On the displayed page, click **Create Task** and choose **Export Database** or **Export SQL Result** as required. The following takes database export as an example.

Alternatively, click **Quick Export** and select the target database. On the displayed page, select a storage path and click **OK**.

**Step 8** On the displayed page, set parameters as required in areas **Basic Information** and **Advanced Settings**. Then, select the tables to be exported on the right.

### NOTE

- In a SQL result export task, the executed SQL statements cannot exceed 5 MB.
- Databases are classified into user databases and system databases. System databases cannot be exported. If system database data is required, deploy system database services in a created user database, so that you can export the system database data from the user database.
- DAS connects to your standby database to export data. This prevents the primary database from being affected by data export. However, if the standby database has a high replication delay, the exported data may not be the latest.

**Step 9** After settings are complete, click **OK**.

**Step 10** In the task list, view the task ID, type, status, and progress.

**Step 11** Click **Details** in the **Operation** column to view task details.

----End

## Importing Data

**Step 1** On the top menu bar, choose **Import and Export > Import**.

**Step 2** Import a file from your local PC or an OBS bucket.

- From your local PC

In the upper left corner, click **Create Task**. On the displayed page, select an import type, select **Upload file** for **File Source**, set the attachment storage, and upload the file. Then, set other parameters as required.

For security purposes, imported files are stored in OBS buckets.

### NOTE

- To keep your data secure, provide your own OBS bucket to store the attachments you upload. In this way, DAS automatically connects to your OBS bucket for in-memory reading.
- If you select **Delete the uploaded file upon an import success**, the file you uploaded will be automatically deleted from the OBS bucket after being imported to the destination database.

- From an OBS bucket

In the upper left corner, click **Create Task**. On the displayed page, select an import type, select **Choose from OBS** for **File Source**, and select a file from the bucket. Then, set other parameters as required.

### NOTE

The file uploaded from an OBS bucket will not be deleted upon an import success.

**Step 3** After setting the import parameters, click **Create**. Confirm the information again before you click **OK** because original data may be overwritten after data import.

**Step 4** View the import progress in the task list or check task details.

----End

## 4.2 Parameter Tuning

### 4.2.1 Suggestions on RDS for MySQL Parameter Tuning

Parameters are key configuration items in a database system. Improper parameter settings may adversely affect the stable running of databases. This section describes some important parameters for your reference. For details, visit the [MySQL official website](#).

For details on how to modify RDS for MySQL parameters on the console, see [Modifying Parameters](#).

#### Sensitive Parameters

The following parameters can result in system security and stability issues if set improperly:

- **lower\_case\_table\_names**

Default value: 1

Function: Controls whether database and tables stored on disks are case sensitive. The value **1** indicates that database and table names are case-insensitive and are lowercase by default.

 **NOTE**

RDS for MySQL 8.0 does not support this parameter.

Impact: Changing this parameter value may cause primary/standby replication exceptions. Exercise caution when performing this operation.

- If you want to change this parameter value from **1** to **0**, change it on read replicas and reboot them first, and then repeat the operations on the primary DB instance.
- If you want to change this parameter value from **0** to **1**, change it on the primary DB instance and reboot it first, and then run **SELECT @@GLOBAL.GTID\_EXECUTED** on read replicas. Wait until the result set is at least the same as the primary DB instance and then change this parameter value on read replicas and reboot them.

- **innodb\_flush\_log\_at\_trx\_commit**

Default value: **1**

Function: Controls the balance between strict ACID compliance for commit operations and higher performance. The default setting of **1** is required for full ACID compliance. Logs are written and flushed to disks at each transaction commit. If the value is set to **0**, logs are written and flushed to disks once per second. If the value is set to **2**, logs are written at each transaction commit and flushed to disks every two seconds.

Impact: If this parameter is not set to **1**, data security is not guaranteed. If the system fails, data may be lost.

- **sync\_binlog**

Default value: **1**

Function: Controls how often the MySQL server synchronizes binary logs to the disk. The default setting of **1** requires synchronization of the binary log to the disk at each transaction commit. If the value is set to **0**, synchronization of the binary log to the disk is not controlled by the MySQL server but relies on the OS to flush the binary log to the disk. This setting provides the best performance, but in the event of a power failure or OS crash, all binary log information in **binlog\_cache** is lost.

Impact: If this parameter is not set to **1**, data security is not guaranteed. If the system fails, data may be lost.

- **innodb\_large\_prefix**

Default value: **OFF**

Function: Specifies the maximum length of a single-column index in an InnoDB table.

 **NOTE**

This parameter is available only for RDS for MySQL 5.6.

Impact: Changing this parameter value during DDL execution may cause primary/standby replication exceptions. Exercise caution when performing this operation.

- If you want to change this parameter value from **OFF** to **ON**, change it on read replicas first and then on the primary DB instance.
- If you want to change this parameter value from **ON** to **OFF**, change it on the primary DB instance first and then on read replicas.

## Performance Parameters

The following parameters can affect database performance:

- The values of **innodb\_spin\_wait\_delay** and **query\_alloc\_block\_size** are determined by the DB instance specifications. If you increase their values, database performance may be affected.
- If **max\_connections** is set to a small value, database access will be affected.
- The default values of the following parameters are determined by the DB instance specifications: **innodb\_buffer\_pool\_size**, **max\_connections**, and **back\_log**. These parameter values are **default** before being specified.
- The values of **innodb\_io\_capacity\_max** and **innodb\_io\_capacity** are determined by the storage type. These parameter values are **default** before being specified.

## Constraints on Parameter Modification

- When the **innodb\_adaptive\_hash\_index** and **innodb\_buffer\_pool\_size** parameters are modified at the same time, the value of **innodb\_adaptive\_hash\_index** will fail to be changed from **OFF** to **ON**.
- The value of **innodb\_buffer\_pool\_size** must be an integer multiple of the product of **innodb\_buffer\_pool\_instances** and **innodb\_buffer\_pool\_chunk\_size**.
- If **innodb\_buffer\_pool\_instances** is set to **2**, the value of **innodb\_buffer\_pool\_size** must be greater than or equal to 1 (unit: GB).
- For MySQL 8.0, if the kernel version is earlier than 8.0.18, the value of **max\_prepared\_stmt\_count** cannot exceed 1048576.

## 4.3 Permissions Management

### 4.3.1 Creating a User and Granting Permissions

This chapter describes how to use Identity and Access Management (IAM) to implement fine-grained permissions control for your RDS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing RDS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or cloud service to perform efficient O&M on your RDS resources.

If your account does not require individual IAM users, skip this chapter.

This section describes the procedure for granting permissions (see [Figure 4-1](#)).

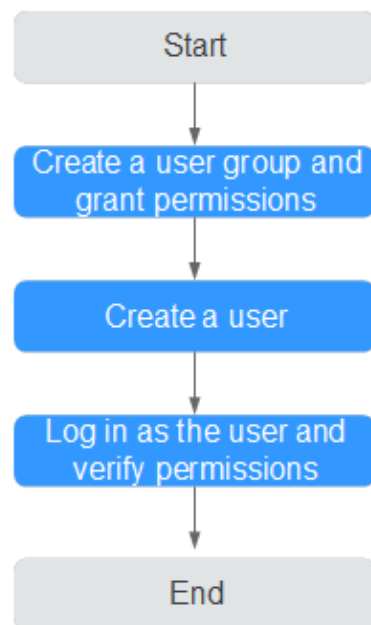
## Prerequisites

Learn about the permissions (see ) supported by RDS and choose policies or roles according to your requirements. For the system policies of other services, see .

For more information about system policies supported by RDS, see [Permissions Management](#).

## Process Flow

**Figure 4-1** Process for granting RDS permissions



1. Create a user group and assign permissions to it.  
Create a user group on the IAM console, and attach the **RDS ReadOnlyAccess** policy to the group.
2. Create an IAM user and add it to the user group  
Create a user on the IAM console and add the user to the group created in **1**.
3. Log in and verify permissions.  
Log in to the RDS console by using the created user, and verify that the user only has read permissions for RDS.
  - Choose **Service List > Relational Database Service** and click **Buy DB Instance**. If a message appears indicating that you have insufficient permissions to perform the operation, the **RDS ReadOnlyAccess** policy has already taken effect.
  - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **RDS ReadOnlyAccess** policy has already taken effect.

## 4.3.2 RDS Custom Policies

Custom policies can be created as a supplement to the system policies of RDS. For the actions supported for custom policies, see "Permissions Policies and Supported Actions" in *Relational Database Service API Reference*.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see "Creating a Custom Policy" in *Identity and Access Management User Guide*. The following section contains examples of common RDS custom policies.

### Example Custom Policies

- Example 1: Allowing users to create RDS DB instances

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["rds:instance:create"]
  }]
}
```

- Example 2: Denying RDS DB instance deletion

A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the **RDS FullAccess** policy to a user but you want to prevent the user from deleting RDS DB instances. Create a custom policy for denying RDS DB instance deletion, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on RDS DB instances except deleting RDS DB instances. The following is an example deny policy:

```
{
  "Version": "1.1",
  "Statement": [{
    "Action": ["rds:instance:delete"],
    "Effect": "Deny"
  }]
}
```

## 4.4 Instance Lifecycle

### 4.4.1 Creating a Same DB Instance as an Existing DB Instance

#### Scenarios

This section describes how to quickly create a DB instance with the same configurations as the selected one.




 **NOTE**

- You can create DB instances with the same configurations numerous times.
- This function is unavailable for read replicas.

## Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Create Same DB Instance** in the **Operation** column.

**Step 5** On the displayed page, the configurations are the same as those of the selected DB instance. You can change them as required. Then, click **Apply Now**.

For details about RDS for MySQL DB instance configurations, see section [Step 1: Create a DB Instance](#).

**Step 6** Confirm the instance specifications.

**Step 7** Refresh the DB instance list and view the status of the DB instance. If the status is **Available**, it has been created successfully.

You can manage the DB instance on the **Instance Management** page.

----End

## 4.4.2 Rebooting DB Instances or Read Replicas

### Scenarios



You may need to reboot a DB instance during maintenance. For example, after you modify some parameters, a reboot is required for the modifications to take effect. You can reboot a primary DB instance or a read replica on the management console.

### Constraints

- If the DB instance status is **Abnormal**, the reboot may fail.
- Rebooting DB instances will cause service interruptions. During the reboot process, the DB instance status is **Rebooting**.
- Rebooting DB instances will cause instance unavailability and clear cached memory. To prevent traffic congestion during peak hours, you are advised to reboot DB instances during off-peak hours.

## Procedure

**Step 1** Log in to the management console.

- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance, or click  and then locate the target read replica. Choose **More > Reboot** in the **Operation** column.

Alternatively, click the target DB instance on the **Instance Management** page to go to the **Basic Information** page. In the upper right corner, click **Reboot**.

You can also select the target DB instance on the **Instance Management** page and choose **More > Reboot** above the DB instance list.

For primary/standby DB instances, if you reboot the primary DB instance, the standby DB instance is also rebooted automatically.

- Step 5** In the displayed dialog box, click **Yes**.
- **Immediate:** RDS reboots the instance immediately.
  - **During maintenance window:** RDS will reboot the instance during the maintenance window you configured.
- Step 6** Refresh the DB instance list and view the status of the DB instance. If its status is **Available**, it has rebooted successfully.



----End

## 4.4.3 Selecting Displayed Items

### Scenarios

You can customize which instance items are displayed on the **Instance Management** page.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click  to edit columns displayed in the DB instance list.
- The following items are displayed by default: **Name/ID, Description, DB Instance Type, DB Engine Version, Status, Floating IP Address, and Operation**.  
These default items cannot be deselected.
  - In a single project, you can select up to 10 items: **Name/ID, Description, DB Instance Type, DB Engine Version, Status, Floating IP Address, Created, Database Port, Storage Type, and Operation**.

- For multiple projects, if you have enabled the ProjectMan permissions, you can select up to 10 items: **Name/ID, Description, DB Instance Type, DB Engine Version, Status, Floating IP Address, Created, Database Port, Storage Type, and Operation.**

----End

## 4.4.4 Exporting DB Instance Information

### Scenarios

You can export information about all or selected DB instances to view and analyze DB instance information.

### Constraints


A tenant can export a maximum of 3,000 instances at a time. The time required for the export depends on the number of instances.

### Exporting Information About All DB Instances

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click  in the upper right corner of the page. By default, information about all DB instances are exported. In the displayed dialog box, you can select the items to be exported and click **Export**.

**Step 5** Find a .csv file locally after the export task is completed.


----End

### Exporting Information About Selected DB Instances

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, filter DB instances by DB engine, DB instance name, DB instance ID, or floating IP address, or select the DB instances to be exported, and click  in the upper right corner of the page. In the displayed dialog box, select the items to be exported and click **Export**.

**Step 5** Find a .csv file locally after the export task is completed.

----End

## 4.4.5 Deleting a DB Instance or Read Replica

### Scenarios

To release resources, you can delete DB instances or read replicas as required on the **Instance Management** page.

### Constraints


- DB instances cannot be deleted when operations are being performed on them. They can be deleted only after the operations are complete.
- If you delete a DB instance, its automated backups will also be deleted and you will no longer be billed for them. Manual backups, however, will be retained and generate additional costs.

---


#### NOTICE


- If you delete a primary DB instance, its standby DB instance and read replicas (if any) are also deleted automatically. Exercise caution when performing this operation.
  - Deleted DB instances cannot be recovered and resources are released. Exercise caution when performing this operation. If you want to retain data, **create a manual backup** first before deleting the DB instance.
  - You can use a manual backup to restore a DB instance. For details, see **Restoring from Backup Files to DB Instances**.
- 

### Deleting a DB Instance

- Step 1** Log in to the management console.
  - Step 2** Click  in the upper left corner and select a region and a project.
  - Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - Step 4** On the **Instance Management** page, locate the primary DB instance to be deleted and click **More > Delete** in the **Operation** column.
  - Step 5** In the displayed dialog box, click **Yes**.
  - Step 6** Refresh the DB instance list later to confirm that the deletion was successful.
- End

### Deleting a Read Replica

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

- Step 4** On the **Instance Management** page, locate the target DB instance and click . All the read replicas created for the DB instance are displayed.
- Step 5** Locate the read replica to be deleted and click **More > Delete** in the **Operation** column.
- Step 6** In the displayed dialog box, click **Yes**.
- Step 7** Refresh the DB instance list later to check that the deletion is successful.
- End






## 4.5 Instance Modifications

### 4.5.1 Changing a DB Instance Name

#### Scenarios

You can change the name of a primary DB instance or read replica.

#### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and click  next to it to edit the DB instance name. Then, click **OK**.
- Alternatively, click the target DB instance to go to the **Basic Information** page. In the **DB Information** area, click  next to the **DB Instance Name** field to edit the DB instance name.
- The DB instance name must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (\_) are allowed.
- To submit the change, click .
  - To cancel the change, click .
- Step 5** View the results on the **Basic Information** page.
- End


### 4.5.2 Changing the Failover Priority

#### Scenarios

You can configure the failover priority for reliability or for availability, depending on your service requirements.

- **Reliability:** This option is selected by default. Data consistency is preferentially ensured during a primary/standby failover. This is recommended for users whose highest priority is data consistency.
- **Availability:** Database availability is preferentially ensured during a primary/standby failover. This is recommended for users who require their databases to provide uninterrupted online services.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target primary/standby DB instances.
- Step 5** In the **DB Information** area on the displayed **Basic Information** page, click **Change** in the **Failover Priority** field. In the displayed dialog box, select a priority and click **OK**.
- Step 6** View the results on the **Basic Information** page.

----End

## 4.5.3 Changing a DB Instance Class


### Scenarios

You can change the instance class (CPU or memory) of a DB instance as required. If the status of a DB instance changes from **Changing instance class** to **Available**, the change is successful.

### Constraints

- An instance cannot be deleted while its instance class is being changed.
- The following operations cannot be performed on an instance whose instance class is being changed: rebooting the instance, scaling up storage space, modifying parameter groups, creating a manual backup, creating a database account, and creating a database.
- After the instance class is changed, some parameters are automatically changed to the default values defined in the new instance class. The parameters are **threadpool\_size**, **innodb\_buffer\_pool\_size**, **innodb\_io\_capacity**, **innodb\_io\_capacity\_max**, **innodb\_buffer\_pool\_instances**, **back\_log**, and **max\_connections**.
- After you change instance classes, the DB instances will reboot and services will be interrupted. Therefore, you are advised to change instance classes during off-peak hours.
- Changing the instance class takes 5 to 15 minutes. Service downtime only occurs during the primary/standby switchover.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Change Instance Class** in the **Operation** column.
- Alternatively, click the target DB instance to go to the **Basic Information** page. In the **DB Information** area, click **Change** in the **Instance Class** field.
- Step 5** On the displayed page, specify the new instance class and click **Next**.
- Step 6** View the DB instance class change result.

Return to the **Instance Management** page and view the instance status. During the change period, the instance status is **Changing instance class**. You can view the execution progress of **Changing a MySQL DB instance class** on the **Task Center** page. After a few minutes, view the DB instance class on the **Basic Information** page to check that the change is successful.

---

### NOTICE

After you change an RDS for MySQL instance class, the values of the following parameters will be changed accordingly: **back\_log**, **innodb\_buffer\_pool\_size**, **innodb\_log\_buffer\_size**, **innodb\_log\_files\_in\_group**, **max\_connections**, **innodb\_page\_cleaners**, **innodb\_buffer\_pool\_instances**, **threadpool\_size**, and **slave\_parallel\_workers**.

---

----End

## 4.5.4 Scaling up Storage Space

### Scenarios

If the original storage space is insufficient as your services grow, scale up storage space of your DB instance.

If your storage space usage reaches up to 95% for a disk less than 1 TB or the remaining space becomes 50 GB for a disk no less than 1 TB, the DB instance status becomes **Storage full** and data cannot be written to databases. In this case, scale up storage space to make the DB instance preserve at least 15% of its capacity to work properly.

You are advised to set alarm rules for the storage space usage by referring to [Setting Alarm Rules](#).

For details about the causes and solutions of insufficient storage space, see section [What Should I Do If My Data Exceeds the Available Storage of an RDS for MySQL Instance?](#)

RDS allows you to scale up storage space of DB instances but you cannot change the storage type. During the scale-up period, services are not interrupted.

## Constraints

- The maximum allowed storage is 4,000 GB. There is no limit on the number of scale-ups.
- The DB instance is in **Scaling up** state when its storage space is being scaled up and the backup services are not affected.
- For primary/standby DB instances, scaling up the primary DB instance will cause the standby DB instance to also be scaled up accordingly.
- You cannot reboot or delete a DB instance that is being scaled up.
- Storage space can only be scaled up, not down.

## Scaling up a Primary DB Instance

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Scale Storage Space** in the **Operation** column.

You can also perform the following operations to scale up storage space:

- Click the target DB instance to enter the **Basic Information** page. In the **Storage Space** area, click **Scale**.

**Step 5** On the displayed page, specify the new storage space and click **Next**.

The minimum increment for each scaling is 10 GB.

**Step 6** Confirm specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

**Step 7** View the scale-up result.

Scaling up storage space takes 3-5 minutes. During the time period, the status of the DB instance on the **Instance Management** page will be **Scaling up**. Click the DB instance and view the utilization on the displayed **Basic Information** page to verify that the scale-up is successful.

If the DB instance is running the MySQL DB engine, you can view the detailed progress and result of the task on the **Task Center** page. For details, see section [Task Center](#).

----End


## Scaling up a Read Replica

Scaling up the storage space of a read replica does not affect that of the primary DB instance. Therefore, you can separately scale read replicas to meet service




requirements. New storage space of read replicas after scaling up must be greater than or equal to that of the primary DB instance.

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and click  in front of it. Locate a read replica to be scaled and choose **More > Scale Storage Space** in the **Operation** column.

You can also perform the following operations to scale up storage space:

- Click the target DB instance to enter the **Basic Information** page. In the **Storage Space** area, click **Scale**.

**Step 5** On the displayed page, specify the new storage space and click **Next**.

The minimum increment for each scaling is 10 GB.

**Step 6** Confirm specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

**Step 7** View the scale-up result.

Scaling up storage space takes 3-5 minutes. During the time period, the status of the read replica on the **Instance Management** page will be **Scaling up**. Click the read replica and view the utilization on the displayed **Basic Information** page to verify that the scale-up is successful.

If the read replica is running the MySQL DB engine, you can view the detailed progress and result of the task on the **Task Center** page. For details, see section [Task Center](#).

----End

## 4.5.5 Changing the Maintenance Window


### Scenarios

The maintenance window is 02:00–06:00 by default and you can change it as required. To prevent service interruptions, you are advised to set the maintenance window to off-peak hours.

### Precautions

- During the maintenance window, the DB instance will be intermittently disconnected for one or two times. Ensure that your applications support automatic reconnection.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance. In the **DB Information** area on the **Basic Information** page, click **Change** in the **Maintenance Window** field.
- Step 5** In the displayed dialog box, select a maintenance window and click **OK**.

### NOTE

Changing the maintenance window does not affect the execution time of the scheduled tasks in the original maintenance period.


----End


## 4.5.6 Changing a DB Instance Type from Single to Primary/Standby

### Scenarios


- RDS enables you to change single DB instances to primary/standby DB instances to improve instance reliability. This operation does not affect the services running on the primary DB instance.
- Primary/standby DB instances support automatic failover. If the primary DB instance fails, the standby DB instance takes over services quickly. You are advised to deploy primary and standby DB instances in different AZs for high availability and disaster recovery.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate a single DB instance and choose **More > Change Type to Primary/Standby** in the **Operation** column.

Alternatively, click the target DB instance. In the DB instance topology, click  on the left to change the instance type from single to primary/standby.

- Step 5** Select a standby AZ. Other configurations are the same as those of the primary DB instance by default. Confirm the configurations and click **Submit**.
- Step 6** After a single DB instance is changed to primary/standby instance, you can view and manage it on the **Instance Management** page.

- The DB instance is in the **Changing type to primary/standby** status. You can view the progress on the **Task Center** page. For details, see section **Task Center**.
- In the upper right corner of the DB instance list, click  to refresh the list. After the DB instance type is changed to primary/standby, the instance status will change to **Available** and the instance type will change to **Primary/Standby**.

----End

## 4.5.7 Promoting a Read Replica Into a Single DB Instance

### Scenarios


RDS enables you to promote a read replica into a single DB instance. When you promote a read replica, replication is stopped. After the promotion is complete, the read replica is available as a single DB instance. This operation does not affect the performance of the original DB instance.

#### NOTE

- This function is available only for RDS for MySQL 5.7 and RDS for MySQL 8.0.
- This function is unavailable for DB instances with proxy enabled.

### Procedure


**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target read replica and choose **More > Promote to Primary** in the **Operation** column.

**Step 5** View the read replica status on the **Instance Management** page.

- During the promotion, the read replica status is **Promoting to primary**.
- Refresh the DB instance list by clicking  to see if the promotion is complete. After the promotion is complete, the read replica is disassociated from the original DB instance and is available as a single DB instance.
- The billing mode on the new DB instance remains unchanged.

----End

## 4.5.8 Manually Switching Between Primary and Standby DB Instances

### Scenarios

If you choose to create primary/standby DB instances, RDS will create a primary DB instance and a synchronous standby DB instance in the same region. You can access the primary DB instance only. The standby instance serves as a backup. You can manually promote the standby DB instance to the new primary instance for failover support.

### Constraints

- A DB instance is running properly.
- The replication between the primary and standby instances is normal.

### Procedure


**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target primary/standby DB instance.

**Step 5** In the **DB Information** area on the displayed **Basic Information** page, click **Switch** in the **DB Instance Type** field.

Alternatively, click  in the DB instance topology on the **Basic Information** page to perform a primary/standby switchover.

---

#### NOTICE

A primary/standby switchover may cause service interruptions for several seconds or minutes (depending on the replication delay). To prevent traffic congestion, you are advised to perform a switchover during off-peak hours.


---

**Step 6** In the **Switch Primary/Standby Instances** dialog box, click **Yes** to switch between the primary and standby DB instances.

If the replication status is **Available** and the replication delay is greater than 300s, the primary/standby switchover task cannot be delivered.

**Step 7** After the switchover is successful, check the status of the DB instance on the **Instance Management** page.

- During the switchover, the DB instance status is **Switchover in progress**.

- In the upper right corner of the DB instance list, click  to refresh the list. After the switchover is successful, the DB instance status will become **Available**.

----End

## 4.5.9 Migrating a Standby DB Instance

### Scenarios


You can migrate a standby DB instance to another AZ in the same region as the original AZ.

#### NOTE

- Only primary/standby DB instances running MySQL 5.6 or 5.7 support standby DB instance migration to another AZ. Among such instances, those configured with local SSDs cannot be migrated.
- DDL operations and scheduled events will be suspended during migration. To prevent service interruptions, perform the migration during off-peak hours.

### Procedure

**Step 1** Log in to the management console.


**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Migrate Standby DB Instance** in the **Operation** column.

**Step 5** On the displayed page, select a target AZ and click **Submit**.

**Step 6** After the migration is complete, you can view and manage the DB instance on the **Instance Management** page.

- During the migration process, the DB instance status is **Migrating standby DB instance**. You can view the progress on the **Task Center** page. For details, see section [Task Center](#).
- In the upper right corner of the DB instance list, click  to refresh the list. After the migration is complete, the DB instance status will become **Available**.
- In the **DB Information** on the **Basic Information** page, you can view the AZ hosting the standby DB instance.

----End

## 4.6 Read Replicas

## 4.6.1 Introducing Read Replicas

### Introduction

RDS for MySQL supports read replicas.

In read-intensive scenarios, a single DB instance may be unable to handle the read pressure and service performance may be affected. To offload read pressure on the primary DB instance, you can create one or more read replicas in the same region as the primary instance. These read replicas can process a large number of read requests and increase application throughput. You need to separately configure connection addresses for the primary DB instance and each read replica on your applications so that all read requests can be sent to read replicas and write requests to the primary DB instance.

A read replica uses a single-node architecture (without a slave node). Changes to the primary DB instance are also automatically synchronized to all associated read replicas through the native MySQL replication function. The synchronization is not affected by network latency. Read replicas and the primary DB instance must be in the same region but can be in different AZs.

### Functions

- Read replica specifications can be different from primary DB instance specifications. It is recommended that the read replica specifications be greater than or equal to the primary DB instance specifications to prevent long delay and high load.
- Read replicas support system performance monitoring.  
RDS provides up to 20 monitoring metrics, including storage space, IOPS, the number of database connections, CPU usage, and network traffic. You can view these metrics to learn about the load on DB instances.
- Read replicas do not support automated backups or manual backups.
- Read replicas do not support restoration from backups to new, existing, or original read replicas.
- Data cannot be migrated to read replicas.
- Read replicas do not support database creation and deletion.
- Read replicas do not support database account creation.

### Constraints

A maximum of five read replicas can be created for each primary DB instance.

### Creating and Managing a Read Replica

- [Creating a Read Replica](#)
- [Managing a Read Replica](#)


## 4.6.2 Creating a Read Replica


### Scenarios

Read replicas are used to enhance the read capabilities and reduce the load on primary DB instances.

After DB instances are created, you can create read replicas for them.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and click **Create Read Replica** in the **Operation** column.

Alternatively, click the target DB instance. In the DB instance topology, click  under the primary DB instance to create read replicas.

- Step 5** On the displayed page, configure information about the DB instance and click **Next**.

**Table 4-1** Basic information

Parameter	Description
Region	By default, read replicas are in the same region as the primary DB instance.
DB Instance Name	Must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.
DB Engine	Same as the DB engine of the primary DB instance by default and cannot be changed.
DB Engine Version	Same as the DB engine version of the primary DB instance by default and cannot be changed.
AZ	RDS allows you to deploy primary DB instances and read replicas in a single AZ or across AZs to improve reliability.

**Table 4-2** Instance specifications

Parameter	Description
Instance Class	<p>Refers to the CPU and memory of a DB instance. Different instance classes have different numbers of database connections and maximum IOPS.</p> <p>For details about instance classes, see section <a href="#">DB Instance Classes</a>.</p> <p>After a DB instance is created, you can change its instance class (CPU and memory). For details, see section <a href="#">Changing a DB Instance Class</a>.</p>
Storage Type	<p>Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be.</p> <ul style="list-style-type: none"> <li>• <b>Common I/O</b>: uses the SATA disk type that supports a maximum throughput of 90 MB/s.</li> <li>• <b>Ultra-high I/O</b>: uses the SSD disk type that supports a maximum throughput of 350 MB/s.</li> </ul>
Storage Space	<p>Contains the file system overhead required for inode, reserved block, and database operation.</p> <p>By default, storage space of a read replica is the same as that of the primary DB instance.</p>

**Table 4-3** Network

Parameter	Description
VPC	Same as the primary DB instance's VPC.
Subnet	Same as the primary DB instance's subnet. A floating IP address is automatically assigned when you create a read replica. You can also enter an unused floating IP address in the subnet CIDR block. After the read replica is created, you can change the floating IP address.
Security Group	Same as the primary DB instance's security group.

**Step 6** Confirm specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

**Step 7** After a read replica is created, you can view and manage it.

For details about how to manage read replicas, see [Managing a Read Replica](#).



You can view the detailed progress and result of the task on the **Task Center** page.

----End


## Follow-up Operations

### Managing a Read Replica


## 4.6.3 Managing a Read Replica

### Entering the Management Interface Through a Read Replica

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.


**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** In the DB instance list, click  to expand the DB instance details and click the target read replica to go to the **Basic Information** page.

----End

### Entering the Management Interface Through a Primary DB Instance

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.


**Step 4** Click the name of the primary DB instance with which the target read replica is associated to go to the **Basic Information** page.

**Step 5** In the DB instance topology, click the name of the target read replica. You can view and manage it in the displayed pane.


----End

### Deleting a Read Replica

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** In the DB instance list, click  in front of a DB instance, locate the read replica to be deleted, and choose **More > Delete** in the **Operation** column.

----End

## 4.7 Backups and Restorations

### 4.7.1 Working with Backups

RDS supports backups and restorations to ensure data reliability.

#### Automated Backups

Automated backups are created during the backup time window for your DB instances. RDS saves automated backups based on a retention period you specify. If necessary, you can restore a DB instance to any point in time during your backup retention period. For details, see [Configuring an Automated Backup Policy](#).

#### Manual Backups

Manual backups are user-initiated full backups of DB instances. They are retained until you delete them manually and will not be released with instance deletion. For details, see [Creating a Manual Backup](#).

#### Downloading a Backup File

You can download a full or an incremental backup file for local data backup or restoration. For details, see [Downloading a Backup File](#) and [Downloading a Binlog Backup File](#).

### 4.7.2 Configuring an Automated Backup Policy

#### Scenarios

When you create a DB instance, an automated backup policy is enabled by default. For security purposes, the automated backup policy cannot be disabled. After the DB instance is created, you can customize the automated backup policy as required and then RDS backs up data based on the automated backup policy you configure.

RDS backs up data at the DB instance level, rather than the database level. If a database is faulty or data is damaged, you can restore it from backups. Backups are saved as packages in OBS buckets to ensure data confidentiality and durability. Since backing up data affects database read and write performance, the automated backup time window should be set to off-peak hours.

The automated backup policy is enabled by default as follows:

- Retention period: 7 days
- Time window: An hour within 24 hours, such as 01:00-02:00 or 12:00-13:00. The backup time is configured based on UTC time and is adjusted for daylight saving time, which changes at different times depending on the time zone.
- Backup cycle: Each day of the week by default

## Constraints

- The system verifies the connection to the DB instance when starting a full backup task. If either of the following conditions is met, the verification fails and a retry is automatically performed. If the retry fails, the backup will fail.
  - DDL operations are being performed on the DB instance.
  - The backup lock failed to be obtained from the DB instance.

## Modifying an Automated Backup Policy

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** On the **Backups & Restorations** page, click **Modify Backup Policy**.

- **Retention Period** is the number of days that your automated backups are saved for. Increasing the retention period will improve data reliability.
- If you shorten the retention period, the new backup policy takes effect for all backup files. Any backup files that have expired, based on a newly configured retention period, will be deleted.
- The backup retention period is the number of days you want automated full backups and binlog backups of your DB instance to be saved for. It ranges from 1 to 732 days. The backup time window is one hour. You are advised to select an off-peak time window for automated backups. All the days of the week are selected for **Backup Cycle** by default. You can specify which days of the week you want backups to be taken on.

**Step 6** Click **OK**.

----End

## 4.7.3 Setting a Cross-Region Backup Policy


### Scenarios

RDS can store backup files in the storage space that is in a different region from the DB instance for disaster recovery. If a DB instance in a region is faulty, you can use the backup files in another region to restore data to a new DB instance.


After you enable cross-region backup, the backup files are automatically stored in the region you specify. On the **Backup Management** page of the RDS console, you can click **View Backup** in the **Operation** column and manage cross-region backup files.

### Enabling or Modifying a Cross-Region Backup Policy

**Step 1** Log in to the management console.

- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Backups & Restorations**. On the displayed page, click **Set Cross-Region Backup Policy**.
- If you enable **Cross-Region Full Backup**, automated full backup files of the DB instance are stored in OBS in the region you specify.
  - If you enable **Cross-Region Log Backup**, binlog (incremental) backup files of the DB instance are stored in OBS in the region you specify.
  - Cross-region backup files can be retained from 1 to 1,825 days.
  - Only new backup files generated after you set a cross-region backup policy will be stored in OBS in the region you specify.
  - After the cross-region log backup function is enabled, you can restore a DB instance to a specified time point only after the next automated full backup replication is complete. The specified time point must be later than the time when the automated full backup is complete.
  - All cross-region backups of your DB instances are stored in the region you specify.
  - After you enable cross-region backup, the completed backup files in the region where your instance is located will be asynchronously replicated to the region you specify.
- Step 6** Click **OK**.
- Step 7** On the **Cross-Region Backups** tab of the **Backup Management** page, manage cross-region backup files.
- By default, all instances with cross-region backups are displayed.
    - To modify the cross-region backup policy, click **Set Cross-Region Backup** in the **Operation** column.
    - To view generated cross-region backup files, click **View Cross-Region Backup** in the **Operation** column. If a DB instance fails, you can use the cross-region backup files to restore data to a new DB instance.
- End

## Disabling a Cross-Region Backup Policy

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Backup Management** page, click the **Cross-Region Backups** tab.
- Step 5** Locate a target DB instance and click **Set Cross-Region Backup** in the **Operation** column. On the displayed page, disable the cross-region backup policy.

**Step 6** Click **OK**.

----End

## 4.7.4 Creating a Manual Backup

### Scenarios

RDS allows you to create manual backups of a running primary DB instance. You can use these backups to restore data.

#### NOTE

When you delete a DB instance, its automated backups are also deleted but its manual backups are retained.

### Constraints

- The number of tables in a DB instance affects the backup speed. The maximum number of tables is 250,000.
- The system verifies the connection to the DB instance when starting a full backup task. If either of the following conditions is met, the verification fails and a retry is automatically performed. If the retry fails, the backup will fail.
  - DDL operations are being performed on the DB instance.
  - The backup lock failed to be obtained from the DB instance.

### Method 1

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Create Backup** in the **Operation** column.

**Step 5** In the displayed dialog box, enter a backup name and description. Then, click **OK**. If you want to cancel the backup creation task, click **Cancel**.

- The backup name must consist of 4 to 64 characters and start with a letter. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (\_).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=
- The time required for creating a manual backup depends on the amount of data.


**Step 6** After a manual backup has been created, you can view and manage it on the **Backup Management** page.

Alternatively, click the target DB instance. On the **Backups & Restorations** page, you can view and manage the manual backups.

----End

## Method 2

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** On the **Backups & Restorations** page, click **Create Backup**. In the displayed dialog box, enter a backup name and description and click **OK**. If you want to cancel the backup creation task, click **Cancel**.

- The backup name must consist of 4 to 64 characters and start with a letter. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (\_).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=
- The time required for creating a manual backup depends on the amount of data.

**Step 6** After a manual backup has been created, you can view and manage it on the **Backup Management** page.

Alternatively, click the target DB instance. On the **Backups & Restorations** page, you can view and manage the manual backups.

----End

## 4.7.5 Downloading a Backup File

### Scenarios

This section describes how to download a manual or an automated backup file to a local device and restore data from the backup file.

RDS for MySQL allows you to download full backup files in .qp format.

### Constraints

- If the size of the backup data is greater than 400 MB, you are advised to use OBS Browser+ to download the backup data.

### Method 1: Using OBS Browser+

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Backup Management** page, locate the backup to be downloaded and click **Download** in the **Operation** column.

Alternatively, click the target DB instance. In the navigation pane on the left, choose **Backups & Restorations**. On the **Full Backups** page, locate the backup to be downloaded and click **Download** in the **Operation** column.

**Step 5** In the displayed dialog box, select **Use OBS Browser+** for **Download Method** and click **OK**.

1. Download OBS Browser+
2. Decompress and install OBS Browser+.
3. Log in to OBS Browser+.

For details about how to log in to OBS Browser+, see "Logging In to OBS Browser+" in the *OBS Browser+ Operation Guide*.

4. Disable certificate verification on OBS Browser+.

For details on how to configure OBS Browser+, see "Configuring the System" in the *OBS Browser+ Operation Guide*.

 **NOTE**

The OBS bucket name displayed in the **Download Backup File** pane on the RDS console does not support certificate verification. OBS Browser+ certificate verification needs to be disabled before the external bucket can be added, and then it must be enabled again after the backup is downloaded.

5. Add an external bucket.

In the **Add Bucket** dialog box of OBS Browser+, select **Add external bucket** and enter the bucket name provided in step 2 "Add an External Bucket" on the RDS console.

For details about how to add external buckets, see "Adding External Buckets" in the *OBS Browser+ Operation Guide*.

6. Download the backup file.

On the OBS Browser+ page, click the bucket that you added. In the search box on the right of OBS Browser+, enter the backup file name provided in step 3 "Download the Backup File" on the RDS console. In the search result, locate the target backup and download it.

7. After the backup is downloaded, enable OBS Browser+ certificate verification.

----End

## Method 2: Using Current Browser

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Backup Management** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

Alternatively, click the target DB instance. In the navigation pane on the left, choose **Backups & Restorations**. On the **Full Backups** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

**Step 5** In the displayed dialog box, select **Use Current Browser** for **Download Method** and click **OK**.

----End

### Method 3: Using Download URL

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Backup Management** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

Alternatively, click the target DB instance. In the navigation pane on the left, choose **Backups & Restorations**. On the **Full Backups** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

**Step 5** In the displayed dialog box, select **Use Download URL** for **Download Method**, click  to copy the URL, and click **OK**.

A valid URL for downloading the backup data is displayed.

- You can use various download tools to download backup files.
- You can also run the following command to download backup files:

```
wget -O FILE_NAME --no-check-certificate "DOWNLOAD_URL"
```

The parameters in the command are as follows:

*FILE\_NAME*: indicates the new backup file name after the download is successful. The original backup file name may be too long and exceed the maximum characters allowed by the client file system. You are advised to use the **-O** argument with **wget** to rename the backup file.

*DOWNLOAD\_URL*: indicates the location of the backup file to be downloaded. If the location contains special characters, escape is required.

----End

## 4.7.6 Downloading a Binlog Backup File


### Scenarios

RDS for MySQL allows you to download binlog backup files to your client computer and use them to restore DB instances if necessary.

### Downloading a Binlog Backup File

**Step 1** Log in to the management console.



- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance. The **Basic Information** page is displayed.
- Step 5** In the navigation pane on the left, choose **Backups & Restorations**. On the **Binlog Backups** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.
- You can also select the binlog backups to be downloaded and click **Download** above the list.
- Step 6** After the download is complete, you can view the binlog backups locally.
- End


## 4.7.7 Restoring from Backup Files to DB Instances

### Scenarios

This section describes how to use an automated or manual backup to restore a DB instance to the status when the backup was created. The restoration is at the DB instance level.

When you restore a DB instance from a backup file, a full backup file is downloaded from OBS and then restored to the DB instance at an average speed of 40 MB/s.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Backup Management** page, select the backup to be restored and click **Restore** in the **Operation** column.

Alternatively, click the target DB instance on the **Instance Management** page. On the displayed page, choose **Backups & Restorations**. On the displayed page, select the target backup to be restored and click **Restore** in the **Operation** column.

- Step 5** Select a restoration method and click **OK**.
- Create New Instance  
The **Create New Instance** page is displayed.
    - The DB engine and version of the new DB instance are the same as those of the original DB instance and cannot be changed.

- Storage space of the new DB instance is the same as that of the original DB instance by default and the new instance must be at least as large as the original DB instance.
- Other settings are the same as those of the original DB instance by default and can be modified. For details, see [Step 1: Create a DB Instance](#).
- Restore to Original
  - a. Select "I acknowledge that after I select Restore to Original, data on the original databases will be overwritten and the original DB instance will be unavailable during the restoration." and click **Next**.
  - b. Confirm the information and click **OK**.

---

**NOTICE**

- If the DB instance for which the backup is created has been deleted, data cannot be restored to the original DB instance.
- Restoring to the original DB instance will overwrite all existing data and the DB instance will be unavailable during the restoration process.

- 
- Restore to Existing
    - a. Select "I acknowledge that restoring to an existing DB instance will overwrite data on it and cause the existing DB instance to be unavailable during the restoration." and click **Next**.
    - b. Confirm the information and click **OK**.

---

**NOTICE**

- If the target existing DB instance has been deleted, data cannot be restored to it.
- Restoring to an existing DB instance will overwrite data on it and cause the existing DB instance to be unavailable.
- To restore backup data to an existing DB instance, the selected DB instance must use the same DB engine and the same or a later version than the original DB instance.
- Ensure that the storage space of the selected existing DB instance is greater than or equal to the storage space of the original DB instance. Otherwise, data will not be restored.

---

**Step 6** View the restoration result. The result depends on which restoration method was selected:

- Create New Instance

A new DB instance is created using the backup data. The status of the DB instance changes from **Creating** to **Available**.

The new DB instance is independent from the original one. If you need read replicas to offload read pressure, create one or more for the new DB instance.

After the new instance is created, a full backup will be automatically triggered.

- **Restore to Original**  
On the **Instance Management** page, the status of the original DB instance changes from **Restoring** to **Available**. If the original DB instance contains read replicas, the read replica status is the same as the original DB instance status.  
After the restoration is complete, a full backup will be automatically triggered.
- **Restore to Existing**  
On the **Instance Management** page, the status of the target existing DB instance changes from **Restoring** to **Available**. If the target existing DB instance contains read replicas, the read replica status is the same as the target existing DB instance status.  
After the restoration is complete, a full backup will be automatically triggered.

----End


## 4.7.8 Restoring a DB Instance to a Point in Time

### Scenarios

You can restore from automated backups to a specified point in time.

When you enter the time point that you want to restore the DB instance to, RDS downloads the most recent full backup file from OBS to the DB instance. Then, incremental backups are also restored to the specified point in time on the DB instance. Data is restored at an average speed of 30 MB/s.

### Restoring a DB Instance

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Backups & Restorations**. On the displayed page, click **Restore to Point in Time**.
- Step 6** Select the restoration date and time range, enter a time point within the selected time range, and select a restoration method. Then, click **OK**.
  - **Create New Instance**  
The **Create New Instance** page is displayed.
    - The DB engine and version of the new DB instance are the same as those of the original DB instance and cannot be changed.
    - Other settings are the same as those of the original DB instance by default and can be modified. For details, see [Step 1: Create a DB Instance](#).

- Restore to Original
  - a. Select "I acknowledge that after I select Restore to Original, data on the original databases will be overwritten and the original DB instance will be unavailable during the restoration." and click **Next**.
  - b. Confirm the information and click **OK**.

---

**NOTICE**

Restoring to the original DB instance will overwrite all existing data and the DB instance will be unavailable during the restoration process.

- Restore to Existing
  - a. Select "I acknowledge that restoring to an existing DB instance will overwrite data on it and cause the existing DB instance to be unavailable during the restoration." and click **Next**.
  - b. Confirm the information and click **OK**.

---

**NOTICE**

- Restoring to an existing DB instance will overwrite data on it and cause the existing DB instance to be unavailable.
- To restore backup data to an existing DB instance, the selected DB instance must use the same DB engine and the same or a later version than the original DB instance.
- Ensure that the storage space of the selected DB instance is greater than or equal to the storage space of the original DB instance. Otherwise, data will not be restored.

---

**Step 7** View the restoration result. The result depends on which restoration method was selected:

- Create New Instance

A new DB instance is created using the backup data. The status of the DB instance changes from **Creating** to **Available**.

The new DB instance is independent from the original one. If you need read replicas to offload read pressure, create one or more for the new DB instance.

After the new DB instance is created, a full backup will be automatically triggered.

- Restore to Original

On the **Instance Management** page, the status of the DB instance changes from **Restoring** to **Available**.

A new restoration time range is available. There will be a difference between the new and original time ranges. This difference reflects the duration of the restoration.

After the restoration is complete, a full backup will be automatically triggered.

- Restore to Existing  
On the **Instance Management** page, the status of the DB instance changes from **Restoring** to **Available**.  
After the restoration is complete, a full backup will be automatically triggered.
- End

## 4.7.9 Restoring a Table to a Point in Time

### Scenarios

RDS allows you to restore table data using point-in-time recovery (PITR). This ensures your data integrity and minimizes impact on the original instance performance. You can select a table and restore it to a specified point in time. The most recent full backup file will be downloaded from OBS to a temporary DB instance for restoration. After the restoration is complete, binlogs will be replayed on the temporary instance to the specified point in time. Table data will then be written back to the original DB instance. The average restoration rate is 20 MB/s.

The time required depends on the amount of data to be backed up and restored on the DB instance. Restoring tables will not overwrite data in the DB instance. You can select tables to be restored.

### Constraints

- This function is supported only for RDS for MySQL DB instances.
- RDS for MySQL table PITR does not support tables with foreign keys.
- To restore tables to a point in time, the number of tables to be restored must be less than 20,000. If the number of tables to be restored exceeds 20,000, you can restore the instance to a point in time. For details, see [Restoring a DB Instance to a Point in Time](#).
- During the table PITR, DB instances and read replicas cannot be rebooted or deleted, and their instance specifications cannot be modified.
- During the table PITR, the database or table information to be restored is read from the latest full backup before the selected time point. You can select any time point within the restoration time range. Therefore, a database or table can be restored to the earliest full backup time point when its information exists.

### Prerequisites

After the table is restored, a new table will be generated in the DB instance. Ensure the DB instance has sufficient storage space for the generated table.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** Choose **Backups & Restorations** in the navigation pane on the left. On the **Full Backups** page, choose **More > Restore Table** above the backup list. Alternatively, on the **Binlog Backups** page, click **Restore Table** above the backup list.
- Step 6** Set the restoration date, time range, time point, and tables to be restored, and click **Next: Confirm**.
- To facilitate your operations, you can search for the tables and databases to be restored.
  - After the restoration is complete, new tables with timestamps appended as suffixes to original table names are generated in the DB instance. You can rename the new tables.
  - The new table name must be unique and consist of 1 to 64 characters. Only letters, digits, underscores (\_), hyphens (-), and dollar signs (\$) are allowed.
  - Table PITR does not support the restoration of databases whose names contain periods (.).
- Step 7** On the displayed page, confirm the information and click **Submit**.
- Step 8** On the **Instance Management** page, the DB instance status is **Restoring**. During the restoration process, services are not interrupted.

You can also view the progress and result of restoring tables to a specified point in time on the **Task Center** page.

After the restoration is successful, you can manage data in the tables as required.

----End

## 4.7.10 Replicating a Backup

### Scenarios

This section describes how to replicate a manual or an automated backup. The new backup name must be different from the original backup name.


### Constraints

You can replicate backups and use them only within the same region.

### Backup Retention Policy

- RDS will delete automated backups when they expire or the DB instance for which the backups are created is deleted.
- If you want to retain the automated backups for a long time, you can replicate them to generate manual backups, which will be always retained until you delete them.
- If the storage occupied by manual backups exceeds the provisioned free backup storage, additional storage costs may incur.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance. On the **Backups & Restorations** page, locate the target backup to be replicated and click **Replicate** in the **Operation** column.
- Alternatively, choose **Backup Management**. On the displayed page, locate the manual backup to be replicated and choose **More > Replicate** or locate an automated backup and click **Replicate** in the **Operation** column.
- Step 5** In the displayed dialog box, enter a new backup name and description and click **OK**.
- The backup name must consist of 4 to 64 characters and start with a letter. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (\_).
  - The description consists of a maximum of 256 characters and cannot contain the following special characters: >!<"&'=
- Step 6** After the new backup has been created, you can view and manage it on the **Backup Management** page.

----End

## 4.7.11 Deleting a Manual Backup

### Scenarios

You can delete manual backups to free up backup storage.


---

#### NOTICE

Deleted manual backups cannot be recovered. Exercise caution when performing this operation.

---

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** In the navigation pane on the left, choose **Backup Management**. On the displayed page, locate the target manual backup to be deleted and choose **More > Delete** in the **Operation** column.

The following backups cannot be deleted:

- Automated backups
- Backups that are being restored
- Backups that are being replicated

**Step 5** In the displayed dialog box, click **OK**.

----End

## 4.8 Parameter Template Management

### 4.8.1 Creating a Parameter Template

You can use database parameter templates to manage the DB engine configuration. A database parameter template acts as a container for engine configuration values that can be applied to one or more DB instances.

This default template contains DB engine defaults and system defaults that are configured based on the engine, compute class, and allocated storage of the instance. Default parameter templates cannot be modified, but you can create your own parameter template to change parameter settings.

---

#### NOTICE

Not all of the DB engine parameters in a custom parameter template can be changed.

---

If you want to use a custom parameter template, you simply create a parameter template and select it when you create a DB instance or apply it to an existing DB instance following the instructions provided in section [Applying a Parameter Template](#).

When you have already created a parameter template and want to include most of the custom parameters and values from that template in a new parameter template, you can replicate that parameter template following the instructions provided in section [Replicating a Parameter Template](#).

The following are the key points you should know when using parameters in a parameter template:

- When you change a dynamic parameter value in a parameter template and save the change, the change takes effect immediately. When you change a static parameter value in a parameter template and save the change, the change will take effect only after you manually reboot the DB instances that the parameter template applies to.
- Improper parameter settings may have unintended consequences, including reduced performance and system instability. Exercise caution when modifying database parameters and you need to back up data before modifying parameters in a parameter template. Before applying parameter template changes to a production DB instance, you should try out these changes on a test DB instance.



 NOTE

You can create a maximum of 100 parameter templates for RDS DB instances. All RDS DB engines share the parameter template quota.

## Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, click **Create Parameter Template**.

**Step 5** In the displayed dialog box, configure required information and click **OK**.

- Select a DB engine for the parameter template.
- The template name must consist of 1 to 64 characters. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), underscores (\_), and periods (.).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=

----End

## 4.8.2 Modifying Parameters

You can modify parameters in a custom parameter template to optimize RDS database performance.

You can only change parameter values in custom parameter templates. You cannot change the parameter values in default parameter templates. When you change parameter values in a custom parameter template, the changes take effect for all DB instances that the parameter template applies to.

Global parameters must be modified on the console. Session-level parameters can be modified using SQL statements. When you modify a parameter, the time when the modification takes effect depends on the type of the parameter.


The RDS console displays the statuses of DB instances that the parameter template applies to. For example, if the DB instance has not yet used the latest modifications made to its parameter template, its status is **Parameter change. Pending reboot**. Manually reboot the DB instance for the latest modifications to take effect for that DB instance.

 NOTE

RDS has default parameter templates whose parameter values cannot be changed. You can view these parameter values by clicking the default parameter templates. If a custom parameter template is set incorrectly, the database startup may fail. If this happens, you can re-configure the custom parameter template based on the settings of the default parameter template.

## Modifying a Custom Parameter Template and Applying It to DB Instances

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** Choose **Parameter Templates** in the navigation pane on the left. On the **Custom Templates** page, click the target parameter template.

**Step 5** On the **Parameters** page, modify parameters as required.

For parameter description details, see [Suggestions on RDS for MySQL Parameter Tuning](#).

Available operations are as follows:

- To save the modifications, click **Save**.
- To cancel the modifications, click **Cancel**.
- To preview the modifications, click **Preview**.

**Step 6** After the parameter values are modified, you can click **Change History** to view the details.

**Step 7** The modifications do not take effect until you apply the parameter template to your DB instances. For details, see [Applying a Parameter Template](#).

**Step 8** View the status of the DB instance to which the parameter template was applied.

If the DB instance status is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.

- The DB instance reboot caused by instance class changes will not make parameter modifications take effect.
- If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/standby DB instances, the parameter modifications are also applied to the standby DB instance.)
- If you have modified parameters of a read replica, you need to reboot the read replica for the modifications to take effect.

----End

## Modifying Parameters of a DB Instance

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

- Step 5** In the navigation pane on the left, choose **Parameters**. On the displayed page, modify parameters as required.

#### NOTICE

Check the value in the **Effective upon Reboot** column.


- If the value is **Yes** and the DB instance status on the **Instance Management** page is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.
  - If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/standby DB instances, the parameter modifications are also applied to the standby DB instance.)
  - If you have modified parameters of a read replica, you need to reboot the read replica for the modifications to take effect.
- If the value is **No**, the modifications take effect immediately.

- To save the modifications, click **Save**.
- To cancel the modifications, click **Cancel**.
- To preview the modifications, click **Preview**.

After parameters are modified, you can click **Change History** to view parameter modification details.

----End

## Modifying Parameters of DB Instances in Batches

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, select DB instances with the same DB engine and DB engine version and choose **More > Modify Parameters** above the DB instance list.
- Step 5** On the **Modify Parameters** page, select the parameters to be modified, change the parameter values, and click **Apply**.

Only selected parameters will be applied to your DB instances. The modified parameters are automatically selected. You can also deselect them. A maximum of 30 parameters can be modified at a time.

**NOTICE**

Check the value in the **Effective upon Reboot** column.

- If the value is **Yes** and the DB instance status on the **Instance Management** page is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.
  - If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/standby DB instances, the parameter modifications are also applied to the standby DB instance.)
  - If you have modified parameters of a read replica, you need to reboot the read replica for the modifications to take effect.
- If the value is **No**, the modifications take effect immediately.

**Step 6** In the displayed dialog box, click **OK**.

**Step 7** After the parameters are modified, click the **Parameter Changes** tab on the **Parameter Templates** page to view details about the modified parameters.

----End

## 4.8.3 Exporting a Parameter Template

### Scenarios

- You can export a parameter template of a DB instance for future use. You can also apply the exported parameter template to DB instances by referring to [Applying a Parameter Template](#).
- You can export the parameter template information (parameter names, values, and descriptions) of a DB instance to a CSV file for viewing and analysis.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Parameters**. On the displayed page, click **Export** above the parameter list.

- Exporting to a custom template  
In the displayed dialog box, configure required information and click **OK**.

 **NOTE**

- The template name must consist of 1 to 64 characters. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), underscores (\_), and periods (.).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<'&'=

After the parameter template is exported, a new template is generated in the list on the **Parameter Templates** page.

- Exporting to a file

The parameter template information (parameter names, values, and descriptions) of a DB instance is exported to a CSV file. In the displayed dialog box, enter the file name and click **OK**.

 **NOTE**

The file name must start with a letter and consist of 4 to 64 characters. Only letters, digits, hyphens (-), and underscores (\_) are allowed.

----End

## 4.8.4 Comparing Parameter Templates

### Scenarios

You can compare DB instance parameters with a parameter template that uses the same DB engine to understand the differences of parameter settings.

You can also compare default parameter templates that use the same DB engine to understand the differences of parameter settings.

### Comparing Instance Parameters with a Parameter Template

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.


**Step 5** In the navigation pane on the left, choose **Parameters**. On the displayed page, click **Compare** above the parameter list.

**Step 6** In the displayed dialog box, select a parameter template to be compared and click **OK**.

- If their settings are different, the parameter names and values of both parameter templates are displayed.
- If their settings are the same, no data is displayed.

----End

## Comparing Parameter Templates

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template and click **Compare** in the **Operation** column.
- Step 5** In the displayed dialog box, select a parameter template that uses the same DB engine as the target template and click **OK**.
- If their settings are different, the parameter names and values of both parameter templates are displayed.
  - If their settings are the same, no data is displayed.

----End

## 4.8.5 Viewing Parameter Change History


### Scenarios

You can view the change history of DB instance parameters or custom parameter templates.

 **NOTE**

An exported or custom parameter template has initially a blank change history.

### Viewing Change History of a DB Instance

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Parameters**. On the displayed page, click **Change History**.


You can view the parameter name, original parameter value, new parameter value, modification status, modification time, application status, and application time.

You can apply the parameter template to DB instances as required by referring to [Applying a Parameter Template](#).

----End

## Viewing Change History of a Parameter Template

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** Choose **Parameter Templates** in the navigation pane on the left. On the **Custom Templates** page, click the target parameter template.

**Step 5** On the displayed page, choose **Change History** in the navigation pane on the left.

You can view the parameter name, original parameter value, new parameter value, modification status, and modification time.

----End

## Viewing Parameter Changes

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, click the **Parameter Changes** tab.

**Step 5** Click **View Details** in the **Operation** column.

You can view detailed information about the modified parameters.

----End

## 4.8.6 Replicating a Parameter Template

### Scenarios

You can replicate a parameter template you have created. When you have already created a parameter template and want to include most of the custom parameters and values from that template in a new parameter template, you can replicate that parameter template. You can also export the parameter template to generate a new parameter template for future use.

After a parameter template is replicated, it takes about 5 minutes before the new template is displayed.

Default parameter templates cannot be replicated, but you can create parameter templates based on the default ones.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template and click **Replicate** in the **Operation** column.

Alternatively, click the target DB instance on the **Instance Management** page. On the **Parameters** page, click **Export** to generate a new parameter template for future use.

**Step 5** In the displayed dialog box, configure required information and click **OK**.

- The template name must consist of 1 to 64 characters. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), underscores (\_), and periods (.).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=

After the parameter template is replicated, a new template is generated in the list on the **Parameter Template Management** page.

----End

## 4.8.7 Resetting a Parameter Template

### Scenarios

You can reset all parameters in a custom parameter template to their default settings.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template and choose **More > Reset** in the **Operation** column.

**Step 5** Click **Yes**.

**Step 6** The modifications take effect only after you apply the parameter template to DB instances. For details, see [Applying a Parameter Template](#).

**Step 7** View the status of the DB instance to which the parameter template is applied.

If the DB instance status is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.

- The DB instance reboot caused by instance class changes will not make parameter modifications take effect.



- If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/standby DB instances, the parameter modifications are also applied to the standby DB instance.)
- If you have modified parameters of a read replica, you need to reboot the read replica for the modifications to take effect.

----End

## 4.8.8 Applying a Parameter Template


### Scenarios

You can apply parameter templates to DB instances as needed.

- The parameter **innodb\_buffer\_pool\_size** is determined by the memory. DB instances of different specifications have different value ranges. If this parameter value is out of range of the DB instance that the parameter template applies to, the maximum value within the range is used.
- A parameter template can be applied only to DB instances of the same DB engine version.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, perform the following operations based on the type of the parameter template to be applied:

- If you intend to apply a default parameter template to DB instances, click **Default Templates**, locate the target parameter template, and click **Apply** in the **Operation** column.
- If you intend to apply a custom parameter template to DB instances, click **Custom Templates**, locate the target parameter template, and choose **More > Apply** in the **Operation** column.

A parameter template can be applied to one or more DB instances.

**Step 5** In the displayed dialog box, select one or more DB instances to which the parameter template will be applied and click **OK**.

After the parameter template is successfully applied, you can view the application records by referring to section [Viewing Application Records of a Parameter Template](#).


----End

## 4.8.9 Viewing Application Records of a Parameter Template

### Scenarios

You can view the application records of a parameter template.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** Choose **Parameter Templates** in the navigation pane on the left.
- Step 5** On the **Default Templates** page, locate the target parameter template and click **View Application Record** in the **Operation** column. Alternatively, on the **Custom Templates** page, choose **More > View Application Record** in the **Operation** column.

You can view the name or ID of the DB instance that the parameter template applies to, as well as the application status, application time, and failure cause (if failed).

----End

## 4.8.10 Modifying a Parameter Template Description





### Scenarios

You can modify the description of a parameter template you have created.

#### NOTE

You cannot modify the description of a default parameter template.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template and click  in the **Description** column.
- Step 5** Enter a new description. You can click  to submit or  to cancel the modification.
  - The description consists of a maximum of 256 characters and cannot contain the following special characters: >!<"&'=

- After the modification is successful, you can view the new description in the **Description** column of the parameter template list.

----End

## 4.8.11 Deleting a Parameter Template

### Scenarios

You can delete a custom parameter template that is no longer in use.


---

#### NOTICE

- Deleted parameter templates cannot be recovered. Exercise caution when performing this operation.
  - Default parameter templates cannot be deleted.
- 

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template to be deleted and choose **More > Delete** in the **Operation** column.

**Step 5** In the displayed dialog box, click **Yes**.

----End

## 4.9 Connection Management

### 4.9.1 Configuring and Changing a Floating IP Address

#### Scenarios

You can change floating IP addresses after migrating on-premises databases or other cloud databases to RDS.

#### Constraints

After a floating IP address is changed, the domain name needs to be resolved again. This operation takes several minutes and may interrupt database connections. Therefore, you are advised to change a floating IP address during off-peak hours.


## Configuring a Floating IP Address

When you create a DB instance, select a VPC and subnet on the **Create DB Instance** page. Then, a floating IP address will be automatically assigned to your instance.

## Changing a Floating IP Address

You can change the floating IP address of an existing DB instance.

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the **Connection Information** area on the **Basic Information** page, click **Change** next to the **Floating IP Address** field.

**Step 6** In the displayed dialog box, enter a new floating IP address and click **OK**.

An in-use IP address cannot be used as the new floating IP address of the DB instance.

----End

## 4.9.2 Binding and Unbinding an EIP

### Scenarios

By default, a DB instance is not publicly accessible (not bound with an EIP) after being created. You can bind an EIP to a DB instance for public accessibility, and you can unbind the EIP from the DB instance later if needed.

---

#### NOTICE


To ensure that the DB instance is accessible, the security group associated with the instance must allow access over the database port. For example, if the database port is 8635, ensure that the security group allows access over the 8635 port.

---

### Prerequisites

- You have applied for an EIP on the VPC console.
- You can bind an EIP to a primary DB instance or a read replica only.
- If a DB instance has already been bound with an EIP, you must unbind the EIP from the DB instance first before binding a new EIP to it.

## Binding an EIP


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Connection Management**. In the **Connection Information** area on the **Public Connection** page, click **Bind** in the **EIP** field.
- Step 6** In the displayed dialog box, all unbound EIPs are listed. Select the EIP to be bound and click **OK**.
- Step 7** On the **EIPs** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

To unbind the EIP from the DB instance, see [Unbinding an EIP](#).

----End

## Unbinding an EIP

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the DB instance that has an EIP bound.
- Step 5** In the navigation pane on the left, choose **Connection Management**. In the **Connection Information** area on the **Public Connection** page, click **Unbind** in the **EIP** field. In the displayed dialog box, click **Yes**.
- Step 6** On the **EIPs** page, view the results.

You can also view the progress or the results of unbinding an EIP from a DB instance on the **Task Center** page.

To bind an EIP to the DB instance again, see [Binding an EIP](#).

----End

## 4.9.3 Changing a Database Port

### Scenarios

This section describes how to change the database port of a primary DB instance or a read replica. For primary/standby DB instances, changing the database port of

the primary DB instance will cause the database port of the standby DB instance to also be changed.

If specific security group rules have been configured for a DB instance, you need to change the inbound rules of the security group to which the DB instance belongs after changing the database port.

## Constraints

When the database port of a DB instance is being changed, you cannot:


- Bind an EIP to the DB instance.
- Delete the DB instance.
- Create a backup for the DB instance.
- Restore from backup data or from a specific point in time to the original DB instance.


## Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.



**Step 4** On the **Instance Management** page, click the target DB instance or click  first and then click the target read replica.

**Step 5** In the **Connection Information** area on the **Basic Information** page, click  next to the **Database Port** field.

Alternatively, choose **Connection Management** in the navigation pane on the left. In the **Connection Information** area, click  next to the **Database Port** field.

### NOTE

RDS for MySQL instances can use database port 2100 to 9500.

- To submit the change, click .
  - In the dialog box, click **Yes**.
    - i. If you change the database port of the primary DB instance, that of the standby DB instance will also be changed and both DB instances will be rebooted.
    - ii. If you change the database port of a read replica, the change will not affect other DB instances. Only the read replica will be rebooted.
    - iii. This process takes 1-5 minutes.
  - In the dialog box, click **No** to cancel the modification.
- To cancel the change, click .

**Step 6** View the results on the **Basic Information** page.

----End

## 4.9.4 Configuring a Security Group Rule

### Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted in a VPC.

This section describes how to create a security group to enable specific IP addresses and ports to access RDS.

- When you attempt to connect to an RDS DB instance through an EIP, you need to configure an inbound rule for the security group associated with the DB instance.
- Check whether the ECS and RDS DB instance are in the same security group.
  - If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured.
  - If the ECS and RDS DB instance are in different security groups, you need to configure security group rules for them, separately.
    - RDS DB instance: Configure an inbound rule for the security group with which the RDS DB instance is associated.
    - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

### Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated only with one security group, but a security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

#### NOTE

If you use **0.0.0.0/0**, RDS DB instances in the security group can be accessed from any IP address.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Under **Network**, click **Virtual Private Cloud**.
- Step 3** In the navigation pane on the left, choose **Access Control > Security Groups**.
- Step 4** On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- Step 5** On the displayed page, click **Add Rule**.
- Step 6** In the displayed dialog box, set required parameters to add an inbound rule.
- Step 7** Click **OK**.

----End

## 4.10 Database Proxy (Read/Write Splitting)

### 4.10.1 Introducing Read/Write Splitting

Read/write splitting enables read and write requests to be automatically routed through a read/write splitting address. You can [enable read/write splitting](#) after read replicas are created. Write requests are automatically routed to the primary DB instance and read requests are routed to read replicas by user-defined weights.

#### NOTE

To use read/write splitting, connect to DB instances through a private network because read/write splitting addresses are private IP addresses.

## Constraints

---

### NOTICE

When read/write splitting is enabled, the system automatically deletes the existing account `rdsProxy` and creates a new `rdsProxy` account. When read/write splitting is disabled, the system automatically deletes the existing account `rdsProxy`. To prevent the system from deleting your created `rdsProxy` account, you are advised not to create it.

- RDS for MySQL 5.6 and 5.7 support read/write splitting, but RDS for MySQL 8.0 does not.
- The RDS for MySQL 8.0 client does not support connections using the read/write splitting address.
- If you delete a primary DB instance after read/write splitting is enabled, the read replicas are also deleted and the read/write splitting function is disabled.
- After read/write splitting is enabled, the database port, security group, and floating IP address of the primary DB instance and read replica cannot be changed.



- Read/write splitting does not support SSL encryption.
- Read/write splitting does not support the compression protocol.
- Read/write splitting does not support the READ UNCOMMITTED transaction isolation level.
- If multi-statements are executed, all subsequent requests will be routed to the primary DB instance. To restore the read/write splitting function, disconnect the connection from your applications and establish a connection again.
- When read and write requests are split through the read/write splitting address, all transaction requests are routed to the primary DB instance while the non-transaction read consistency is not ensured. To ensure read consistency, encapsulate requests into transactions.
- When the read/write splitting address is used, the LAST\_INSERT\_ID() function can be used only in transactions.
- When the read/write splitting address is used, the execution results of the **show processlist** command are inconsistent.
- When the read/write splitting address is used, the **show errors** and **show warnings** commands are not supported.
- When the read/write splitting address is used, user-defined variables, such as the **SET @variable** statements, are not supported.
- When the read/write splitting address is used, if stored procedures and functions depend on user variables (@variable), the execution result may be incorrect.

## 4.10.2 Best Practices for Database Proxy

### User Authentication and Connection

1. A user must have the remote login permission before using a database proxy to log in to databases.

To check whether the host of the account contains the CIDR block for read/write splitting, run the following SQL statement:

```
SELECT user,host FROM mysql.user;
```



```
mysql> select user,host from mysql.user;
+-----+-----+
| user          | host          |
+-----+-----+
| app           | %             |
| rdsProxy      | %             |
| repl         | %             |
| root         | %             |
| test         | %             |
| testGTPUser  | %             |
| mysql.session | localhost    |
| mysql.sys    | localhost    |
| root         | localhost    |
+-----+-----+
```

If the host does not contain the CIDR block, you need to grant remote access permissions. For example, you could run the following command to grant user **root** the permissions to connect to the MySQL server from **192.168.0.X**:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'192.168.0.%' IDENTIFIED BY password WITH
```

```
GRANT
OPTION;
flush privileges;
```

To query the CIDR block for read/write splitting, perform the following steps:

- a. On the **Basic Information** page of the primary instance, click the subnet name in the **Connection Information** area to go to the subnet console.
- b. Find **IPv4 CIDR Block** on the **Summary** page.
2. When modifying a security group, ensure that the inbound and outbound rules allow access to the read/write splitting address. The default port for read/write splitting is **3306**.
  - a. Log in to the management console.
  - b. Click  in the upper left corner and select a region and a project.
  - c. Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - d. On the **Instance Management** page, click  in front of the DB instance and click a read replica to go to the **Basic Information** page.
  - e. In the **Connection Information** area, click the security group.
  - f. On the **Inbound Rules** tab, check whether access through port **3306** is allowed by default. If this rule does not exist, click **Fast-Add Rule**. In the displayed dialog box, select **MySQL (3306)** and click **OK**.
3. Database proxy does not support the identity authentication plugin `caching_sha2_password` of RDS for MySQL 8.0. If the error message "auth user failed" is displayed while you are attempting to access a database proxy using an RDS for MySQL 8.0 client, run the following SQL statement to check whether the identity authentication plugin is `mysql_native_password`:

```
select plugin from mysql.user where user="Username";
```

```
mysql> select plugin from mysql.user where user="test";
+-----+
| plugin |
+-----+
| mysql_native_password |
+-----+
1 row in set (0.00 sec)
```

- If yes, add `--default-auth=mysql_native_password` or use an RDS for MySQL 5.\* client to connect to the database proxy.

```
C:\Users\...> mysql -uroot -p -h127.0.0.1 -P6033 --default-auth=mysql_native_password
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 8.0.19 MySQL Community Server - GPL

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

- If no, run the following SQL statements to change the identity authentication plugin to `mysql_native_password`:

```
ALTER USER 'Username'@'%' IDENTIFIED WITH 'mysql_native_password' BY
'Password';
FLUSH PRIVILEGES;
```

## Connection Pool Configuration

To ensure that your application obtains an available connection from a connection pool, you need to configure how the connection pool will check connection availability. For example, set **testOnBorrow** to **true** for a JDBC or Druid connection pool or set **connectionTestQuery** to **SELECT 1** for a HikariCP connection pool.

```
<bean id="hikariConfig" class="com.zaxxer.hikari.HikariConfig">
  <property name="poolName" value="springHikariCP" />
  <property name="connectionTestQuery" value="SELECT 1" />
  <property name="dataSourceClassName" value="com.mysql.jdbc.jdbc2.optional.MysqlDataSource" />
  <property name="dataSourceProperties">
    <props>
      <prop key="url">${jdbc.url}</prop>
      <prop key="user">${jdbc.username}</prop>
      <prop key="password">${jdbc.password}</prop>
    </props>
  </property>
</bean>

<bean id="dataSource" class="com.zaxxer.hikari.HikariDataSource" destroy-method="close">
  <constructor-arg ref="hikariConfig" />
</bean>
```

## Read Requests Routed to the Primary DB Instance

1. If a query statement is placed in a transaction, all transaction requests will be routed to the primary DB instance. If **set autocommit=0** is configured before a query statement, the query statement will be treated as a transaction and routed to the primary DB instance.
2. If no read replica exists, all read replicas are abnormal, or the read weights allocated to the read replicas are 0, queries will be routed to the primary DB instance. You can set read weights allocated to read replicas and the primary DB instance after read/write splitting is enabled. For details, see [Configuring Delay Threshold and Distributing Read Weight](#).
3. If multiple statements (for example, **insert xxx;select xxx**) are executed, all subsequent requests will be routed to the primary DB instance. To restore read/write splitting, disconnect the connection from your applications and then reconnect.
4. Read operations with locks (for example, **SELECT for UPDATE**) will be routed to the primary DB instance.
5. When the **/\*FORCE\_MASTER\*/** hint is used, requests will be routed to the primary DB instance.

### 4.10.3 Enabling Read/Write Splitting


Read/write splitting enables read and write requests to be automatically routed through a read/write splitting address. This section describes how to enable read/write splitting.

#### Prerequisites

There is at least one read replica created for your DB instance.

#### Procedure

- Step 1** Log in to the management console.

- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance. The **Basic Information** page is displayed.
- Step 5** In the navigation pane on the left, choose **Database Proxy**.
- Alternatively, in the **Connection Information** area on the **Basic Information** page, click **Apply** in the **Read/Write Splitting Address** field.
- Step 6** On the displayed page, click **Enable now**.
- Step 7** In the displayed dialog box, click **OK**.
- Read/write splitting maintains the database connectivity and splits read and write requests. After read/write splitting is enabled, an additional address called a read/write splitting address is provided. To use read/write splitting, switch your applications to this address.
  - Read/write splitting address: You can connect to databases through the read/write splitting address, with read and write requests automatically distributed. The read/write splitting address and the floating IP address of the primary DB instance are in the same VPC and subnet and are independent from each other.
  - Delay threshold: You can set the delay threshold after read/write splitting is enabled. For details, see section [Configuring Delay Threshold and Distributing Read Weight](#).
  - Read weight distribution: You can set read weights distributed to read replicas and primary DB instances after read/write splitting is enabled. For details, see section [Configuring Delay Threshold and Distributing Read Weight](#).
- End



## 4.10.4 Configuring Delay Threshold and Distributing Read Weight

After the read/write splitting function is enabled, you can set the delay threshold and read weight distribution as required.

**Table 4-4** Read/write splitting parameters


Parameter	Description
Delay Threshold	<p>The maximum delay for data to be synchronized from primary DB instances to read replicas. To prevent data inconsistencies between primary DB instances and read replicas for a long time, when the delay of a read replica exceeds the configured threshold, read requests are not forwarded to the read replica regardless of the read weight distributed to it.</p> <p>When read/write splitting is enabled, the default delay threshold is 30s and the default value range is 0–7,200s. It is recommended that the threshold be greater than or equal to 30s. Traffic is not allocated to read replicas whose delay exceeds the configured threshold.</p>
Read Weight Distribution	<p>When read/write splitting is enabled, the read weight of the primary DB instance is 0 by default. You can modify the read weights distributed to read replicas.</p> <p>Read replicas with higher read weight distributions process more read requests. For example, if the read weights distributed to one primary DB instance and four read replicas are 0, 100, 200, 500, and 300, respectively, the primary DB instance does not process read requests (write requests are all automatically forwarded to the primary DB instance) while the four read replicas process read requests with a ratio of 1:2:5:3.</p> <p>The system automatically distributes weights to read replicas, including read replicas created afterwards, according to their specifications based on the distribution rules listed in <a href="#">Rules for Distributing Weights</a>.</p>

## Setting Delay Threshold

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance. The **Basic Information** page is displayed.
- Step 5** In the navigation pane on the left, choose **Database Proxy**. On the displayed page, click the **Read/Write Splitting** tab.
- Step 6** In the **Read/Write Splitting** area, click  in the **Delay Threshold** field.

----End

## Distributing Read Weight

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance. The **Basic Information** page is displayed.
- Step 5** In the navigation pane on the left, choose **Database Proxy**. On the displayed page, click the **Read/Write Splitting** tab.
- Step 6** In the **Read Weight Distribution** area, click **Set Read Weight**.

### NOTE

The system automatically distributes weights to read replicas, including read replicas created afterwards, according to the default distribution rules. If a read replica breaks down or is deleted, the weight is automatically removed. After the read replica recovers, the weight is automatically restored.

----End

## 4.10.5 Changing the Read/Write Splitting Address

### Scenarios

After read/write splitting is enabled, you can change the read/write splitting address.

### Precautions


Changing the read/write splitting address will interrupt database connections and services. Therefore, change the read/write splitting address during off-peak hours or when services are stopped.

### Constraints

- The new IP address is not in use and must be in the same subnet as the RDS for MySQL DB instance.

### Procedure

You can change the read/write splitting address for DB instances with read/write splitting enabled.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the **Connection Information** area on the **Basic Information** page, click **Change** next to the **Read/Write Splitting Address** field.

Alternatively, click **Database Proxy** in the navigation pane on the left. In the **Read/Write Splitting** area on the displayed page, click **Change** next to the **Read/Write Splitting Address** field.

**Step 6** In the displayed dialog box, enter a new address. Click **OK**.

In-use IP addresses cannot be used as read/write splitting addresses.

----End

## 4.10.6 Changing the Instance Class of a DB Proxy Instance

### Scenarios

You can change the instance class (CPU or memory) of a DB proxy instance as required. If the DB instance status changes from **Changing proxy instance class** to **Available**, the change was successful.

### Constraints

- You can change the instance class of a DB proxy instance only when the statuses of your primary DB instance, read replicas, and DB proxy instance are **Available**.
- A DB proxy instance cannot be deleted when its instance class is being changed.
- Changing the instance class of a DB proxy instance will cause the instance to reboot. Therefore, perform the operation during off-peak hours.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the primary DB instance.

**Step 5** Choose **Database Proxy** from the navigation pane on the left. In the **Proxy Instance Information** area, click **Change** in the **Proxy Instance Class** field.

You can change the DB proxy instance class if required.

Changing the DB proxy instance class will cause the instance to reboot. To prevent service interruptions, change the DB proxy instance class during off-peak hours.

If you have selected **Maintenance Window** for **Scheduled Time**, the DB proxy instance will be rebooted during the instance class change time and services will be interrupted. To prevent service interruptions, you are advised to set the

maintenance window to off-peak hours. For details, see [Changing the Maintenance Window](#).

**Step 6** Confirm the specifications.

- If you need to modify your settings, click **Previous**.
- Click **Submit**.

To view the cost incurred by the instance class change, choose **Billing Center** > **My Orders** in the upper right corner.

**Step 7** View the instance class change result.

Changing the DB proxy instance class takes 13–15 minutes. During this period, the status of the primary DB instance on the **Instance Management** page is **Changing proxy instance class**. After a few minutes, view the proxy instance class on the **Database Proxy** page to check that the change is successful.

----End

## 4.10.7 Upgrading the Kernel Version of Database Proxy

### Scenarios

You can manually upgrade the RDS for MySQL database proxy to the latest kernel version to improve performance, add new functions, and fix problems.

### Precautions


- Intermittent disconnections occur during the upgrade. The time required to complete the upgrade depends on how many proxy instances there are. Perform the upgrade during off-peak hours.

### Constraints

- Only proxy instances with kernel version 2.3.0.1 or later can be upgraded manually on the console.
- A version upgrade cannot be rolled back after the upgrade is complete.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** On the **Database Proxy** page, in the **Proxy Instance Information** area, click **Upgrade** in the **Version** field.

**Step 6** In the displayed dialog box, select a scheduled time and click **OK**.

----End



## 4.10.8 Enabling or Disabling Access Control

If load balancing is enabled for a database proxy instance, the security group associated with the proxy instance does not apply. You need to use access control to grant access from specific IP addresses.


### Enabling Access Control

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** On the **Database Proxy** page, in the **Proxy Instance Information** area, click  in the **Access Control** field.

**Step 6** Click **Configure**. In the displayed dialog box, set the access control mode and IP addresses or CIDR blocks.

- Access control: The blocklist and allowlist cannot be configured at the same time. If you switch between lists, your previously entered settings will be lost. IP addresses or CIDR blocks in the blocklist are not allowed to access proxy instances.
- IP address or CIDR block: Enter valid IP addresses or CIDR blocks that meet the following requirements:
  - Each line contains an IP address or a CIDR block and ends with a line break.
  - Each IP address or CIDR block can include a description separated by a vertical bar symbol (|), for example, 192.168.10.10|RDS01. The description can include up to 50 characters but cannot contain angle brackets (<>).
  - Up to 300 IP addresses or CIDR blocks can be added.

----End


### Disabling Access Control

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.


**Step 5** On the **Database Proxy** page, in the **Proxy Instance Information** area, click  in the **Access Control** field.

----End

## 4.10.9 Disabling Read/Write Splitting

You can disable read/write splitting as required.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance. The **Basic Information** page is displayed.
- Step 5** In the navigation pane on the left, choose **Database Proxy**.
- Step 6** In the **Proxy Instance Information** area on the **Database Proxy** page, click **Disable Database Proxy**. In the displayed dialog box, click **Yes**.

#### NOTE

If database proxy is disabled, read/write splitting is also disabled and services using the read/write splitting address are interrupted. You need to switch your applications to the instance address.

----End

## 4.10.10 Rules for Distributing Weights

This section describes the rules of distributing read weights to DB instances of different specifications.

### Weight Distribution Rules

When the system automatically sets the read weights for DB instances, the weight values are fixed, as shown in the following table.

#### NOTE

The default weight equals to the number of vCPUs multiplied by 50. The weight ranges from 100 to 1000.

### Specifying Whether a SQL Statement Is Sent to the Primary DB Instance or Read Replica By Adding a Hint

Hints supported by RDS read/write splitting are as follows:

`/*FORCE_MASTER*/`: A SQL statement is executed on the primary DB instance.

`/*FORCE_SLAVE*/`: A SQL statement is executed on a read replica.

 NOTE

- In addition to the weight distribution system of read/write splitting, hints are a useful type of SQL syntax that allows you to specify whether a SQL statement is executed on the primary DB instance or on a read replica.
- Hints are only used as routing suggestions. In non-read-only SQL and non-transaction scenarios, SQL statements cannot be routed to read replicas.

### 4.10.11 Testing Read/Write Splitting Performance

After read/write splitting is enabled, databases can be connected through a read/write splitting address. You can use internal SQL commands to verify the read/write splitting performance.

#### Procedure

- Step 1** Connect to a database through a read/write splitting address by referring to [Enabling Read/Write Splitting](#).
- Step 2** Run `show last route` to view the routing result of the previous SQL statement.

Figure 4-2 Query result

```
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.


Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select 1;
+----+
| 1 |
+----+
1 row in set (0.08 sec)

mysql> show last route;
+-----+
| LAST ROUTE |
+-----+
| 193.144.128.52 |
+-----+
1 row in set (0.05 sec)

mysql>
```

 DB instance  
floating IP address

----End

## 4.11 Data Security

### 4.11.1 Resetting the Administrator Password

#### Scenarios


You can reset the administrator password of a primary instance.

If you forget the password of the administrator account **root**, you can reset the password.

## Precautions

- If you have changed the administrator password of the primary DB instance, the administrator passwords of the standby DB instance and read replicas (if any) will also be changed.
- The time required for the new password to take effect depends on the amount of service data currently being processed by the primary DB instance.
- To protect against brute force hacking attempts and ensure system security, change your password periodically.

## Method 1

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Reset Password** in the **Operation** column.
- Step 5** Enter and confirm the new password.

---

### NOTICE

Keep this password secure. The system cannot retrieve it.


---

The new password must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@\$#%^\*\_-=+?,). Enter a strong password and periodically change it for security reasons.

- To submit the new password, click **OK**.
- To cancel the reset operation, click **Cancel**.

----End

## Method 2

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the **DB Information** area on the **Basic Information** page, click **Reset Password** in the **Administrator** field.

**Step 6** Enter and confirm the new password.

#### NOTICE

Keep this password secure. The system cannot retrieve it.

The new password must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@\$#%^\*\_-=+?.). Enter a strong password and periodically change it for security reasons.

- To submit the new password, click **OK**.
- To cancel the reset operation, click **Cancel**.

----End

## 4.11.2 Changing a Security Group

### Scenarios

This section describes how to change the security group of a primary DB instance or read replica. For primary/standby DB instances, changing the security group of the primary DB instance will cause the security group of the standby DB instance to be changed as well.


### Procedure



**Step 1** Log in to the management console.


**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target primary DB instance or read replica.

**Step 5** In the **Connection Information** area on the **Basic Information** page, click  next to the **Security Group** field.

- To submit the change, click .
- To cancel the change, click .

**Step 6** Changing the security group takes 1 to 3 minutes. Click  in the upper right corner on the **Basic Information** page to view the results.

----End

## 4.12 Metrics and Alarms

## 4.12.1 Configuring Displayed Metrics

The RDS Agent monitors RDS DB instances and collects monitoring metrics only.

### Description

This section describes the RDS metrics that can be monitored by Cloud Eye as well as their namespaces and dimensions. You can use APIs provided by Cloud Eye to query the monitoring metrics and alarms generated for RDS.

### Namespace

SYS.RDS

### DB Instance Monitoring Metrics

[Table 4-5](#) lists the performance metrics of RDS for MySQL DB instances.

**Table 4-5** Performance metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds001_cpu_util	CPU Usage	CPU usage of the monitored object	0-100%	RDS for MySQL instance	1 minute
rds002_mem_util	Memory Usage	Memory usage of the monitored object	0-100%	RDS for MySQL instance	1 minute
rds003_iops	IOPS	Average number of I/O requests processed by the system in a specified period	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds004_bytes_in	Network Input Throughput	Incoming traffic in bytes per second	≥ 0 bytes/s	RDS for MySQL instance	1 minute
rds005_bytes_out	Network Output Throughput	Outgoing traffic in bytes per second	≥ 0 bytes/s	RDS for MySQL instance	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds006_conn_count	Total Connections	Total number of connections that attempt to connect to the MySQL server	≥ 0 counts	RDS for MySQL instance	1 minute
rds007_conn_active_count	Current Active Connections	Number of current active connections	≥ 0 counts	RDS for MySQL instance	1 minute
rds008_qps	QPS	Query times of SQL statements (including stored procedures) per second	≥ 0 queries/s	RDS for MySQL instance	1 minute
rds009_tps	TPS	Execution times of submitted and rollback transactions per second	≥ 0 transactions/s	RDS for MySQL instance	1 minute
rds010_innodb_buf_usage	Buffer Pool Usage	Ratio of idle pages to the total number of buffer pool pages in the InnoDB buffer	0-1	RDS for MySQL instance	1 minute
rds011_innodb_buf_hit	Buffer Pool Hit Ratio	Ratio of read hits to read requests in the InnoDB buffer	0-1	RDS for MySQL instance	1 minute
rds012_innodb_buf_dirty	Buffer Pool Dirty Block Ratio	Ratio of dirty data to used pages in the InnoDB buffer	0-1	RDS for MySQL instance	1 minute
rds013_innodb_reads	InnoDB Read Throughput	Number of read bytes per second in the InnoDB buffer	≥ 0 bytes/s	RDS for MySQL instance	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds014_innodb_write_s	InnoDB Write Throughput	Number of write bytes per second in the InnoDB buffer	≥ 0 bytes/s	RDS for MySQL instance	1 minute
rds015_innodb_read_count	InnoDB File Read Frequency	Number of times that InnoDB reads data from files per second	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds016_innodb_write_count	InnoDB File Write Frequency	Number of times that InnoDB writes data to files per second	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds017_innodb_log_write_req_count	InnoDB Log Write Requests per Second	Number of InnoDB log write requests per second	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds018_innodb_log_physical_write_count	InnoDB Log Physical Write Frequency	Number of InnoDB physical write times to log files per second	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds019_innodb_log_fsync_count	InnoDB Log fsync() Write Frequency	Number of completed fsync() write times to InnoDB log files per second	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds020_temp_tbl_count	Temporary Tables	Number of temporary tables automatically created on hard disks when MySQL statements are executed	≥ 0 tables	RDS for MySQL instance	1 minute



Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds021_myisam_buf_usage	Key Buffer Usage	MyISAM key buffer usage	0-1	RDS for MySQL instance	1 minute
rds022_myisam_buf_write_hit	Key Buffer Write Hit Ratio	MyISAM key buffer write hit ratio	0-1	RDS for MySQL instance	1 minute
rds023_myisam_buf_read_hit	Key Buffer Read Hit Ratio	MyISAM key buffer read hit ratio	0-1	RDS for MySQL instance	1 minute
rds024_myisam_disk_write_count	MyISAM Disk Write Frequency	Number of times that indexes are written to disks per second	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds025_myisam_disk_read_count	MyISAM Disk Read Frequency	Number of times that indexes are read from disks per second	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds026_myisam_buf_write_count	MyISAM Buffer Pool Write Requests per Second	Number of requests for writing indexes into the MyISAM buffer pool per second	≥ 0 counts/s	RDS for MySQL instance	1 minute
rds027_myisam_buf_read_count	MyISAM Buffer Pool Read Requests per Second	Number of requests for reading indexes from the MyISAM buffer pool per second	≥ 0 counts/s	RDS for MySQL instance	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds028_comd_ml_del_count	DELETE Statements per Second	Number of DELETE statements executed per second	≥ 0 queries/s	RDS for MySQL instance	1 minute
rds029_comd_ml_ins_count	INSERT Statements per Second	Number of INSERT statements executed per second	≥ 0 queries/s	RDS for MySQL instance	1 minute
rds030_comd_ml_ins_sel_count	INSERT_SELECT Statements per Second	Number of INSERT_SELECT statements executed per second	≥ 0 queries/s	RDS for MySQL instance	1 minute
rds031_comd_ml_rep_count	REPLACE Statements per Second	Number of REPLACE statements executed per second	≥ 0 queries/s	RDS for MySQL instance	1 minute
rds032_comd_ml_rep_sel_count	REPLACE_SELECTION Statements per Second	Number of REPLACE_SELECTION statements executed per second	≥ 0 queries/s	RDS for MySQL instance	1 minute
rds033_comd_ml_sel_count	SELECT Statements per Second	Number of SELECT statements executed per second	≥ 0 queries/s	RDS for MySQL instance	1 minute
rds034_comd_ml_upd_count	UPDATE Statements per Second	Number of UPDATE statements executed per second	≥ 0 queries/s	RDS for MySQL instance	1 minute
rds035_innodb_del_row_count	Row Delete Frequency	Number of rows deleted from the InnoDB table per second	≥ 0 rows/s	RDS for MySQL instance	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds036_innodb_ins_row_count	Row Insert Frequency	Number of rows inserted into the InnoDB table per second	≥ 0 rows/s	RDS for MySQL instance	1 minute
rds037_innodb_read_row_count	Row Read Frequency	Number of rows read from the InnoDB table per second	≥ 0 rows/s	RDS for MySQL instance	1 minute
rds038_innodb_upd_row_count	Row Update Frequency	Number of rows updated into the InnoDB table per second	≥ 0 rows/s	RDS for MySQL instance	1 minute
rds039_disk_util	Storage Space Usage	Storage space usage of the monitored object	0-100%	RDS for MySQL instance	1 minute
rds047_disk_total_size	Total Storage Space	Total storage space of the monitored object	40-4,000 GB	RDS for MySQL instance	1 minute
rds048_disk_used_size	Used Storage Space	Used storage space of the monitored object	0-4,000 GB	RDS for MySQL instance	1 minute
rds049_disk_read_throughput	Disk Read Throughput	Number of bytes read from the disk per second	≥ 0 bytes/s	RDS for MySQL instance	1 minute
rds050_disk_write_throughput	Disk Write Throughput	Number of bytes written into the disk per second	≥ 0 bytes/s	RDS for MySQL instance	1 minute

## Dimension

Key	Value
rds_instance_id	RDS for MySQL DB instance ID

## 4.12.2 Setting Alarm Rules

### Scenarios

You can set alarm rules to customize the monitored objects and notification policies and keep track of the RDS running status.

The RDS alarm rules include alarm rule names, resource types, dimensions, monitored objects, metrics, alarm thresholds, monitoring period, and whether to send notifications.

### Setting Alarm Rules

- Step 1** Log in to the management console.
  - Step 2** Under **Management & Governance**, click **Cloud Eye**.
  - Step 3** In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.
  - Step 4** On the displayed **Alarm Rules** page, click **Create Alarm Rule**.
- End

## 4.12.3 Viewing Monitoring Metrics

### Scenarios

Cloud Eye monitors the statuses of RDS DB instances. You can view RDS metrics on the management console.

Monitored data takes some time before it can be displayed. The RDS status displayed on the Cloud Eye console is about 5 to 10 minutes delayed. When you create a new RDS DB instance, it takes 5 to 10 minutes before monitoring data is displayed on Cloud Eye.

### Prerequisites

- RDS is running properly.  
Monitoring metrics of the RDS DB instances that are faulty or have been deleted are not displayed on the Cloud Eye console. You can view their monitoring metrics after they are rebooted or restored to normal.


#### NOTE

If an RDS DB instance has been faulty for 24 hours, Cloud Eye considers it to no longer exist and deletes it from the monitoring object list. You need to manually clear the alarm rules created for the DB instance.

- RDS has been running properly for about 10 minutes.  
For a newly created RDS DB instance, you need to wait a bit before you can view the metrics.

## Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and click **View Metric** in the **Operation** column to go to the Cloud Eye console.

Alternatively, click the target DB instance. On the displayed page, click **View Metric** in the upper right corner of the page to go to the Cloud Eye console.

**Step 5** On the Cloud Eye console, view monitoring metrics of the DB instance.

Cloud Eye can monitor performance metrics from the last 1 hour, 3 hours, 12 hours, 1 day, 30 days, and 7 days.

----End

## 4.13 Log Management

### 4.13.1 Viewing and Downloading Error Logs

RDS log management allows you to view database-level logs, including error logs and slow SQL query logs.

Error logs help you analyze problems with databases. You can download error logs for further analysis.

#### Viewing Log Details

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.


**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Logs**. On the **Error Logs** page, click **Log Details** to view details about error logs.

- You can select a log level in the upper right corner to view logs of the selected level.

 **NOTE**

For RDS for MySQL DB instances, the following levels of logs are displayed:

- ERROR
  - WARNING
  - NOTE
- You can click  in the upper right corner to view error logs generated in different time segments.
  - If the description of a log is truncated, locate the log and move your pointer over the description in the **Description** column to view details.

----End

## Downloading an Error Log

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Logs**. On the **Error Logs** page, click **Download**. In the log list, locate a log whose status is **Preparation completed** and click **Download** in the **Operation** column.

- The system automatically loads the downloading preparation tasks. The loading duration is determined by the log file size and network environment.
  - When the log is being prepared for download, the log status is **Preparing**.
  - When the log is ready for download, the log status is **Preparation completed**.
  - If the preparation for download fails, the log status is **Abnormal**.

Logs in the **Preparing** or **Abnormal** status cannot be downloaded.

- If the size of a log to be downloaded is greater than 40 MB, you need to use OBS Browser+ to download it. For details, see [Method 1: Using OBS Browser+](#).
- The download link is valid for 5 minutes. After the download link expires, a message is displayed indicating that the download link has expired. If you need to download the log, click **OK**.

----End

## 4.13.2 Viewing and Downloading Slow Query Logs

### Scenarios


Slow query logs record statements that exceed **long\_query\_time**. You can use these logs to identify and optimize the statements that are executing slowly.

RDS supports the following statement types:

- SELECT
- INSERT
- UPDATE
- DELETE
- CREATE

## Viewing Log Details

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Logs**. On the **Slow Query Logs** page, click **Log Details** to view details about slow query logs.

- You can view the slow query log records of a specified execution statement type or a specific time period.
- Slow query logs only record executed statements whose execution duration exceeds the threshold.
- The **long\_query\_time** parameter determines when a slow query log is recorded. However, changes to this parameter do not affect already recorded logs. If **long\_query\_time** is changed from 1s to 0.1s, none of the previously recorded logs that do not meet the new threshold are deleted. For example, a 1.5s SQL statement that was recorded when the threshold was 1s will not be deleted now that the new threshold is 2s.

----End

## Downloading a Slow Query Log

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Logs**. On the **Slow Query Logs** page, click **Download**. In the log list, locate a log whose status is **Preparation completed** and click **Download** in the **Operation** column.

- The system automatically loads the downloading preparation tasks. The loading duration is determined by the log file size and network environment.
  - When the log is being prepared for download, the log status is **Preparing**.

- When the log is ready for download, the log status is **Preparation completed**.
  - If the preparation for download fails, the log status is **Abnormal**.  
Logs in the **Preparing** or **Abnormal** status cannot be downloaded.
  - If the size of a log to be downloaded is greater than 40 MB, you need to use OBS Browser+ to download it. For details, see [Method 1: Using OBS Browser+](#).
  - The download link is valid for 5 minutes. After the download link expires, a message is displayed indicating that the download link has expired. If you need to download the log, click **OK**.
- End


### 4.13.3 Viewing Failover/Switchover Logs

You can view failover or switchover logs of RDS for MySQL DB instances to evaluate the impact on services.

 **NOTE**

Only failover and switchover logs within 30 days are displayed.

#### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Logs**. On the displayed page, click **Failover/Switchover Logs** to view log details.

These logs record the failovers caused by database exceptions and manual switchovers.

----End

### 4.13.4 Enabling the SQL Audit Function

After you enable the SQL audit function, all SQL operations will be recorded in log files. You can [download](#) audit logs to view log details.

By default, SQL audit is disabled because enabling this function may affect database performance. This section describes how to enable, modify, or disable SQL audit.

 **NOTE**

- After you enable the SQL audit function, the system records all SQL operations and uploads logs every half an hour or when the size is accumulated to 100 MB.
- After SQL audit is enabled, log files will occupy your backup space.




## Constraints



Only the versions listed below support SQL audit. .

- MySQL 5.6.43 and later versions for DB instances using cloud disks, 5.6.47.3 and later versions for DB instances using local disks
- MySQL 5.7.23 and later versions for DB instances using cloud disks, MySQL 5.7.29.3 and later versions for DB instances using local disks
- MySQL 8.0

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **SQL Audits**. On the displayed page, click **Set SQL Audit** above the list. In the displayed dialog box, configure information as required and click **OK**.

### Enabling or setting SQL audit

- To retain SQL audit logs, set  (disabled) to  (enabled).
- Audit logs are retained for 7 days by default but can be retained from anywhere from 1 to 732 days if needed.

### Disabling SQL audit

To disable SQL audit, toggle  (enabled) to  (disabled).

- If you select the check box "I acknowledge that after audit log is disabled, all audit logs are deleted.", all audit logs will be deleted.

---

#### NOTICE

Deleted audit logs cannot be recovered. Exercise caution when performing this operation.

---

- If you do not select the check box "I acknowledge that after audit log is disabled, all audit logs are deleted.", the audit logs will be retained.


----End

## 4.13.5 Downloading SQL Audit Logs

If you [enable the SQL audit function](#), all SQL operations will be logged, and you can download audit logs to view details. The minimum time unit of audit logs is

second. By default, the SQL audit function is disabled. Enabling this function may affect performance.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **SQL Audits**.
- Step 6** On the displayed page, select a time range in the upper right corner, select SQL audit logs to be downloaded in the list, and click **Download** above the list to download SQL audit logs in batches.

Alternatively, select an audit log and click **Download** in the **Operation** column to download an individual SQL audit log.

- Step 7** The following figure shows the SQL audit log content. For field descriptions, see [Table 4-6](#).

**Figure 4-3** RDS for MySQL audit logs

```
"6","408543","1159","Connect",2020-03-20T03:35:05 UTC,"", "", "", "", "", "", "", "", ""
"7","408543","0","Quit",2020-03-20T03:35:05 UTC,"", "", "", "", "", "", "", "", ""
"8","408544","1159","Connect",2020-03-20T03:35:20 UTC,"", "", "", "", "", "", "", "", ""
"9","408544","0","Quit",2020-03-20T03:35:20 UTC,"", "", "", "", "", "", "", "", ""
"10","408546","1159","Connect",2020-03-20T03:35:35 UTC,"", "", "", "", "", "", "", "", ""
"11","408546","0","Quit",2020-03-20T03:35:35 UTC,"", "", "", "", "", "", "", "", ""
"12","408547","1159","Connect",2020-03-20T03:35:50 UTC,"", "", "", "", "", "", "", "", ""
"13","408547","0","Quit",2020-03-20T03:35:50 UTC,"", "", "", "", "", "", "", "", ""
```

**Table 4-6** Audit log field description

Parameter	Description
record_id	ID of a single record, which is the unique global ID of each SQL statement recorded in the audit log.
connection_id	ID of the session executed by the record, which is the same as the ID in the <b>show processlist</b> command output.
connection_status	Session status, which is usually the returned error code of a statement. If a statement is successfully executed, the value <b>0</b> is returned.
name	Recorded type name. Generally, DML and DDL operations are QUERY, connection and disconnection operations are CONNECT and QUIT, respectively.
timestamp	Recorded UTC time.

Parameter	Description
command_class	SQL command type. The value is the parsed SQL type, for example, select or update. (This field does not exist if the connection is disconnected.)
sqltext	Executed SQL statement content. (This field does not exist if the audit connection is disconnected.)
user	Login account.
host	Login host. The value is <b>localhost</b> for local login and is empty for remote login.
external_user	External username.
ip	IP address of the remotely-connected client. The local IP address is empty.
default_db	Default database on which SQL statements are executed.

----End

## 4.14 Task Center

### 4.14.1 Viewing a Task

You can view the progress and results of tasks on the **Task Center** page.

#### NOTE

RDS allows you to view and manage the following tasks:

- Creating DB instances
- Creating read replicas
- Scaling up storage space
- Changing single DB instances to primary/standby
- Switching primary/standby DB instances
- Rebooting DB instances
- Binding EIPs to DB instances
- Unbinding EIPs from DB instances
- Restoring data to new DB instances
- Migrating a standby MySQL DB instance
- Restoring MySQL data to existing DB instances

#### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** Choose **Task Center** in the navigation pane on the left. Locate the target task and view its details.
- To identify the target task, you can use the task name, order ID, or DB instance name/ID, or simply enter the target task name in the search box in the upper right corner.
  - You can view the progress and status of tasks in a specific period. The default period is seven days.  
The task list shows tasks that have been executed in the past 30 days.
  - You can view instant tasks in the following statuses:
    - Running
    - Completed
    - Failed
  - You can view the task creation and completion time.

----End

## 4.14.2 Deleting a Task Record

You can delete task records so that they are no longer displayed in the task list. This operation only deletes the task records, and does not delete the DB instances or terminate the tasks that are being executed.


---

### NOTICE

Deleted task records cannot be recovered. Exercise caution when performing this operation.

---

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** Choose **Task Center** in the navigation pane on the left. On the displayed page, locate the target task record to be deleted and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

You can delete the records of instant tasks in any of the following statuses:

- Completed
- Failed

----End

# 5 Working with RDS for PostgreSQL

---

## 5.1 Database Migration

### 5.1.1 Migrating Data to RDS for PostgreSQL Using psql

#### Preparing for Data Migration

PostgreSQL supports logical backups. You can use the `pg_dump` logical backup function to export backup files and then import them to RDS using `psql`.

You can access RDS DB instances through an EIP or through an ECS.

#### Preparations

1. Prepare an ECS for accessing DB instances in the same VPC or prepare a device for accessing RDS through an EIP.
  - To connect to a DB instance through an ECS, you need to create an ECS first.  
For details about how to create and connect to an ECS, see section [How Can I Obtain the IP Address of an ECS?](#)
  - To connect to a DB instance through an EIP, you must:
    - i. Bind an EIP to the DB instance. For details, see [Binding an EIP](#).
    - ii. Ensure that the local device can access the EIP that has been bound to the DB instance.

2. Install the PostgreSQL client on the prepared ECS or device.

For details, see [How Can I Install a PostgreSQL Client?](#)

#### NOTE

The PostgreSQL client version must be the same as the version of RDS for PostgreSQL. The PostgreSQL database or client will provide `pg_dump` and `psql`.

## Exporting Data

Before migrating an existing PostgreSQL database to RDS, you need to export the PostgreSQL database.

### NOTICE

- The export tool must match the DB engine version.
- Database migration is performed offline. Before the migration, you must stop any applications using the source database.

**Step 1** Log in to the ECS or the device that can access RDS.

**Step 2** Use the `pg_dump` tool to export the source database into an SQL file.

```
pg_dump --username=<DB_USER> --host=<DB_ADDRESS> --port=<DB_PORT> --format=plain --file=<BACKUP_FILE> <DB_NAME>
```

- **DB\_USER** indicates the database username.
- **DB\_ADDRESS** indicates the database address.
- **DB\_PORT** indicates the database port.
- **BACKUP\_FILE** indicates the name of the file to which the data will be exported.
- **DB\_NAME** indicates the name of the database to be migrated.

Enter the database password when prompted.

Example:

```
$ pg_dump --username=root --host=192.168.151.18 --port=5432 --format=plain --file=backup.sql my_db
```

**Password for user root:**

After this command is executed, a **backup.sql** file will be generated as follows:

```
[rds@localhost ~]$ ll backup.sql
```

```
-rw-r-----. 1 rds rds 2714 Sep 21 08:23 backup.sql
```

----End

## Importing Data

**Step 1** Log in to the ECS or the device that can access RDS.

**Step 2** Ensure that the destination database to which data is to be imported exists.

If the destination database does not exist, run the following command to create a database:

```
# psql --host=<RDS_ADDRESS> --port=<DB_PORT> --username=root --dbname=postgres -c "create database <DB_NAME>;"
```

- **RDS\_ADDRESS** indicates the IP address of the RDS DB instance.

- **DB\_PORT** indicates the RDS DB instance port.
- **DB\_NAME** indicates the name of the database to be imported.

**Step 3** Import the exported file to RDS.

```
# psql --host=<RDS_ADDRESS> --port=<DB_PORT> --username=root --
dbname=<DB_NAME> --file=<BACKUP_DIR>/backup.sql
```

- **RDS\_ADDRESS** indicates the IP address of the RDS DB instance.
- **DB\_PORT** indicates the RDS DB instance port.
- **DB\_NAME** indicates the name of the database to which data is to be imported. Ensure that the database exists.
- **BACKUP\_DIR** indicates the directory where the **backup.sql** file is stored.

Enter the password for the RDS DB instance when prompted.

Example:

```
# psql --host=172.16.66.198 --port=5432 --username=root --dbname=my_db --
file=backup.sql
```

**Password for user root:**

**Step 4** View the import result.

```
my_db=> \l my_db
```

In this example, the database named **my\_db** has been imported.

```
my_db=> \l my_db
List of databases
Name | Owner | Encoding | Collate | Ctype | Access privileges
-----+-----+-----+-----+-----+-----
my_db | root | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
(1 row)
```

----End

## 5.1.2 Migrating Data to RDS for PostgreSQL Using the Export and Import Functions of DAS

### Scenarios


To back up or migrate data, you can use Data Admin Service (DAS) to export data from the source database first and then import the data to from your local PC or OBS bucket to the destination database.

### Constraints

- Only one file that is no larger than 1 GB can be imported at a time.
- Binary fields such as BINARY, VARBINARY, TINYBLOB, BLOB, MEDIUMBLOB, and LONGBLOB are not supported.

### Exporting Data

**Step 1** Log in to the management console.

- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Databases**, click **Relational Database Service**.
- Step 4** On the **Instances** page, locate the DB instance and click **Log In** in the **Operation** column.
- Step 5** On the displayed login page, enter the username and password and click **Log In**.
- Step 6** On the top menu bar, choose **Import and Export > Export**.
- Step 7** On the displayed page, click **Create Task** and choose **Export Database** or **Export SQL Result** as required. The following takes database export as an example.
- Alternatively, click **Quick Export** and select the target database. On the displayed page, select a storage path and click **OK**.
- Step 8** On the displayed page, set parameters as required in areas **Basic Information** and **Advanced Settings**. Then, select the tables to be exported on the right.

 **NOTE**

- In a SQL result export task, the executed SQL statements cannot exceed 5 MB.
- Databases are classified into user databases and system databases. System databases cannot be exported. If system database data is required, deploy system database services in a created user database, so that you can export the system database data from the user database.
- DAS connects to your standby database to export data. This prevents the primary database from being affected by data export. However, if the standby database has a high replication delay, the exported data may not be the latest.

- Step 9** After settings are complete, click **OK**.
- Step 10** In the task list, view the task ID, type, status, and progress.
- Step 11** Click **Details** in the **Operation** column to view task details.
- End

## Importing Data

- Step 1** On the top menu bar, choose **Import and Export > Import**.
- Step 2** Import a file from your local PC or an OBS bucket.
- From your local PC

In the upper left corner, click **Create Task**. On the displayed page, select an import type, select **Upload file** for **File Source**, set the attachment storage, and upload the file. Then, set other parameters as required.

For security purposes, imported files are stored in OBS buckets.

 **NOTE**

- To keep your data secure, provide your own OBS bucket to store the attachments you upload. In this way, DAS automatically connects to your OBS bucket for in-memory reading.
- If you select **Delete the uploaded file upon an import success**, the file you uploaded will be automatically deleted from the OBS bucket after being imported to the destination database.



- From an OBS bucket  
In the upper left corner, click **Create Task**. On the displayed page, select an import type, select **Choose from OBS** for **File Source**, and select a file from the bucket. Then, set other parameters as required.

 **NOTE**

The file uploaded from an OBS bucket will not be deleted upon an import success.

**Step 3** After setting the import parameters, click **Create**. Confirm the information again before you click **OK** because original data may be overwritten after data import.

**Step 4** View the import progress in the task list or check task details.

----End

## 5.2 Parameter Tuning

### 5.2.1 Suggestions on RDS for PostgreSQL Parameter Tuning

Parameters are key configuration items in a database system. Improper parameter settings may adversely affect the stable running of databases. This section describes some important parameters for your reference. For details, visit the [PostgreSQL official website](#).

For details on how to modify RDS for PostgreSQL parameters on the console, see [Modifying Instance Parameters](#).

#### Sensitive Parameters

The following parameters can result in system security and stability issues if set improperly:

- The **search\_path** parameter must be set to a schema sequence where schemas are separated by commas (.). Ensure that the schemas exist. Otherwise, the database performance will be affected.
- If you enable the parameter **log\_duration**, SQL statements containing sensitive information may be recorded in logs. You are advised to disable this parameter.
- **log\_min\_duration\_statement** specifies how many milliseconds a query has to run before it has to be logged. The unit is millisecond. Setting this parameter to **0** means that all statements are recorded. Setting this parameter to **-1** means that no statement is recorded.
- The **temp\_file\_limit** parameter specifies the maximum amount of disk space (in KB) that a session can use for temporary files. It supports RDS for PostgreSQL 11, 12, and 13 only. Changing this parameter value is a high-risk operation. Exercise caution when deciding to perform this operation.
  - If the parameter value exceeds the threshold, the DB instance will become unavailable.
  - If the parameter value is changed to a larger value for temporary use but is not changed to the original value after the use, the disk space will be

continuously used to store temporary files. If the disk space is used up, services will be interrupted and the DB instance will become unavailable.

## Performance Parameters

The following parameters can affect database performance:

- If **log\_statement** is set to **ddl**, **mod**, or **all**, the operations for creating and deleting database users (including passwords and other sensitive information) are recorded. This operation affects database performance. Exercise caution when setting this parameter.
- Enabling the following parameters will affect the database performance: **log\_hostname**, **log\_duration**, **log\_connections**, and **log\_disconnections**. Exercise caution when enabling these parameters.

## 5.3 Permissions Management

### 5.3.1 Creating a User and Granting Permissions

This chapter describes how to use Identity and Access Management (IAM) to implement fine-grained permissions control for your RDS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing RDS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or cloud service to perform efficient O&M on your RDS resources.

If your account does not require individual IAM users, skip this chapter.

This section describes the procedure for granting permissions (see [Figure 5-1](#)).

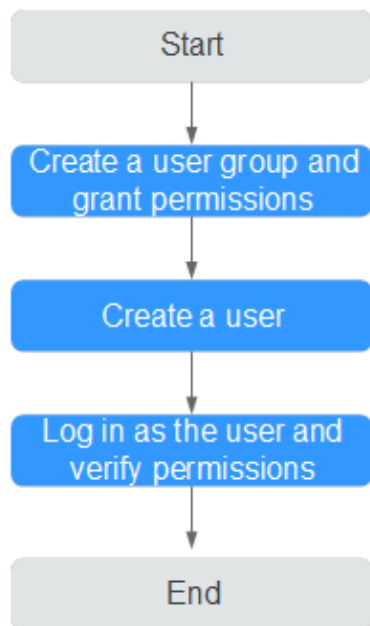
### Prerequisites

Learn about the permissions (see ) supported by RDS and choose policies or roles according to your requirements. For the system policies of other services, see .

For more information about system policies supported by RDS, see [Permissions Management](#).

## Process Flow

**Figure 5-1** Process for granting RDS permissions



1. Create a user group and assign permissions to it.  
Create a user group on the IAM console, and attach the **RDS ReadOnlyAccess** policy to the group.
2. Create an IAM user and add it to the user group  
Create a user on the IAM console and add the user to the group created in **1**.
3. Log in and verify permissions.  
Log in to the RDS console by using the created user, and verify that the user only has read permissions for RDS.
  - Choose **Service List > Relational Database Service** and click **Buy DB Instance**. If a message appears indicating that you have insufficient permissions to perform the operation, the **RDS ReadOnlyAccess** policy has already taken effect.
  - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **RDS ReadOnlyAccess** policy has already taken effect.

### 5.3.2 RDS Custom Policies

Custom policies can be created as a supplement to the system policies of RDS. For the actions supported for custom policies, see "Permissions Policies and Supported Actions" in *Relational Database Service API Reference*.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see "Creating a Custom Policy" in *Identity and Access Management User Guide*. The following section contains examples of common RDS custom policies.

## Example Custom Policies

- Example 1: Allowing users to create RDS DB instances

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["rds:instance:create"]
  }]
}
```

- Example 2: Denying RDS DB instance deletion

A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the **RDS FullAccess** policy to a user but you want to prevent the user from deleting RDS DB instances. Create a custom policy for denying RDS DB instance deletion, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on RDS DB instances except deleting RDS DB instances. The following is an example deny policy:

```
{
  "Version": "1.1",
  "Statement": [{
    "Action": ["rds:instance:delete"],
    "Effect": "Deny"
  }]
}
```

## 5.4 Instance Lifecycle

### 5.4.1 Creating a Same DB Instance as an Existing DB Instance

#### Scenarios


This section describes how to quickly create a DB instance with the same configurations as the selected one.

#### NOTE

- You can create DB instances with the same configurations numerous times.
- This function is unavailable for read replicas.

#### Procedure

**Step 1** Log in to the management console.

- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Create Same DB Instance** in the **Operation** column.
- Step 5** On the displayed page, the configurations are the same as those of the selected DB instance. You can change them as required. Then, click **Next**.
- For details about RDS for PostgreSQL DB instance configurations, see section [Step 1: Create a DB Instance](#).
- Step 6** Confirm the instance specifications.
- Step 7** Refresh the DB instance list and view the status of the DB instance. If the status is **Available**, it has been created successfully.
- You can manage the DB instance on the **Instance Management** page.
- End

## 5.4.2 Rebooting DB Instances or Read Replicas



### Scenarios

You may need to reboot a DB instance during maintenance. For example, after you modify some parameters, a reboot is required for the modifications to take effect. You can reboot a primary DB instance or a read replica on the management console.

### Constraints

- If the DB instance status is **Abnormal**, the reboot may fail.
- Rebooting a DB instance will cause service interruptions. During this period, the DB instance status is **Rebooting**.
- Rebooting DB instances will cause instance unavailability and clear cached memory. To prevent traffic congestion during peak hours, you are advised to reboot DB instances during off-peak hours.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance, or click  in the front of a DB instance and then locate the target read replica. Choose **More > Reboot** in the **Operation** column.
- Alternatively, click the target DB instance on the **Instance Management** page to go to the **Basic Information** page. In the upper right corner, click **Reboot**.

For primary/standby DB instances, if you reboot the primary DB instance, the standby DB instance is also rebooted automatically.

**Step 5** In the displayed dialog box, select a scheduled time, and click **Yes**.

**Step 6** Refresh the DB instance list and view the status of the DB instance. If its status is **Available**, it has rebooted successfully.

----End

## 5.4.3 Selecting Displayed Items

### Scenarios


You can customize which instance items are displayed on the **Instance Management** page.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click  to edit columns displayed in the DB instance list.

- The following items are displayed by default: **Name/ID, Description, DB Instance Type, DB Engine Version, Status, Floating IP Address, and Operation**.

These default items cannot be deselected.

- In a single project, you can select up to 10 items: **Name/ID, Description, DB Instance Type, DB Engine Version, Status, Floating IP Address, Created, Database Port, Storage Type, and Operation**.
- For multiple projects, if you have enabled the ProjectMan permissions, you can select up to 10 items: **Name/ID, Description, DB Instance Type, DB Engine Version, Status, Floating IP Address, Created, Database Port, Storage Type, and Operation**.

----End

## 5.4.4 Exporting DB Instance Information



### Scenarios

You can export information about all or selected DB instances to view and analyze DB instance information.



### Constraints

A tenant can export a maximum of 3,000 instances at a time. The time required for the export depends on the number of instances.

## Exporting Information About All DB Instances

- Step 1** Log in to the management console.
  - Step 2** Click  in the upper left corner and select a region and a project.
  - Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - Step 4** On the **Instance Management** page, click  in the upper right corner of the page. By default, information about all DB instances are exported. In the displayed dialog box, you can select the items to be exported and click **Export**.
  - Step 5** Find a .csv file locally after the export task is completed.
- End

## Exporting Information About Selected DB Instances

- Step 1** Log in to the management console.
  - Step 2** Click  in the upper left corner and select a region and a project.
  - Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - Step 4** On the **Instance Management** page, filter DB instances by DB engine, DB instance name, DB instance ID, or floating IP address, or select the DB instances to be exported, and click  in the upper right corner of the page. In the displayed dialog box, select the items to be exported and click **Export**.
  - Step 5** Find a .csv file locally after the export task is completed.
- End

## 5.4.5 Deleting a DB Instance or Read Replica

### Scenarios

To release resources, you can delete DB instances or read replicas as required on the **Instance Management** page.


### Constraints

- DB instances cannot be deleted when operations are being performed on them. They can be deleted only after the operations are complete.
- If you delete a DB instance, its automated backups will also be deleted and you will no longer be billed for them. Manual backups, however, will be retained and generate additional costs.



#### NOTICE

- If you delete a primary DB instance, its standby DB instance and read replicas (if any) are also deleted automatically. Exercise caution when performing this operation.
- Deleted DB instances cannot be recovered and resources are released. Exercise caution when performing this operation. If you want to retain data, **create a manual backup** first before deleting the DB instance.
- You can use a manual backup to restore a DB instance. For details, see **Restoring from Backup Files to DB Instances**.

## Deleting a DB Instance

- Step 1** Log in to the management console.
  - Step 2** Click  in the upper left corner and select a region and a project.
  - Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - Step 4** On the **Instance Management** page, locate the primary DB instance to be deleted and click **More > Delete** in the **Operation** column.
  - Step 5** In the displayed dialog box, click **Yes**.
  - Step 6** Refresh the DB instance list later to confirm that the deletion was successful.
- End

## Deleting a Read Replica

- Step 1** Log in to the management console.
  - Step 2** Click  in the upper left corner and select a region and a project.
  - Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - Step 4** On the **Instance Management** page, locate the target DB instance and click . All the read replicas created for the DB instance are displayed.
  - Step 5** Locate the read replica to be deleted and click **More > Delete** in the **Operation** column.
  - Step 6** In the displayed dialog box, click **Yes**.
  - Step 7** Refresh the DB instance list later to check that the deletion is successful.
- End

## 5.5 Instance Modifications






## 5.5.1 Changing a DB Instance Name

### Scenarios



You can change the name of a primary DB instance or read replica.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and click  next to it to edit the DB instance name. Then, click **OK**.

Alternatively, click the target DB instance to go to the **Basic Information** page. In the **DB Instance Name** field in the **DB Information** area, click  to edit the DB instance name.

Different DB instances can have the same name. The instance name must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (\_) are allowed.

- To submit the change, click .
- To cancel the change, click .

- Step 5** View the results on the **Basic Information** page.

----End


## 5.5.2 Changing the Failover Priority

### Scenarios

You can configure the failover priority for reliability or for availability, depending on your service requirements.

- **Reliability:** This option is selected by default. Data consistency is preferentially ensured during a primary/standby failover. This is recommended for users whose highest priority is data consistency.
- **Availability:** Database availability is preferentially ensured during a primary/standby failover. This is recommended for users who require their databases to provide uninterrupted online services.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.

- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - Step 4** On the **Instance Management** page, click the target primary/standby DB instances.
  - Step 5** In the **DB Information** area on the displayed **Basic Information** page, click **Change** in the **Failover Priority** field. In the displayed dialog box, select a priority and click **OK**.
  - Step 6** View the results on the **Basic Information** page.
- End

## 5.5.3 Changing a DB Instance Class


### Scenarios

You can change the instance class (CPU or memory) of a DB instance as required. If the status of a DB instance changes from **Changing instance class** to **Available**, the change is successful.

### Constraints

- A DB instance cannot be deleted when its instance class is being changed.
- If the primary DB instance has a read replica, the new DB instance class must be less than or equal to the read replica class. When changing the read replica class, ensure that the selected class is greater than or equal to the current primary instance class.
- After the instance class is changed, some parameters are automatically changed to the default values defined in the new instance class. The parameters are **max\_connections**, **max\_worker\_processes**, **max\_wal\_senders**, **max\_prepared\_transactions**, and **max\_locks\_per\_transaction**.
- After you change instance classes, the DB instances will be rebooted and service will be interrupted. Therefore, you are advised to change instance classes during off-peak hours.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Change Instance Class** in the **Operation** column.  
  
Alternatively, click the target DB instance to go to the **Basic Information** page. In the **DB Information** area, click **Change** in the **Instance Class** field.
- Step 5** On the displayed page, specify the new instance class and click **Next**.

**Step 6** View the DB instance class change result.

Changing the DB instance class takes 5–15 minutes. During this period, the status of the DB instance on the **Instance Management** page is **Changing instance class**. After a few minutes, click the DB instance and view the instance class on the displayed **Basic Information** page to check that the change is successful.

**NOTICE**

After the CPU or memory of an RDS for PostgreSQL DB instance is changed, the system will change the values of the following parameters accordingly:

- **shared\_buffers**
- **max\_connections**
- **maintenance\_work\_mem**

----End

## 5.5.4 Scaling up Storage Space

### Scenarios

If the original storage space is insufficient as your services grow, scale up storage space of your DB instance.

The DB instance needs to preserve at least 15% of its capacity to work properly. The new minimum storage space required to make this instance available has been automatically calculated for you. You are advised to set alarm rules for the **Storage Space Usage** metric to learn about the storage usage in a timely manner. For details, see [Setting Alarm Rules](#).

For details about the causes and solutions of insufficient storage space, see [What Should I Do If My Data Exceeds the Available Storage of an RDS for MySQL Instance?](#)


RDS allows you to scale up storage space of DB instances but you cannot change the storage type. During the scale-up period, services are not interrupted.

### Constraints

- The maximum allowed storage is 4,000 GB. There is no limit on the number of scale-ups.
- For primary/standby DB instances, scaling up the primary DB instance will cause the standby DB instance to also be scaled up accordingly.
- The instance cannot be deleted during scaling.
- Storage space can only be scaled up.

### Scaling up a Primary DB Instance

**Step 1** Log in to the management console.

- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Scale Storage Space** in the **Operation** column.

You can also perform the following operations to scale up storage space:

- Click the target DB instance to enter the **Basic Information** page. In the **Storage Space** area, click **Scale**.

- Step 5** On the displayed page, specify the new storage space and click **Next**.

The minimum start value of each scaling is 10 GB. A DB instance can be scaled up only by a multiple of 10 GB. The allowed maximum storage space is 4,000 GB.

- Step 6** Confirm specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

- Step 7** View the scale-up result.


Scaling up storage space takes 3-5 minutes. During the time period, the status of the DB instance on the **Instance Management** page will be **Scaling up**. Click the DB instance and view the utilization on the displayed **Basic Information** page to verify that the scale-up is successful.

----End


## Scaling up a Read Replica

Scaling up the storage space of a read replica does not affect that of the primary DB instance. Therefore, you can separately scale read replicas to meet service requirements. New storage space of read replicas after scaling up must be greater than or equal to that of the primary DB instance.

- Step 1** Log in to the management console.

- Step 2** Click  in the upper left corner and select a region and a project.

- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

- Step 4** On the **Instance Management** page, locate the target DB instance and click  in front of it. Locate a read replica to be scaled and choose **More > Scale Storage Space** in the **Operation** column.

You can also perform the following operations to scale up storage space:

- Click the target DB instance to enter the **Basic Information** page. In the **Storage Space** area, click **Scale**.

- Step 5** On the displayed page, specify the new storage space and click **Next**.

The minimum start value of each scaling is 10 GB. A read replica can be scaled up only by a multiple of 10 GB. The allowed maximum storage space is 4,000 GB.

**Step 6** Confirm specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

**Step 7** View the scale-up result.

Scaling up storage space takes 3-5 minutes. During this time, the status of the read replica on the **Instance Management** page will be **Scaling up**. Click the read replica and view the utilization on the displayed **Basic Information** page to verify that the scale-up is successful.

----End

## 5.5.5 Changing the Maintenance Window

### Scenarios


The maintenance window is 02:00–06:00 by default and you can change it as required. To prevent service interruptions, you are advised to set the maintenance window to off-peak hours.

### Precautions

- During the maintenance window, the DB instance will be intermittently disconnected for one or two times. Ensure that your applications support automatic reconnection.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance. In the **DB Information** area on the **Basic Information** page, click **Change** in the **Maintenance Window** field.

**Step 5** In the displayed dialog box, select a maintenance window and click **OK**.

#### NOTE

Changing the maintenance window does not affect the execution time of the scheduled tasks in the original maintenance period.

----End


## 5.5.6 Changing a DB Instance Type from Single to Primary/Standby

### Scenarios

- RDS enables you to change single DB instances to primary/standby DB instances to improve instance reliability.
- Primary/standby DB instances support automatic failover. If the primary DB instance fails, the standby DB instance takes over services quickly. You are advised to deploy primary and standby DB instances in different AZs for high availability and disaster recovery.
- Anti-affinity deployment is supported for primary/standby DB instances to prevent the entire instance unavailability due to the failure of a single host.


### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.


**Step 4** On the **Instance Management** page, locate a single DB instance and choose **More > Change Type to Primary/Standby** in the **Operation** column.

Alternatively, click the target DB instance. In the DB instance topology, click  on the left to change the instance type from single to primary/standby.

**Step 5** Select a standby AZ. Other configurations are the same as those of the primary DB instance by default. Confirm the configurations and click **Submit**.

It is recommended that the standby AZ be different from the primary AZ to provide failover and high availability.

**Step 6** After a single DB instance is changed to primary/standby instance, you can view and manage it on the **Instance Management** page.

- The DB instance is in the **Changing type to primary/standby** status. You can view the progress on the **Task Center** page. For details, see [Task Center](#).
- In the upper right corner of the DB instance list, click  to refresh the list. After the DB instance type is changed to primary/standby, the instance status will change to **Available** and the instance type will change to **Primary/Standby**.

----End

## 5.5.7 Manually Switching Between Primary and Standby DB Instances

### Scenarios

If you choose to create primary/standby DB instances, RDS will create a primary DB instance and a synchronous standby DB instance in the same region. You can access the primary DB instance only. The standby instance serves as a backup. You can manually promote the standby DB instance to the new primary instance for failover support.

### Constraints

- A DB instance is running properly.
- The replication between the primary and standby instances is normal.

### Procedure


**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target primary/standby DB instance.

**Step 5** In the **DB Information** area on the displayed **Basic Information** page, click **Switch** in the **DB Instance Type** field.

Alternatively, click  in the DB instance topology on the **Basic Information** page to perform a primary/standby switchover.

---

#### NOTICE

A primary/standby switchover may cause service interruptions for several seconds or minutes (depending on the replication delay). To prevent traffic congestion, you are advised to perform a switchover during off-peak hours.


---

**Step 6** In the **Switch Primary/Standby Instances** dialog box, click **Yes** to switch between the primary and standby DB instances.

If the replication status is **Available** and the replication delay is greater than 300s, the primary/standby switchover task cannot be delivered.

**Step 7** After the switchover is successful, check the status of the DB instance on the **Instance Management** page.

- During the switchover, the DB instance status is **Switchover in progress**.

- In the upper right corner of the DB instance list, click  to refresh the list. After the switchover is successful, the DB instance status will become **Available**.

----End

## 5.5.8 Migrating a Standby DB Instance



### Scenarios

You can migrate a standby DB instance to another AZ in the same region as the original AZ.

#### NOTE

- DDL operations and scheduled events will be suspended during migration. To prevent service interruption, perform the migration during off-peak hours.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Migrate Standby DB Instance** in the **Operation** column.
- Step 5** On the displayed page, select a target AZ and click **Submit**.
- Step 6** After the migration is complete, you can view and manage the DB instance on the **Instance Management** page.
  - During the migration process, the DB instance status is **Migrating standby DB instance**. You can view the progress on the **Task Center** page. For details, see section [Task Center](#).
  - In the upper right corner of the DB instance list, click  to refresh the list. After the migration is complete, the DB instance status will become **Available**.
  - In the **DB Information** on the **Basic Information** page, you can view the AZ hosting the standby DB instance.

----End

## 5.6 Read Replicas



## 5.6.1 Introducing Read Replicas

### Introduction

RDS for PostgreSQL supports read replicas.

In read-intensive scenarios, a single DB instance may be unable to handle the read pressure and service performance may be affected. To expand the DB instance read ability to offload read pressure on the database, you can create one or more read replicas in a region. These read replicas can process a large number of read requests and increase application throughput. You need to separately configure connection addresses of the primary DB instance and each read replica on your applications so that all read requests can be sent to read replicas and write requests to the primary DB instance.

A read replica uses a single-node architecture (without a slave node). Changes to the primary DB instance are also automatically synchronized to all associated read replicas through the native PostgreSQL replication function. The synchronization is not affected by network latency. Read replicas and the primary DB instance must be in the same region but can be in different AZs.

### Functions

- The specifications of a read replica must be at least equal to those of the primary DB instance to prevent long delay and high load.
- You do not need to maintain separate database accounts or databases. They are synchronized from the primary DB instance.
- Read replicas support system performance monitoring. RDS provides up to 20 monitoring metrics, including storage space, IOPS, the number of database connections, CPU usage, and network traffic. You can view these metrics to learn about the load on DB instances.
- Read replicas do not support automated backups or manual backups.
- Read replicas do not support restoration from backups to new, existing, or original read replicas.
- Data cannot be migrated to read replicas.
- Read replicas do not support database creation and deletion.
- Read replicas do not support database account creation.
- The specifications of read replicas must be greater than or equal to the specifications of the current primary DB instance.

### Constraints

- You can purchase read replicas only for your created primary DB instance.
- A maximum of five read replicas can be created for each primary DB instance.

### Creating and Managing a Read Replica

- [Creating a Read Replica](#)
- [Managing a Read Replica](#)

## 5.6.2 Creating a Read Replica

### Scenarios

Read replicas are used to enhance the read capabilities and reduce the load on primary DB instances.

You can create read replicas as needed.


#### NOTE

A maximum of five read replicas can be created for a primary DB instance.

The specifications of read replicas must be greater than or equal to the specifications of the current primary DB instance.


### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and click **Create Read Replica** in the **Operation** column.

Alternatively, click the target DB instance. In the DB instance topology, click  under the primary DB instance to create read replicas.

**Step 5** On the displayed page, configure information about the DB instance and click **Next**.

**Table 5-1** Basic information

Parameter	Description
Region	By default, read replicas are in the same region as the primary DB instance.
DB Instance Name	Different DB instances can have the same name. The instance name must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.
DB Engine	Same as the DB engine of the primary DB instance by default and cannot be changed.
DB Engine Version	Same as the DB engine version of the primary DB instance by default and cannot be changed.
AZ	RDS allows you to deploy primary DB instances and read replicas in a single AZ or across AZs to improve reliability.

**Table 5-2** Instance specifications


Parameter	Description
Instance Class	<p>Refers to the CPU and memory of a DB instance. Different instance classes have different numbers of database connections and maximum IOPS.</p> <p>For details about instance classes, see section <a href="#">DB Instance Classes</a>.</p> <p>After a DB instance is created, you can change its CPU and memory. For details, see section <a href="#">Changing a DB Instance Class</a>.</p>
Storage Type	<p>Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be.</p> <ul style="list-style-type: none"> <li>• <b>Common I/O</b>: uses the SATA disk type that supports a maximum throughput of 90 MB/s.</li> <li>• <b>Ultra-high I/O</b>: uses the SSD disk type that supports a maximum throughput of 350 MB/s.</li> </ul>
Storage Space	<p>Contains the file system overhead required for inode, reserved block, and database operation.</p> <p>By default, storage space of a read replica is the same as that of the primary DB instance.</p>

**Table 5-3** Network

Parameter	Description
VPC	Same as the primary DB instance's VPC.
Subnet	Same as the primary DB instance's subnet. A floating IP address is automatically assigned when you create a read replica. You can also enter an unused floating IP address in the subnet CIDR block. After the read replica is created, you can change the floating IP address.
Security Group	Same as the primary DB instance's security group.

**Step 6** Confirm specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

**Step 7** After a read replica has been created, you can view and manage it on the **Instance Management** page by clicking  on the left of the DB instance to which it belongs.

Alternatively, click the target DB instance. In the DB instance topology, click the name of the target read replica. You can view and manage it in the displayed pane.

----End


## Follow-up Operations

### Managing a Read Replica


## 5.6.3 Managing a Read Replica

### Entering the Management Interface Through a Read Replica

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** In the DB instance list, click  to expand the DB instance details and click the target read replica to go to the **Basic Information** page.

----End

### Entering the Management Interface Through a Primary DB Instance

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** Click the name of the primary DB instance with which the target read replica is associated to go to the **Basic Information** page.

**Step 5** In the DB instance topology, click the name of the target read replica. You can view and manage it in the displayed pane.

----End

## Deleting a Read Replica

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** In the DB instance list, click  in front of a DB instance, locate the read replica to be deleted, and choose **More > Delete** in the **Operation** column.

----End

## 5.7 Backups and Restorations

### 5.7.1 Working with Backups

RDS supports backups and restorations to ensure data reliability.

#### Automated Backups

Automated backups are created during the backup time window for your DB instances. RDS saves automated backups based on a retention period you specify. If necessary, you can restore to any point in time during your backup retention period. For details, see [Configuring an Automated Backup Policy](#).

#### Manual Backups

Manual backups are user-initiated full backups of DB instances. They are retained until you delete them manually. For details, see [Creating a Manual Backup](#).

#### Downloading a Backup File

You can download a full or an incremental backup file for local data backup or restoration. For details, see [Downloading a Full Backup File](#) and [Downloading an Incremental Backup File](#).

### 5.7.2 Configuring an Automated Backup Policy

#### Scenarios

When you create a DB instance, an automated backup policy is enabled by default. For security purposes, the automated backup policy cannot be disabled. After the DB instance is created, you can customize the automated backup policy as required and then RDS backs up data based on the automated backup policy you configure.

RDS backs up data at the DB instance level, rather than the database level. If a database is faulty or data is damaged, you can restore it from backups. Backups are saved as packages in OBS buckets to ensure data confidentiality and durability. Since backing up data affects database read and write performance, the automated backup time window should be set to off-peak hours.


The automated backup policy is enabled by default as follows:

- Retention period: 7 days. Backup files that exceed the retention period will be deleted and cannot be restored.
- Time window: An hour within 24 hours, such as 01:00-02:00 or 12:00-13:00. The backup time is configured based on UTC time and is adjusted for daylight saving time, which changes at different times depending on the time zone.

- Backup cycle: Each day of the week

## Modifying an Automated Backup Policy

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** On the **Backups & Restorations** page, click **Modify Backup Policy**.

- **Retention Period** is the number of days that your automated backups are saved for. Increasing the retention period will improve data reliability.
- If you shorten the retention period, the new backup policy takes effect for all backup files. The backup files that have expired will be deleted.
- The backup retention period is the number of days you want automated full and incremental backups of your DB instance to be saved for. It ranges from 1–732 days. The backup time window is one hour. You are advised to select an off-peak time window for automated backups. By default, each day of the week is selected for **Backup Cycle** and you can change it. At least one day must be selected.

**Step 6** Click **OK**.

----End

## 5.7.3 Set a Cross-Region Backup Policy

### Scenarios

RDS can store backup files in the storage space that is in a different region from the DB instance for disaster recovery. If a DB instance in a region is faulty, you can use the backup files in another region to restore data to a new DB instance.

After you enable cross-region backup, the backup files are automatically stored in the region you specify. On the **Backup Management** page of the RDS console, you can click **View Backup** in the **Operation** column and manage cross-region backup files.

### Enabling or Modifying a Cross-Region Backup Policy

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Backups & Restorations**. On the displayed page, click **Set Cross-Region Backup Policy**.

- If you enable **Cross-Region Full Backup**, automated full backup files of the DB instance are stored in OBS in the region you specify.
- If you enable **Cross-Region Log Backup**, full and incremental backup files of the DB instance are stored in OBS in the region you specify.
- Cross-region backup files can be retained from 1 to 1,825 days.
- Only new backup files generated after you set a cross-region backup policy will be stored in OBS in the region you specify.
- After the cross-region log backup function is enabled, you can restore a DB instance to a specified time point only after the next automated full backup replication is complete. The specified time point must be later than the time when the automated full backup is complete.
- All cross-region backups of your DB instances are stored in the region you specify.
- After you enable cross-region backup, the completed backup files in the region where your instance is located will be asynchronously replicated to the region you specify.

**Step 6** Click **OK**.

**Step 7** Choose **Backup Management** in the left navigation pane and click **Cross-Region Backups** to manage cross-region backup files.

- By default, all instances with cross-region backups are displayed.
  - To modify the cross-region backup policy, click **Set Cross-Region Backup** in the **Operation** column.
  - To view generated cross-region backup files, click **View Cross-Region Backup** in the **Operation** column. If a DB instance fails, you can use the cross-region backup files to restore data to a new DB instance.

----End

## Disabling a Cross-Region Backup Policy

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Backup Management** page, click the **Cross-Region Backups** tab.

**Step 5** Locate a target DB instance and click **Set Cross-Region Backup** in the **Operation** column. On the displayed page, disable the cross-region backup policy.

**Step 6** Click **OK**.

----End

## 5.7.4 Creating a Manual Backup


### Scenarios

RDS allows you to create manual backups of a running primary DB instance. You can use these backups to restore data.

#### NOTE

When you delete a DB instance, its automated backups are also deleted but its manual backups are retained.


### Method 1

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Create Backup** in the **Operation** column.
- Step 5** In the displayed dialog box, enter a backup name and description. Then, click **OK**. If you want to cancel the backup creation task, click **Cancel**.
  - The backup name must consist of 4 to 64 characters and start with a letter. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (\_).
  - The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=
  - The time required for creating a manual backup depends on the amount of data.
- Step 6** After a manual backup has been created, you can view and manage it on the **Backup Management** page.

Alternatively, click the target DB instance. On the **Backups & Restorations** page, you can view and manage the manual backups.

----End

### Method 2

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.



- Step 5** On the **Backups & Restorations** page, click **Create Backup**. In the displayed dialog box, enter a backup name and description and click **OK**. If you want to cancel the backup creation task, click **Cancel**.
- The backup name must consist of 4 to 64 characters and start with a letter. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (\_).
  - The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=
  - The time required for creating a manual backup depends on the amount of data.
- Step 6** After a manual backup has been created, you can view and manage it on the **Backup Management** page.
- Alternatively, click the target DB instance. On the **Backups & Restorations** page, you can view and manage the manual backups.
- End

## 5.7.5 Downloading a Full Backup File

### Scenarios


This section describes how to download a manual or an automated backup file to a local device and restore data from the backup file.

RDS for PostgreSQL enables you to download full backup files.

### Constraints

- If the size of the backup data is greater than 400 MB, you are advised to use OBS Browser+ to download the backup data.

### Method 1: Using OBS Browser+

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Backup Management** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.
- Alternatively, click the target DB instance. In the navigation pane on the left, choose **Backups & Restorations**. On the **Full Backups** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.
- Step 5** In the displayed dialog box, select **Use OBS Browser+** for **Download Method** and click **OK**.
1. Download OBS Browser+
  2. Decompress and install OBS Browser+.

3. Log in to OBS Browser+.
4. Disable certificate verification on OBS Browser+.  
For details on how to configure OBS Browser+, see "Configuring the System" in the *OBS Browser+ Operation Guide*.

 **NOTE**

The OBS bucket name displayed in the **Download Backup File** pane on the RDS console does not support certificate verification. OBS Browser+ certificate verification needs to be disabled before the external bucket can be added, and then it must be enabled again after the backup is downloaded.

5. Add an external bucket.  
In the **Add Bucket** dialog box of OBS Browser+, select **Add external bucket** and enter the bucket name provided in step 2 "Add an External Bucket" on the RDS console.
6. Download the backup file.  
On the OBS Browser+ page, click the bucket that you added. In the search box on the right of OBS Browser+, enter the backup file name provided in step 3 "Download the Backup File" of the RDS console. In the search result, locate the target backup and download it.
7. After the backup is downloaded, enable OBS Browser+ certificate verification.

**Step 6** Restore data locally as required.

----End

## Method 2: Using Current Browser

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Backup Management** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

Alternatively, click the target DB instance. In the navigation pane on the left, choose **Backups & Restorations**. On the **Full Backups** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

**Step 5** In the displayed dialog box, select **Use Current Browser** for **Download Method** and click **OK**.

**Step 6** Restore data locally as required.

----End

## Method 3: Using Download URL

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Backup Management** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

Alternatively, click the target DB instance. In the navigation pane on the left, choose **Backups & Restorations**. On the **Full Backups** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

**Step 5** In the displayed dialog box, select **Use Download URL** for **Download Method**, click  to copy the URL, and click **OK**.

A valid URL for downloading the backup data is displayed.

- You can use various download tools to download backup files.
- You can also run the following command to download backup files:

```
wget -O FILE_NAME --no-check-certificate "DOWNLOAD_URL"
```

The parameters in the command are as follows:

*FILE\_NAME*: indicates the new backup file name after the download is successful. The original backup file name may be too long and exceed the maximum characters allowed by the client file system. You are advised to use the **-O** argument with **wget** to rename the backup file.

*DOWNLOAD\_URL*: indicates the location of the backup file to be downloaded. If the location contains special characters, escape is required.

**Step 6** Restore data locally as required.

----End

## 5.7.6 Downloading an Incremental Backup File


### Scenarios

This section describes how to download a manual or an automated backup file to a local device and restore data from the backup file.

RDS for PostgreSQL enables you to download incremental backup files.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance. Choose **Backups & Restorations** in the navigation pane on the left. On the **Incremental Backups** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

You can also select the incremental backups to be downloaded and click **Download** above the list.

**Step 5** After the download is complete, you can view the incremental backups locally.

----End

## 5.7.7 Restoring from Backup Files to RDS for PostgreSQL

### Scenarios

This section describes how to use an automated or manual backup to restore a DB instance to the status when the backup was created. The restoration is at the DB instance level.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Backup Management** page, select the backup to be restored and click **Restore** in the **Operation** column.

Alternatively, click the target DB instance on the **Instance Management** page. On the displayed page, choose **Backups & Restorations**. On the displayed page, select the target backup to be restored and click **Restore** in the **Operation** column.

**Step 5** Select a restoration method and click **OK**.

- Create New Instance

The **Create New Instance** page is displayed.

- The DB engine and version of the new DB instance are the same as those of the original DB instance and cannot be changed.
- Storage space of the new DB instance is the same as that of the original DB instance by default and the new instance must be at least as large as the original DB instance.
- Other settings are the same as those of the original DB instance by default and can be modified. For details, see [Step 1: Create a DB Instance](#).

- Restore to Original

- a. Select "I acknowledge that after I select Restore to Original, data on the original databases will be overwritten and the original DB instance will be unavailable during the restoration." and click **Next**.
- b. Confirm the information and click **OK**.

---

**NOTICE**

- If the DB instance for which the backup is created has been deleted, data cannot be restored to the original DB instance.
- Restoring to the original DB instance will overwrite all existing data and the DB instance will be unavailable during the restoration process.

- 
- Restore to Existing
    - a. Select "I acknowledge that restoring to an existing DB instance will overwrite data on it and cause the existing DB instance to be unavailable during the restoration." and click **Next**.
    - b. Confirm the information and click **OK**.

---

**NOTICE**

- If the target existing DB instance has been deleted, data cannot be restored to it.
- Restoring to an existing DB instance will overwrite data on it and cause the existing DB instance to be unavailable.
- To restore backup data to an existing DB instance, the selected DB instance must be in the same VPC as the original DB instance and must have the same DB engine and the same or later version than the original DB instance.
- Ensure that the storage space of the selected DB instance is greater than or equal to the storage space of the original DB instance. Otherwise, data will not be restored.

---

**Step 6** View the restoration result. The result depends on which restoration method was selected:

- Create New Instance

A new DB instance is created using the backup data. The status of the DB instance changes from **Creating** to **Available**.

The new DB instance is independent from the original one. If you need read replicas to offload read pressure, create one or more for the new DB instance.

After the new instance is created, a full backup will be automatically triggered.
- Restore to Original

On the **Instance Management** page, the status of the target existing DB instance changes from **Restoring** to **Available**. If the original existing DB instance contains read replicas, the read replica status is the same as the original DB instance status.

After the restoration is complete, a full backup will be automatically triggered.
- Restore to Existing

On the **Instance Management** page, the status of the target existing DB instance changes from **Restoring** to **Available**. If the target existing DB

instance contains read replicas, the read replica status is the same as the target existing DB instance status.

After the restoration is complete, a full backup will be automatically triggered.

----End

## 5.7.8 Restoring a DB Instance to a Point in Time


### Scenarios

You can restore from automated backups to a specified point in time.

RDS for PostgreSQL supports restoration to a new, the original, or an existing DB instance.

When you enter the time point that you want to restore the DB instance to, RDS downloads the most recent full backup file from OBS to the DB instance. Then, incremental backups are also restored to the specified point in time on the DB instance. Data is restored at an average speed of 30 MB/s.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Backups & Restorations**. On the displayed page, click **Restore to Point in Time**.
- Step 6** Select the restoration date and time range, enter a time point within the selected time range, and select a restoration method. Then, click **OK**.
  - Create New Instance
 

The **Create New Instance** page is displayed.

    - The DB engine and version of the new DB instance are the same as those of the original DB instance and cannot be changed.
    - Storage space of the new DB instance is the same as that of the original DB instance by default and the new instance must be at least as large as the original DB instance.
    - Other settings are the same as those of the original DB instance by default and can be modified. For details, see section [Step 1: Create a DB Instance](#).
  - Restore to Original
    - a. Select "I acknowledge that after I select Restore to Original, data on the original databases will be overwritten and the original DB instance will be unavailable during the restoration." and click **Next**.
    - b. Confirm the information and click **OK**.

---

**NOTICE**

Restoring to the original DB instance will overwrite all existing data and the DB instance will be unavailable during the restoration process.

- Restore to Existing
  - a. Select "I acknowledge that restoring to an existing DB instance will overwrite data on it and cause the existing DB instance to be unavailable during the restoration." and click **Next**.
  - b. Confirm the information and click **OK**.

---

**NOTICE**

- Restoring to an existing DB instance will overwrite data on it and cause the existing DB instance to be unavailable.
- To restore backup data to an existing DB instance, the selected DB instance must be in the same VPC as the original DB instance and must have the same DB engine and the same or later version than the original DB instance.
- Ensure that the storage space of the selected DB instance is greater than or equal to the storage space of the original DB instance. Otherwise, data will not be restored.

---

**Step 7** View the restoration result. The result depends on which restoration method was selected:

- Create New Instance

A new DB instance is created using the backup data. The status of the DB instance changes from **Creating** to **Available**.

The new DB instance is independent from the original one. If you need read replicas to offload read pressure, create one or more for the new DB instance.

After the restoration is complete, a full backup will be automatically triggered.
- Restore to Original

On the **Instance Management** page, the status of the DB instance changes from **Restoring** to **Available**.

A new restoration time range is available on the **Restore to Point in Time** page. There will be a difference between the new and original time ranges. This difference reflects the duration of the restoration.

After the restoration is complete, a full backup will be automatically triggered.
- Restore to Existing

On the **Instance Management** page, the status of the DB instance changes from **Restoring** to **Available**.

After the restoration is complete, a full backup will be automatically triggered.

----End

## 5.7.9 Replicating a Backup

### Scenarios

This section describes how to replicate a manual or an automated backup. The new backup name must be different from the original backup name.

### Constraints

You can replicate backups and use them only within the same region.

### Backup Retention Policy

- RDS will delete automated backups when they expire or the DB instance for which the backups are created is deleted.
- If you want to retain the automated backups for a long time, you can replicate them to generate manual backups, which will be always retained until you delete them.
- If the storage occupied by manual backups exceeds the provisioned free backup storage, additional storage costs may incur.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance. On the **Backups & Restorations** page, locate the target backup to be replicated and click **Replicate** in the **Operation** column.

Alternatively, choose **Backup Management**. On the displayed page, locate the manual backup to be replicated and choose **More > Replicate** or locate an automated backup and click **Replicate** in the **Operation** column.

**Step 5** In the displayed dialog box, enter a new backup name and description and click **OK**.

- The backup name must consist of 4 to 64 characters and start with a letter. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (\_).
- The description consists of a maximum of 256 characters and cannot contain the following special characters: >!<"&'=

**Step 6** After the new backup has been created, you can view and manage it on the **Backup Management** page.

----End



## 5.7.10 Deleting a Manual Backup

### Scenarios

You can delete manual backups to free up backup storage.


---

**NOTICE**

Deleted manual backups cannot be recovered. Exercise caution when performing this operation.

---

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** In the navigation pane on the left, choose **Backup Management**. On the displayed page, locate the target manual backup to be deleted and choose **More > Delete** in the **Operation** column.

The following backups cannot be deleted:

- Automated backups
- Backups that are being restored
- Backups that are being replicated

- Step 5** In the displayed dialog box, click **OK**.

----End

## 5.8 Parameter Template Management

### 5.8.1 Creating a Parameter Template

You can use database parameter templates to manage the DB engine configuration. A database parameter template acts as a container for engine configuration values that can be applied to one or more DB instances.

This default template contains DB engine defaults and system defaults that are configured based on the engine, compute class, and allocated storage of the instance. Default parameter templates cannot be modified, but you can create your own parameter template to change parameter settings.

**NOTICE**

Not all of the DB engine parameters in a custom parameter template can be changed.

If you want to use a custom parameter template, you simply create a parameter template and select it when you create a DB instance or apply it to an existing DB instance following the instructions provided in section [Applying a Parameter Template](#).

When you have already created a parameter template and want to include most of the custom parameters and values from that template in a new parameter template, you can replicate that parameter template following the instructions provided in section [Replicating a Parameter Template](#).

The following are the key points you should know when using parameters in a parameter template:

- When you change a dynamic parameter value in a parameter template and save the change, the change takes effect immediately. When you change a static parameter value in a parameter template and save the change, the change will take effect only after you manually reboot the DB instances that the parameter template applies to.
- Improper parameter settings may have unintended consequences, including reduced performance and system instability. Exercise caution when modifying database parameters and you need to back up data before modifying parameters in a parameter template. Before applying parameter template changes to a production DB instance, you should try out these changes on a test DB instance.

 **NOTE**

You can create a maximum of 100 parameter templates for RDS DB instances. All RDS DB engines share the parameter template quota.

## Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, click **Create Parameter Template**.

**Step 5** In the displayed dialog box, configure required information and click **OK**.

- Select a DB engine for the parameter template.
- The template name must consist of 1 to 64 characters. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), underscores (\_), and periods (.).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=

----End

## 5.8.2 Modifying Instance Parameters

You can modify parameters in a custom parameter template to optimize RDS database performance.

You can change parameter values in custom parameter templates only and cannot change parameter values in default parameter templates. When you change parameter values in a custom parameter template, the changes take effect for all DB instances that the parameter template applies to.


When you modify a parameter, the time when the modification takes effect is determined by the type of the parameter.

The RDS console displays the statuses of DB instances that the parameter template applies to. For example, if the DB instance has not yet used the latest modifications made to its parameter template, its status is **Parameter change. Pending reboot**. Manually reboot the DB instance for the latest modifications to take effect for that DB instance.

### NOTE

RDS has default parameter templates whose parameter values cannot be changed. You can view these parameter values by clicking the default parameter templates. If a custom parameter template is set incorrectly, the database startup may fail. If this happens, you can re-configure the custom parameter template based on the settings of the default parameter template.

## Modifying a Custom Parameter Template and Applying It to DB Instances

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Parameters**. On the displayed page, modify parameters as required.

Available operations are **Save**, **Cancel**, and **Preview**:

- To save the modifications, click **Save**.
- To cancel the modifications, click **Cancel**.
- To preview the modifications, click **Preview**.

### NOTICE

In the **Effective upon Reboot** column:

- If the value is **Yes** and the DB instance status on the **Instance Management** page is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.
  - If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/standby DB instances, the parameter modifications are also applied to the standby DB instance.)
  - If you have modified parameters of a read replica, you need to reboot the read replica for the modifications to take effect.
- If the value is **No**, the modifications take effect immediately.

After parameters are modified, you can view parameter change history by referring to section [Viewing Parameter Change History](#).

----End

## Modifying Parameter Template Parameters

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** Choose **Parameter Templates** in the navigation pane on the left. On the **Custom Templates** page, click the target parameter template.

**Step 5** On the **Parameters** page, modify parameters as required.

Available operations are **Save**, **Cancel**, and **Preview**:

- To save the modifications, click **Save**.
- To cancel the modifications, click **Cancel**.
- To preview the modifications, click **Preview**.

**Step 6** After the parameter values are modified, you can click **Change History** to view the modification details.

**Step 7** The modifications take effect only after you apply the parameter template to DB instances. For details, see [Applying a Parameter Template](#).

**Step 8** View the status of the DB instance to which the parameter template was applied.

If the DB instance status is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.

- A DB instance reboot caused by instance class changes will not make parameter modifications take effect.
- If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/

standby DB instances, the parameter modifications are also applied to the standby DB instance.)

- If you have modified parameters of a read replica, you need to reboot the read replica for the modifications to take effect.

----End

## 5.8.3 Exporting a Parameter Template

### Scenarios

- You can export a parameter template of a DB instance for future use. You can also apply the exported parameter template to DB instances by referring to [Applying a Parameter Template](#).
- You can export the parameter template information (parameter names, values, and descriptions) of a DB instance to a CSV file for viewing and analysis.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Parameters**. On the displayed page, click **Export** above the parameter list.

- Exporting to a custom template

In the displayed dialog box, configure required information and click **OK**.

#### NOTE

- The template name must consist of 1 to 64 characters. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), underscores (\_), and periods (.).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=

After the parameter template is exported, a new template is generated in the list on the **Parameter Templates** page.

- Exporting to a file

The parameter template information (parameter names, values, and descriptions) of a DB instance is exported to a CSV file. In the displayed dialog box, enter the file name and click **OK**.

#### NOTE

The file name must start with a letter and consist of 4 to 64 characters. Only letters, digits, hyphens (-), and underscores (\_) are allowed.

----End

## 5.8.4 Comparing Parameter Templates

### Scenarios

You can compare DB instance parameters with a parameter template that uses the same DB engine to understand the differences of parameter settings.

You can also compare default parameter templates that use the same DB engine to understand the differences of parameter settings.

### Comparing Instance Parameters with a Parameter Template

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Parameters**. On the displayed page, click **Compare** above the parameter list.

**Step 6** In the displayed dialog box, select a parameter template to be compared and click **OK**.

- If their settings are different, the parameter names and values of both parameter templates are displayed.
- If their settings are the same, no data is displayed.

----End

### Comparing Parameter Templates

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template and click **Compare** in the **Operation** column.

**Step 5** In the displayed dialog box, select a parameter template that uses the same DB engine as the target template and click **OK**.

- If their settings are different, the parameter names and values of both parameter templates are displayed.
- If their settings are the same, no data is displayed.

----End

## 5.8.5 Viewing Parameter Change History

### Scenarios


You can view the change history of DB instance parameters or custom parameter templates.

 **NOTE**

An exported or custom parameter template has initially a blank change history.

### Viewing Change History of a DB Instance

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Parameters**. On the displayed page, click **Change History**.


You can view the parameter name, original parameter value, new parameter value, modification status, modification time, application status, and application time.

You can apply the parameter template to DB instances as required by referring to section [Applying a Parameter Template](#).

----End

### Viewing Change History of a Parameter Template

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** Choose **Parameter Templates** in the navigation pane on the left. On the **Custom Templates** page, click the target parameter template.

**Step 5** On the displayed page, choose **Change History** in the navigation pane on the left.

You can view the parameter name, original parameter value, new parameter value, modification status, and modification time.

----End

## 5.8.6 Replicating a Parameter Template

### Scenarios

You can replicate a parameter template you have created. When you have already created a parameter template and want to include most of the custom parameters and values from that template in a new parameter template, you can replicate that parameter template. You can also export the parameter template to generate a new parameter template for future use.

After a parameter template is replicated, it takes about 5 minutes before the new template is displayed.

Default parameter templates cannot be replicated, but you can create parameter templates based on the default ones.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template and click **Replicate** in the **Operation** column.

Alternatively, click the target DB instance on the **Instance Management** page. On the **Parameters** page, click **Export** to generate a new parameter template for future use.

**Step 5** In the displayed dialog box, configure required information and click **OK**.

- The template name must consist of 1 to 64 characters. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), underscores (\_), and periods (.).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=

After the parameter template is replicated, a new template is generated in the list on the **Parameter Template Management** page.

----End

## 5.8.7 Resetting a Parameter Template


### Scenarios

You can reset all parameters in a custom parameter template to their default settings.

### Procedure

**Step 1** Log in to the management console.



- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template and choose **More > Reset** in the **Operation** column.
- Step 5** Click **Yes**.
- Step 6** The modifications take effect only after you apply the parameter template to DB instances. For details, see [Applying a Parameter Template](#).
- Step 7** View the status of the DB instance to which the parameter template is applied.

If the DB instance status is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.

- The DB instance reboot caused by instance class changes will not make parameter modifications take effect.
- If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/standby DB instances, the parameter modifications are also applied to the standby DB instance.)
- If you have modified parameters of a read replica, you need to reboot the read replica for the modifications to take effect.


----End

## 5.8.8 Applying a Parameter Template

### Scenarios

You can apply parameter templates to DB instances as needed. A parameter template can be applied only to DB instances of the same version.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Parameter Templates** page, perform the following operations based on the type of the parameter template to be applied:
- If you intend to apply a default parameter template to DB instances, click **Default Templates**, locate the target parameter template, and click **Apply** in the **Operation** column.
  - If you intend to apply a custom parameter template to DB instances, click **Custom Templates**, locate the target parameter template, and choose **More > Apply** in the **Operation** column.

A parameter template can be applied to one or more DB instances.

**Step 5** In the displayed dialog box, select one or more DB instances to which the parameter template will be applied and click **OK**.

After the parameter template is successfully applied, you can view the application records by referring to section [Viewing Application Records of a Parameter Template](#).

----End

## 5.8.9 Viewing Application Records of a Parameter Template

### Scenarios

You can view the application records of a parameter template.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** Choose **Parameter Templates** in the navigation pane on the left.

**Step 5** On the **Default Templates** page, locate the target parameter template and click **View Application Record** in the **Operation** column. Alternatively, on the **Custom Templates** page, choose **More > View Application Record** in the **Operation** column.

You can view the name or ID of the DB instance that the parameter template applies to, as well as the application status, application time, and failure cause (if failed).

----End

## 5.8.10 Modifying a Parameter Template Description

### Scenarios


You can modify the description of a parameter template you have created.

#### NOTE




You cannot modify the description of a default parameter template.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

- Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template and click  in the **Description** column.
- Step 5** Enter a new description. You can click  to submit or  to cancel the modification.
- The description consists of a maximum of 256 characters and cannot contain the following special characters: >!<"&'=
  - After the modification is successful, you can view the new description in the **Description** column of the parameter template list.
- End

## 5.8.11 Deleting a Parameter Template

### Scenarios


You can delete a custom parameter template that is no longer in use.

---

#### NOTICE

- Deleted parameter templates cannot be recovered. Exercise caution when performing this operation.
  - Default parameter templates cannot be deleted.
- 

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Parameter Templates** page, click **Custom Templates**. Locate the target parameter template to be deleted and choose **More > Delete** in the **Operation** column.
- Step 5** In the displayed dialog box, click **Yes**.
- End

## 5.9 Connection Management

### 5.9.1 Configuring and Changing a Floating IP Address

#### Scenarios

You can change floating IP addresses after migrating on-premises databases or other cloud databases to RDS.

## Constraints


After a floating IP address is changed, the domain name needs to be resolved again. This operation takes several minutes and may interrupt database connections. Therefore, you are advised to change a floating IP address during off-peak hours.

## Configuring a Floating IP Address

You can use an automatically-assigned IP address when creating a DB instance.

## Changing a Floating IP Address

You can change the floating IP address of an existing DB instance.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the **Connection Information** area on the **Basic Information** page, click **Change** in the **Floating IP Address** field.
- Step 6** In the displayed dialog box, enter a new floating IP address and click **OK**.

An in-use IP address cannot be used as the new floating IP address of the DB instance.

----End

## 5.9.2 Binding and Unbinding an EIP

### Scenarios

By default, a DB instance is not publicly accessible (not bound with an EIP) after being created. You can bind an EIP to a DB instance for public accessibility, and you can unbind the EIP from the DB instance later if needed.

---

#### NOTICE

To ensure that the DB instance is accessible, the security group associated with the instance must allow access over the database port. For example, if the database port is 5432, ensure that the security group allows access over the 5432 port.

---

### Prerequisites

- You have assigned an EIP on the VPC console.
- You can bind an EIP to a primary DB instance or a read replica only.

- If a DB instance has already been bound with an EIP, you must unbind the EIP from the DB instance first before binding a new EIP to it.

## Binding an EIP

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Connection Management**. In the **Connection Information** area on the **Public Connection** page, click **Bind** next to the **EIP** field.

**Step 6** In the displayed dialog box, all unbound EIPs are listed. Select the EIP to be bound and click **OK**. If no available EIPs are displayed, click **View EIP** and obtain an EIP.

**Step 7** On the **Connection Management** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

To unbind the EIP from the DB instance, see [Unbinding an EIP](#).

----End

## Unbinding an EIP

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the DB instance that has an EIP bound.

**Step 5** In the navigation pane on the left, choose **Connection Management**. In the **Connection Information** area on the **Public Connection** page, click **Unbind** next to the **EIP** field. In the displayed dialog box, click **Yes**.

**Step 6** On the **Connection Management** page, view the results.

You can also view the progress or the results of unbinding an EIP from a DB instance on the **Task Center** page.

To bind an EIP to the DB instance again, see [Binding an EIP](#).

----End




## 5.9.3 Changing a Database Port

### Scenarios

This section describes how to change the database port of a primary DB instance or a read replica. For primary/standby DB instances, changing the database port of the primary DB instance will cause the database port of the standby DB instance to also be changed.



If specific security group rules have been configured for a DB instance, you need to change the inbound rules of the security group to which the DB instance belongs after changing the database port.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance or click  first and then click the target read replica.
- Step 5** In the **Connection Information** area on the **Basic Information** page, click  in the **Database Port** field.

#### NOTE

RDS for PostgreSQL instances can use database ports 2100 to 9500.

- To submit the change, click .
  - In the dialog box, click **Yes**.
    - i. If you change the database port of the primary DB instance, that of the standby DB instance will also be changed and both DB instances will be rebooted.
    - ii. If you change the database port of a read replica, the change will not affect other DB instances. Only the read replica will be rebooted.
    - iii. This process takes 1-5 minutes.
  - In the dialog box, click **No** to cancel the modification.
- To cancel the change, click .

- Step 6** View the results on the **Basic Information** page.

----End

## 5.9.4 Connecting to a DB Instance Through pgAdmin

You can use the pgAdmin client to connect to an RDS DB instance.

**NOTICE**

The pgAdmin version must be 4 or later.

## Preparations

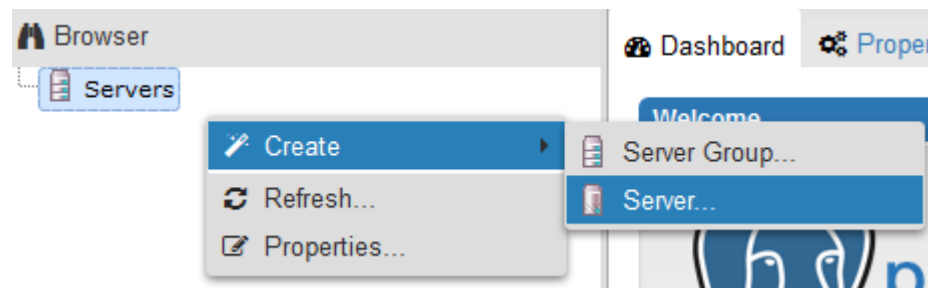
1. Prepare an **ECS** or a device that can access RDS DB instances.  
To connect to a DB instance through a floating IP address, you must:
  - Ensure that the ECS and DB instance must be in the same VPC.
  - Ensure that the ECS must be allowed by the security group to access RDS DB instances.To connect to a DB instance through an EIP, you must:
  - a. Bind the EIP to the DB instance. For details, see [Binding an EIP](#).
  - b. Ensure that the local device can access the EIP that has been bound to the DB instance.
2. Install the pgAdmin client on the prepared ECS or device.

## Procedure

**Step 1** Start pgAdmin.

**Step 2** In the displayed login window, choose **Servers > Create > Server**.

**Figure 5-2** Creation



**Step 3** On the **General** page, specify **Name**. On the **Connection** page, specify information about the DB instance to be connected. Then, click **Save**.

Figure 5-3 General page

The screenshot shows a dialog box titled "Create - Server" with a close button (X) in the top right corner. It has two tabs: "General" (selected) and "Connection". The "General" tab contains the following fields:

- Name**: An empty text input field.
- Server group**: A dropdown menu with "Servers" selected.
- Connect now?**: A checked checkbox.
- Comments**: A large empty text area.

A red error bar at the bottom of the dialog contains the text "Name must be specified.". At the bottom right, there are three buttons: "Save" (blue), "Cancel" (red), and "Reset" (yellow). On the bottom left, there are two small icons: an information icon (i) and a help icon (?).

Figure 5-4 Connection page

The screenshot shows the same "Create - Server" dialog box, but with the "Connection" tab selected. The "General" tab is now greyed out. The "Connection" tab contains the following fields:

- Host name/address**: An empty text input field.
- Port**: A text input field containing "5432".
- Maintenance database**: A text input field containing "postgres".
- User name**: An empty text input field.
- Password**: An empty text input field.
- Save password?**: An unchecked checkbox.
- Role**: An empty text input field.
- SSL mode**: A dropdown menu with "Prefer" selected.

A red error bar at the bottom of the dialog contains the text "Name must be specified.". At the bottom right, there are three buttons: "Save" (blue), "Cancel" (red), and "Reset" (yellow). On the bottom left, there are two small icons: an information icon (i) and a help icon (?).



Parameter description:

- **Host name/address:** indicates the IP address of the DB instance you want to connect to. If you connect to a DB instance through a floating IP address, enter the floating IP address displayed in the **Connection Information** area on the **Basic Information** page of your DB instance. If you connect to a DB instance through an EIP, enter the EIP of your DB instance.
- **Port:** indicates the database port. By default, the value is **5432**.
- **User name:** indicates the username. By default, the value is **root**.
- **Password:** indicates the password of the target database username.

**Step 4** In the login window, check that the connection information is correct. The target DB instance is successfully connected.

----End

## 5.10 Plugin Management

### 5.10.1 Creating or Deleting a Plugin

RDS provides the PostgreSQL plugin management solution for user **root**. Except the following plugins, you need to manually create other plugins by referring to this section.

- auto\_explain
- passwordcheck
- pg\_profile\_pro
- pg\_sql\_history
- plpgsql
- wal2json
- test\_decoding

#### NOTE

The RDS for PostgreSQL plugin takes effect at the database level, not globally. You need to manually create it on corresponding databases.

The latest minor versions of RDS for PostgreSQL 11, 12, and 13 allow the **root** user to create plugins (create extension) or delete plugins (drop extension).

### Creating a Plugin

**Step 1** Connect to the database **database1** as user **root** and use **template1** to create a database that can support the plugin.

```
# psql --host=<RDS_ADDRESS> --port=<DB_PORT> --dbname=database1 --  
username=root -c "create database <DB_NAME> template template1;"
```

- **RDS\_ADDRESS** indicates the IP address of the RDS DB instance.
- **DB\_PORT** indicates the RDS DB instance port.
- **DB\_NAME** indicates the name of the database to be created.

Enter the password of user **root** when prompted.

Create a database named *my\_extension\_db* that can support the plugin. Example:

```
# psql --host=192.168.6.141 --port=5432 --dbname=database1 --
username=root -c "create database my_extension_db template template1;"
```

```
Password for user root:
CREATE DATABASE
```

Note: If you are creating a database as a common user, log in to the created database as the common user and run the following command to grant all rights to user **root**:

```
GRANT ALL ON DATABASE db1 TO root;
```

**Step 2** Connect to the created database as user **root** and create a plugin.

```
# psql --host=<RDS_ADDRESS> --port=<DB_PORT> --dbname=<DB_NAME> --
username=root -c "select control_extension('create',<EXTENSION_NAME>);"
```

- *RDS\_ADDRESS* indicates the IP address of the RDS DB instance.
- *DB\_PORT* indicates the RDS DB instance port.
- *DB\_NAME* indicates the name of the database to be created.
- *EXTENSION\_NAME* indicates the plugin name. For more information, see [Supported Plugins](#).

Enter the password of user **root** when prompted.

Create the postgis plugin in the database *my\_extension\_db*. Example:

```
# psql --host=192.168.6.141 --port=5432 --dbname=my_extension_db --
username=root -c "select control_extension('create','postgis');"
```

```
Password for user root:
control_extension
-----
create postgis successfully.
(1 row)
```

```
----End
```

## Deleting a Plugin

Connect to the database with a plugin created as user **root** and delete the plugin.

```
# psql --host=<RDS_ADDRESS> --port=<DB_PORT> --username=root --
dbname=<DB_NAME> -c "select control_extension
('drop',<EXTENSION_NAME>);"
```

- *RDS\_ADDRESS* indicates the IP address of the RDS DB instance.
- *DB\_PORT* indicates the RDS DB instance port.
- *DB\_NAME* indicates the name of the database to be created.
- *EXTENSION\_NAME* indicates the plugin name. For more information, see [Supported Plugins](#).

Enter the password of user **root** when prompted.

Example:

```
# psql --host=192.168.6.141 --port=5432 --dbname=my_extension_db --
username=root -c "select control_extension('drop','postgis');"

```

```
Password for user root:
control_extension
-----
drop postgis successfully.
(1 row)

```

## 5.10.2 Supported Plugins

### NOTE

The following table lists the plugins supported by the latest minor versions of RDS for PostgreSQL. You can use **SELECT name FROM pg\_available\_extensions;** to view the plugins supported by your DB instance.

The plugins `mysql_fdw`, `dblink`, `pgsql-ogr-fdw`, `postgres_fdw`, and `tds_fdw` are used to access data stored in remote database servers. Before using any of them, ensure that the server IP addresses of the two DB instances are in the same VPC and subnet.

**Table 5-4** Supported plugins

Plugin Name	Postgr eSQL 9.5	Postgr eSQL 9.6	Postgr eSQL 10	Postgr eSQL 11	Postgr eSQL 12	Postgr eSQL 13	Postgr eSQL 14
address_stand ardizer	2.5.1	2.5.1	2.5.1	2.5.1	3.0.0	3.1.0	3.2.1
address_stand ardizer_data_u s	2.5.1	2.5.1	2.5.1	2.5.1	3.0.0	3.1.0	3.2.1
amcheck	-	-	-	1.1	1.2	1.2	1.3
auth_delay	-	-	-	-	2	2	2
auto_explain	2	2	2	2	2	2	2
bloom	-	-	-	1.0	1.0	1.0	1.0
btree_gin	1.0	1.0	1.2	1.3	1.3	1.3	1.3
btree_gist	1.1	1.2	1.5	1.5	1.5	1.5	1.6
citext	1.1	1.3	1.4	1.5	1.6	1.6	1.6
<b>cube</b> For details, see <a href="#">cube</a> .	1.0	1.2	1.2	1.4	1.4	1.4	1.5
dblink	1.1	1.2	1.2	1.2	1.2	1.2	1.2
dict_int	1.0	1.0	1.0	1.0	1.0	1.0	1.0
dict_xsyn	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Plugin Name	PostgreSQL 9.5	PostgreSQL 9.6	PostgreSQL 10	PostgreSQL 11	PostgreSQL 12	PostgreSQL 13	PostgreSQL 14
<b>earthdistance</b> For details, see <a href="#">earthdistance</a> .	1.0	1.1	1.1	1.1	1.1	1.1	1.1
fuzzystrmatch	1.0	1.1	1.1	1.1	1.1	1.1	1.1
hll	2.12	2.12	2.12	2.12	2.14	2.15.1	2.16
hstore	1.3	1.4	1.4	1.5	1.6	1.7	1.8
hypopg	-	-	-	1.2.0	1.2.0	1.2.0	1.3.1
icu	-	-	-	1.0	1.0	1.0	1.0
intagg	1.0	1.1	1.1	1.1	1.1	1.1	1.1
intarray	1.0	1.2	1.2	1.2	1.2	1.3	1.5
isn	1.0	1.1	1.1	1.2	1.2	1.2	1.2
ltree	1.0	1.1	1.1	1.1	1.1	1.2	1.2
mysql_fdw	-	-	-	2.5.5	2.5.5	2.5.5	2.8.0
old_snapshot	-	-	-	-	-	-	1.0
orafce	3.8.0	3.8.0	3.8.0	3.8.0	3.8.0	3.14.0	3.21.1
pageinspect	1.3	1.5	1.6	1.7	1.7	1.8	1.9
passwordcheck	2	2	2	2	2	2	2
Pgaudit	-	-	-	-	1.6.2	1.6.2	1.6.2
pg_bigm	-	-	-	1.2_20200228	1.2_20200228	1.2_20200228	1.2_20200228
pg_buffercache	1.1	1.2	1.3	1.3	1.3	1.3	1.3
pg_cron	-	-	-	-	1.4.1	1.3.1	1.4.1
pg_freespace_map	1.0	1.1	1.2	1.2	1.2	1.2	1.2
pg_hint_plan	1.1.5	1.2.0	1.3.0	1.3.5	1.3.7	1.3.7	1.4.0
pg_jieba	1.1.0	1.1.0	1.1.0	1.1.0	1.1.0	2.0.1	1.1.0
pg_pathman	1.5.8	1.5.8	1.5.8	1.5.8	1.5.12	1.5.12	-
pg_prewarm	1.0	1.1	1.1	1.2	1.2	1.2	1.2

Plugin Name	PostgreSQL 9.5	PostgreSQL 9.6	PostgreSQL 10	PostgreSQL 11	PostgreSQL 12	PostgreSQL 13	PostgreSQL 14
pg_qualstats	-	-	-	2.0.2	2.0.2	2.0.2	2.0.4
pg_repack	1.4.6	1.4.6	1.4.6	1.4.6	1.4.6	1.4.6	1.4.7
pg_roaringbitmap	-	-	-	0.5.2	0.5.2	0.5.2	0.5.4
pg_stat_kcache	-	-	-	2.2.0	2.2.0	2.2.0	2.2.1
pg_stat_statements	1.3	1.4	1.6	1.6	1.7	1.8	1.9
pg_surgery	-	-	-	-	-	-	1.0
pg_track_settings	-	-	-	2.0.1	2.0.1	2.0.1	2.0.1
pg_trgm	1.1	1.3	1.3	1.4	1.4	1.5	1.6
pg_visibility	-	-	-	1.2	1.2	1.2	1.2
pg_wait_sampling	-	-	-	1.1.3	1.1.3	1.1.3	1.1.3
pgcrypto	1.2	1.3	1.3	1.3	1.3	1.3	1.3
pgl_ddl_deploy	-	-	-	-	2.1.0	2.1.0	2.1.0
pglogical	-	-	-	2.4.1	2.4.1	2.4.1	2.4.1
pgrouting	-	-	-	3.1.0	3.1.0	3.1.3	3.3.1
pgrowlocks	1.1	1.2	1.2	1.2	1.2	1.2	1.2
pg_sql_history	1.1	1.1	1.1	1.1	1.1	1.1	1.1
pgsql-ogr-fdw	-	-	-	1.0.12	1.0.12	1.0.12	-
pgstattuple	1.3	1.4	1.5	1.5	1.5	1.5	1.5
pgvector	-	-	-	-	0.4.1	0.4.1	0.4.1
<b>plpgsql</b> For details, see <a href="#">plpgsql</a> .	1.0	1.0	1.0	1.0	1.0	1.0	1
plperl	-	-	-	1.0	1.0	1.0	1.0
plproxy	-	-	-	2.10.0	2.10.0	2.10.0	2.10.0
plv8	-	-	-	2.3.15	2.3.15	2.3.15	-

Plugin Name	PostgreSQL 9.5	PostgreSQL 9.6	PostgreSQL 10	PostgreSQL 11	PostgreSQL 12	PostgreSQL 13	PostgreSQL 14
<b>postgis</b> For details, see <a href="#">postgis</a> .	2.5.1	2.5.1	2.5.1	2.5.1	3.0.0	3.1.0	3.2.1
postgis_raster	Integrated to postgis	Integrated to postgis	Integrated to postgis	Integrated to postgis	3.0.0	3.1.0	3.2.1
postgis_sfcgal	2.5.1	2.5.1	2.5.1	2.5.1	3.0.0	3.1.0	3.2.1
postgis_tiger_geocoder	2.5.1	2.5.1	2.5.1	2.5.1	3.0.0	3.1.0	3.2.1
postgis_topology	2.5.1	2.5.1	2.5.1	2.5.1	3.0.0	3.1.0	3.2.1
postgres_fdw	1.0	1.0	1.0	1.0	1.0	1.0	1.1
postgres-decoderbufs	-	-	-	1.3.1	1.3.1	1.3.1	1.7.0
postgresql_anonymizer	-	-	-	0.7.1	0.7.1	0.7.1	1.0.0
q3c	-	-	-	2.0.0	2.0.0	2.0.0	2.0.0
rum	-	-	-	1.3.7	1.3.7	1.3.7	1.3.9
sslinfo	-	-	-	1.2	1.2	1.2	1.2
tablefunc	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tds_fdw	-	-	2.0.1	2.0.1	2.0.1	2.0.2	2.0.2
test_decoding	2	2	2	2	2	2	2
<b>timescaledb</b> For details, see <a href="#">timescaledb</a> .	0	1.3.2	1.3.2	1.3.2	1.7.0	2.1.0	2.7.0
tsm_system_rows	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_time	1.0	1.0	1.0	1.0	1.0	1.0	1.0
unaccent	1.0	1.1	1.1	1.1	1.1	1.1	1.1
uuid-osp	1.0	1.1	1.1	1.1	1.1	1.1	1.1
<b>wal2json</b> For details, see <a href="#">wal2json</a> .	-	-	-	2.3	2.3	2.3	2.4

Plugin Name	PostgreSQL 9.5	PostgreSQL 9.6	PostgreSQL 10	PostgreSQL 11	PostgreSQL 12	PostgreSQL 13	PostgreSQL 14
xml2	-	-	-	1.1	1.1	1.1	1.1
zhparser	2.2	2.2	2.2	2.2	2.2	2.2	2.2

## Plugin Description

- **postgis**
  - When postgis is created, the following plugins are created at the same time:
    - postgis
    - postgis\_topology
    - fuzzystrmatch
    - postgis\_tiger\_geocoder
    - address\_standardizer
    - address\_standardizer\_data\_us
  - Creating postgis\_topology and postgis\_tiger\_geocoder will change the **search\_path** settings. However, this change will not take effect for established connections. To use the two plugins, re-establish a connection to update the **search\_path** settings.
- **plpgsql**

plpgsql 1.0 provides the SQL procedural language and is installed by default.
- **earthdistance**

To install the earthdistance plugin, you must install the cube plugin first.
- **cube**

If the earthdistance plugin has been installed, deleting the cube plugin will cause the earthdistance plugin to be unavailable.
- **timescaledb**

The timescaledb plugin does not support the TLS protocol. For more information, see [APIs Not Supported by the timescaledb Plugin](#).
- **wal2json**

This plugin is a logical replication plugin. You can directly use it without installing it through control\_extension.

## APIs Not Supported by the timescaledb Plugin

- add\_compress\_chunks\_policy
- add\_drop\_chunks\_policy
- add\_reorder\_policy
- alter\_job\_schedule
- compress\_chunk

- decompress\_chunk
- drop\_chunks
- interpolate
- locf
- move\_chunk
- remove\_compress\_chunks\_policy
- remove\_drop\_chunks\_policy
- remove\_reorder\_policy
- reorder\_chunk
- set\_integer\_now\_func
- time\_bucket\_gapfill

### 5.10.3 Using pg\_repack

#### Scenarios

pg\_repack can reorganize tables and indexes with minimal locks to restore the physical order. Unlike CLUSTER and VACUUM FULL it works online, without holding an exclusive lock on the processed tables during processing.

#### Constraints

- Only the **root** user can use pg\_repack.
- The target table must have a primary key or at least a unique total index on a NOT NULL column.
- Performing a full-table repack requires free disk space about twice as large as the target table and its indexes.
- pg\_repack cannot reorganize temp tables or cluster tables by GiST indexes.
- You will not be able to perform DDL commands of the target table except VACUUM or ANALYZE while pg\_repack is working.
- pg\_repack can be used only after a client is deployed locally. For details, see the official documentation at [https://reorg.github.io/pg\\_repack/](https://reorg.github.io/pg_repack/).

#### How to Use

- Install the plugin.  

```
select control_extension('create', 'pg_repack');
```
- Delete the plugin.  

```
select control_extension('drop', 'pg_repack');
```

#### Example

Use pg\_repack to repack a table.

1. **Create a test table pg\_repack\_test.**  

```
create table pg_repack_test(id bigint primary key, name varchar);
insert into pg_repack_test select i, to_char(random()*100000, 'FM000000') from generate_series(1, 1000000) i;
delete from pg_repack_test where id in (select i from generate_series(1, 600000, 2) i);
select pg_size_pretty(pg_relation_size('pg_repack_test'));
```



2. **Repack the test table.**

```
pg_repack --host=<RDS_ADDRESS> --port=<DB_PORT> --dbname=<DB_NAME> --username=root --no-superuser-check --no-kill-backend -t pg_repack_test
```

- *RDS\_ADDRESS*: IP address of the RDS DB instance.
- *DB\_PORT*: Port of the RDS DB instance.
- *DB\_NAME*: Name of the database where the pg\_repack\_test table is located.

3. **Check the size of the repacked table.**

```
select pg_size_pretty(pg_relation_size('pg_repack_test'));
```

## FAQs

**Table 5-5** Common error information and solutions

Error Information	Solution
ERROR: pg_repack failed with error: ERROR: permission denied for schema repack	Use the <b>root</b> user.
ERROR: pg_repack failed with error: You must be a superuser to use pg_repack	Add <b>--no-superuser-check</b> to skip superuser checks.
NOTICE: Waiting for 1 transactions to finish. First PID: xxxx	Wait until the transaction is complete.

## 5.11 Tablespace Management

### Scenarios

RDS provides the PostgreSQL tablespace management solution based on user **root**.

### Creating a Tablespace

**Step 1** Connect to the database as user **root** and create a tablespace.

```
# psql --host=<RDS_ADDRESS> --port=<DB_PORT> --dbname=<DB_NAME> --username=root -c "select control_tablespace ('create', '<TABLESPACE_NAME>');"
```

**Table 5-6** Parameter description

Parameter	Description
<i>RDS_ADDRESS</i>	Indicates the IP address of the RDS DB instance.
<i>DB_PORT</i>	Indicates the port of the RDS DB instance.

Parameter	Description
<i>DB_NAME</i>	Indicates the database name.
<i>TABLESPACE_NAME</i>	Indicates the tablespace name.

**Step 2** Enter the password of user **root** when prompted.

Log in to the **my\_db** database and create the **tbspc1** tablespace. Example:

```
# psql --host=192.168.6.141 --port=5432 --dbname=my_db --username=root -c
"select control_tablespace('create', 'tbspc1');"
```

```
Password for user root:
control_tablespace
-----
create tablespace tbspc1 successfully.
(1 row)
```

If the creation fails, view error logs of the DB instance.

 **NOTE**

To ensure performance, a maximum of 20 tablespaces can be created.

----End

## Deleting a Tablespace

**Step 1** Connect to a database as user **root** and delete a tablespace.

```
# psql --host=<RDS_ADDRESS> --port=<DB_PORT> --username=root --
dbname=<DB_NAME> -c "select control_tablespace('drop', '<TABLESPACE
_NAME>');"
```

**Table 5-7** Parameter description

Parameter	Description
<i>RDS_ADDRESS</i>	Indicates the IP address of the RDS DB instance.
<i>DB_PORT</i>	Indicates the port of the RDS DB instance.
<i>DB_NAME</i>	Indicates the database name.
<i>TABLESPACE_NAME</i>	Indicates the tablespace name.

**Step 2** Enter the password of user **root** when prompted.

Example:

```
# psql --host=192.168.6.141 --port=8635 --dbname=my_db --username=root -c
"select control_tablespace('drop', 'tbspc1');"
```

```
Password for user root:
control_tablespace
-----
```

```
drop tablespace tbspc1 successfully.  
(1 row)
```

Before deleting the tablespace, ensure that it is empty. If the deletion fails, view error logs of the DB instance.

----End

## 5.12 Data Security

### 5.12.1 Resetting the Administrator Password

#### Scenarios

You can reset the administrator password of a primary instance.

If you forget the password of the administrator account **root**, you can reset the password.

#### NOTE

- If you have changed the administrator password of the primary DB instance, the administrator passwords of the standby DB instance and read replicas (if any) will also be changed.
- The time required for the new password to take effect depends on the amount of service data currently being processed by the primary DB instance.
- To protect against brute force hacking attempts and ensure system security, change your password periodically, such as every three or six months.

#### Method 1

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and choose **More > Reset Password** in the **Operation** column.

**Step 5** Enter and confirm the new password.

---

#### NOTICE

Keep this password secure. The system cannot retrieve it.

---


The new password must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@#%^\*\_-=+?,.). Enter a strong password and periodically change it for security reasons.

- To submit the new password, click **OK**.

- To cancel the reset operation, click **Cancel**.

----End

## Method 2

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target DB instance.
- Step 5** In the **DB Information** area on the **Basic Information** page, click **Reset Password** in the **Administrator** field.
- Step 6** Enter and confirm the new password.

---

### NOTICE

Keep this password secure. The system cannot retrieve it.

---

The new password must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@#%^\*-\_+=?,). Enter a strong password and periodically change it for security reasons.

- To submit the new password, click **OK**.
- To cancel the reset operation, click **Cancel**.


----End


## 5.12.2 Changing a Security Group



### Scenarios


This section describes how to change the security group of a primary DB instance or read replica. For primary/standby DB instances, changing the security group of the primary DB instance will cause the security group of the standby DB instance to be changed as well.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instance Management** page, click the target primary DB instance or read replica.

**Step 5** In the **Connection Information** area on the **Basic Information** page, click  next to the **Security Group** field.

- To submit the change, click .
- To cancel the change, click .

**Step 6** Changing the security group takes 1 to 3 minutes. Click  in the upper right corner on the **Basic Information** page to view the results.

----End

## 5.13 Metrics and Alarms

### 5.13.1 Configuring Displayed Metrics

The RDS Agent monitors RDS DB instances and collects monitoring metrics only.

#### Description

This section describes the metrics that can be monitored by Cloud Eye as well as their namespaces and dimensions. You can use APIs provided by Cloud Eye to query the monitoring metrics and alarms generated for RDS.

#### Namespace

SYS.RDS

#### DB Instance Monitoring Metrics

- [Table 5-8](#) lists the performance metrics of RDS for PostgreSQL DB instances.

**Table 5-8** Performance metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds001_cpu_util	CPU Usage	CPU usage of the monitored object	0-100 %	RDS for PostgreSQL instance	1 minute
rds002_mem_util	Memory Usage	Memory usage of the monitored object	0-100 %	RDS for PostgreSQL instance	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
read_count_per_second	Read IOPS	Average number of read I/O requests processed by the system in a specified period	counts	RDS for PostgreSQL instance	1 minute
write_count_per_second	Write IOPS	Average number of write I/O requests processed by the system in a specified period	counts	RDS for PostgreSQL instance	1 minute
rds004_bytes_in	Network Input Throughput	Incoming traffic in bytes per second	≥ 0 bytes/s	RDS for PostgreSQL instance	1 minute
rds005_bytes_out	Network Output Throughput	Outgoing traffic in bytes per second	≥ 0 bytes/s	RDS for PostgreSQL instance	1 minute
rds039_disk_util	Storage Space Usage	Storage space usage of the monitored object	0-100 %	RDS for PostgreSQL instance	1 minute
rds040_transaction_logs_usage	Transaction Logs Usage	Storage space usage of transaction logs	≥ 0 MB	RDS for PostgreSQL instance	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds041_replication_slot_usage	Replication Slot Usage	Storage space usage of replication slot files	≥ 0 MB	RDS for PostgreSQL instance	1 minute
rds042_database_connections	Database Connections in Use	Number of database connections in use	≥ 0 counts	RDS for PostgreSQL instance	1 minute
rds043_maximum_used_transaction_ids	Maximum Used Transaction IDs	Maximum number of transaction IDs that have been used	≥ 0 counts	RDS for PostgreSQL instance	1 minute
rds044_transaction_logs_generations	Transaction Logs Generation	Size of transaction logs generated per second	≥ 0 MB/s	RDS for PostgreSQL instance	1 minute
rds045_oldest_replication_slot_lag	Oldest Replication Slot Lag	Lagging size of the most lagging replica in terms of WAL data received	≥ 0 MB	RDS for PostgreSQL instance	1 minute
rds046_replication_lag	Replication Lag	Replication lag	≥ 0 ms	RDS for PostgreSQL instance	1 minute
rds047_disk_total_size	Total Storage Space	Total storage space of the monitored object	40–4,000 GB	RDS for PostgreSQL instance	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
rds048_disk_used_size	Used Storage Space	Used storage space of the monitored object	0–4,000 GB	RDS for PostgreSQL instance	1 minute
rds049_disk_read_throughput	Disk Read Throughput	Number of bytes read from the disk per second	≥ 0 bytes/s	RDS for PostgreSQL instance	1 minute
rds050_disk_write_throughput	Disk Write Throughput	Number of bytes written into the disk per second	≥ 0 bytes/s	RDS for PostgreSQL instance	1 minute

## Dimension

Key	Value
postgresql_instance_id	RDS for PostgreSQL DB instance ID

## 5.13.2 Setting Alarm Rules

### Scenarios

You can set alarm rules to customize the monitored objects and notification policies and keep track of the RDS running status.

The RDS alarm rules include alarm rule names, services, dimensions, monitored objects, metrics, alarm thresholds, monitoring period, and whether to send notifications.

### Setting Alarm Rules

**Step 1** Log in to the management console.

**Step 2** Under **Management & Governance**, click **Cloud Eye**.



**Step 3** In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.

**Step 4** On the displayed **Alarm Rules** page, click **Create Alarm Rule**.

----End

## 5.13.3 Viewing Monitoring Metrics

### Scenarios

Cloud Eye monitors the statuses of RDS DB instances. You can view RDS monitoring metrics on the management console.

Monitored data takes some time before it can be displayed. The RDS status displayed on the Cloud Eye console is about 5 to 10 minutes delayed. When you create a new RDS DB instance, it takes 5 to 10 minutes before monitoring data is displayed on Cloud Eye.

### Prerequisites

- RDS is running properly.  
Monitoring metrics of the RDS DB instances that are faulty or have been deleted are not displayed on the Cloud Eye console. You can view their monitoring metrics after they are rebooted or restored to normal.

#### NOTE

If an RDS DB instance has been faulty for 24 hours, Cloud Eye considers it to no longer exist and deletes it from the monitoring object list. You need to manually clear the alarm rules created for the DB instance.

- RDS has been running properly for about 10 minutes.  
For a newly created RDS DB instance, you need to wait a bit before you can view the metrics.

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, locate the target DB instance and click **View Metric** in the **Operation** column to go to the Cloud Eye console.

Alternatively, click the target DB instance. On the displayed page, click **View Metric** in the upper right corner of the page to go to the Cloud Eye console.

**Step 5** On the Cloud Eye console, view monitoring metrics of the DB instance.

Cloud Eye can monitor performance metrics from the last 1 hour, 3 hours, 12 hours, 1 day, 30 days, and 7 days.

----End

## 5.14 Log Management


### 5.14.1 Viewing Error Logs

#### Scenarios

Error logs contain logs generated during the database running. These can help you analyze problems with the database.

#### Viewing Log Details

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.


**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Logs**. On the **Error Logs** page, click **Log Details** to view details about error logs.

- You can select a log level in the upper right corner of the log list.

#### NOTE

For RDS for PostgreSQL DB instances, the following levels of logs are displayed:

- ERROR
  - FATAL
  - PANIC
- You can click  in the upper right corner to view error logs generated in different time segments.
  - If the description of a log is truncated, locate the log and move your pointer over the description in the **Description** column to view details.

----End

#### Download a Log

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Logs**. On the **Error Logs** page, click **Download**. In the log list, locate a log whose status is **Preparation completed** and click **Download** in the **Operation** column.

- The system automatically loads the downloading preparation tasks. The loading duration is determined by the log file size and network environment.
  - When the log is being prepared for download, the log status is **Preparing**.
  - When the log is ready for download, the log status is **Preparation completed**.
  - If the preparation for download fails, the log status is **Abnormal**.

Logs in the **Preparing** or **Abnormal** status cannot be downloaded.

- If the size of a log to be downloaded is greater than 40 MB, you need to use OBS Browser+ to download it. For details, see [Method 1: Using OBS Browser+](#).
- The download link is valid for 5 minutes. After the download link expires, a message is displayed indicating that the download link has expired. If you need to download the log, click **OK**.

----End

## 5.14.2 Viewing Slow Query Logs

### Scenarios

Slow query logs record statements that exceed the **log\_min\_duration\_statement** value. You can view log details to identify statements that are slowly executed and optimize the statements.

RDS supports the following statement types:

- SELECT
- INSERT
- UPDATE
- DELETE
- CREATE
- DROP
- ALTER
- DO
- CALL
- COPY

### Parameter Description

**Table 5-9** Parameters related to RDS for PostgreSQL slow queries

Parameter	Description
log_min_duration_statement	Specifies how many milliseconds a query has to run before it has to be logged.

Parameter	Description
log_statement	Specifies the statement type. The value can be <b>none</b> , <b>ddl</b> , <b>mod</b> , or <b>all</b> . The default value is <b>none</b> . If you change the value to <b>all</b> , the database log format changes and slow query logs fail to be parsed.

## Viewing Log Details

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.


**Step 5** In the navigation pane on the left, choose **Logs**. On the **Slow Query Logs** page, click **Log Details** to view details about slow query logs.

- You can view the slow query log records of a specified execution statement type or a specific time period.
- The **log\_min\_duration\_statement** parameter determines when a slow query log is recorded. However, changes to this parameter do not affect already recorded logs. If **log\_min\_duration\_statement** is changed from 1,000 ms to 100 ms, none of the previously recorded logs that do not meet the new threshold are deleted. For example, a 1,500 ms SQL statement that was recorded when the threshold was 1,000 ms will not be deleted now that the new threshold is 2,000 ms.

----End

## Downloading a Log

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instance Management** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Logs**. On the **Slow Query Logs** page, click **Download**. In the log list, locate a log whose status is **Preparation completed** and click **Download** in the **Operation** column.

- The system automatically loads the downloading preparation tasks. The loading duration is determined by the log file size and network environment.
  - When the log is being prepared for download, the log status is **Preparing**.

- When the log is ready for download, the log status is **Preparation completed**.
- If the preparation for download fails, the log status is **Abnormal**.

Logs in the **Preparing** or **Abnormal** status cannot be downloaded.

- The download link is valid for 5 minutes. After the download link expires, a message is displayed indicating that the download link has expired. If you need to download the log, click **OK**.

----End

## 5.15 Task Center

### 5.15.1 Viewing a Task

You can view the detailed progress and result of the task on the **Task Center** page.

#### NOTE

You can view and manage the following tasks:

- Creating DB instances
- Creating read replicas
- Changing single DB instances to primary/standby
- Scaling up storage space
- Binding EIPs to DB instances
- Unbinding EIPs from DB instances
- Switching primary/standby DB instances
- Rebooting DB instances
- Restoring data to new DB instances
- Migrating a standby DB instance to another AZ

### Procedure

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Task Center** page, locate the target task and view its details.

----End

### 5.15.2 Deleting a Task Record

You can delete task records so that they are no longer displayed in the task list. This operation only deletes the task records, and does not delete the DB instances or terminate the tasks that are being executed.


---

**NOTICE**

Deleted task records cannot be recovered. Exercise caution when performing this operation.

---

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** Choose **Task Center** in the navigation pane on the left. On the displayed page, locate the target task record to be deleted and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

You can delete the records of instant tasks in any of the following statuses:

- Completed
- Failed

----End

# 6 FAQs

---

## 6.1 Product Consulting

### 6.1.1 What Should I Pay Attention to When Using RDS?

1. DB instance operating systems (OSs) are invisible to you. Your applications can access a database only through an IP address and a port.
2. The backup files stored in Object Storage Service (OBS) and the Elastic Cloud Server (ECS) used by RDS are invisible to you. They are visible only to the RDS instance management system.
3. Before viewing the DB instance list, ensure that the region is the same as the region where the DB instance is purchased.
4. After creating RDS DB instances, you do not need to perform basic O&M operations, such as enabling HA and installing security patches. However, you must pay attention to:
  - a. Whether the CPU, input/output operations per second (IOPS), and space of the RDS DB instance are sufficient. If any of these becomes insufficient, change the CPU/Memory or scale up the DB instance.
  - b. Whether the performance of the RDS DB instances is adequate, a large number of slow query SQL statements exist, SQL statements need to be optimized, or any indexes are redundant or missing.

### 6.1.2 What Is the Availability of RDS DB Instances?

Calculation formula for RDS DB instance availability:

DB instance availability =  $(1 - \text{Failure duration} / \text{Total service duration}) \times 100\%$

### 6.1.3 Does RDS Support Cross-AZ High Availability?

Yes. When you create a DB instance, you can select **Primary/Standby** for **DB Instance Type** and then select different AZs for **Primary AZ** and **Standby AZ**.

 NOTE

RDS does not support 3-AZ deployment.

An AZ is a physical region where resources have independent power supplies and networks. AZs are physically isolated but interconnected through an internal network.

RDS allows you to deploy primary/standby DB instances in an AZ or across AZs. You can determine whether the standby AZ is the same as the primary AZ.

- If they are different (default setting), the primary and standby instances are deployed in different AZs to ensure failover support and high availability.
- If they are the same, the primary and standby instances are deployed in the same AZ. If an AZ failure occurs, high availability cannot be ensured.

## 6.1.4 What Can I Do About Slow Responses of Websites When They Use RDS?

To solve this problem:

- Check the performance of RDS DB instances on the RDS console.
- Compare the database connection statuses of local databases and RDS DB instances. This problem depends on web applications.

## 6.1.5 Can I Change the Replication Mode Between Primary DB Instances and Read Replicas?

- For the MySQL engine:  
The replication mode displayed on the RDS console indicates the data synchronization method between primary and standby DB instances. Semi-synchronous and asynchronous are both supported. The semi-synchronous mode is more secure but the asynchronous mode improves performance.  
The default synchronization between primary DB instances and read replicas is asynchronous and cannot be changed.

## 6.1.6 What Is the Time Delay for Primary/Standby Replication?

When standby instances cannot keep up with the updates on the primary, this generates replication delay. If the standby SQL and I/O thread are running, the replication delay is a positive value measured in seconds. If the standby SQL thread is not running, or if the SQL thread has consumed all of the relay log and the standby I/O thread is running, then it is **NULL** (undefined or unknown)

The delay for primary/standby replication cannot be calculated using a formula as the delay is affected by the following factors:

- Network communication status
- Transaction workload on the primary DB instance in transactions per second (TPS)
- The size of the transaction executed by the primary DB instance (this affects the duration of transaction executions)



- Load balancing of the standby DB instance and read replicas

If the primary DB instance has a heavy load for a certain period of time and executes a large number of transactions per second, replication to the standby DB instance will be delayed. This delay is generally a few seconds.

- RDS for MySQL: Click the DB instance name on the **Instances** page. The replication source is the primary DB instance. When the replication status is normal, view **Real-Time Replication Delay** to obtain the value of the primary/standby replication delay.
- RDS for PostgreSQL: To check data consistency between the primary and standby DB instances, view **Replication Lag** on the Cloud Eye console to obtain the value of the primary/standby replication delay.

### 6.1.7 What Are the Restrictions on MySQL DB Instances After GTID Is Enabled?

By default, GTID is enabled on MySQL and cannot be disabled because functions such as the primary/standby relationship establishment depend on GTID. If GTID is disabled, all RDS functions (such as backup and restoration and primary/standby switchover or failover) will be affected or even become unavailable.

After GTID is enabled for MySQL community edition, an error will be reported in the following conditions:

- Create tables (create table...select).
- A transaction is processed by the engine (InnoDB) that supports transactions and the engine (MyISAM) that does not support transactions at the same time.
- Create temporary tables (create temporary table).

RDS for MySQL resolved these issues by optimizing the kernel.

### 6.1.8 How Many Databases Can Run on an RDS DB Instance?

The maximum number of databases that can run on an RDS DB instance depends on the DB engine settings.

If there are enough CPU, memory, and storage resources, there are no limitations to the number of databases running on a DB instance. However, the number of tables in the databases affects the backup speed. If there are more than 500,000 tables, the backup will fail.

- RDS for MySQL allows you to create numerous databases and tables. For details, see the official MySQL documentation.
- RDS for PostgreSQL allows you to create numerous databases and database accounts.

### 6.1.9 What Is the Maximum Size Allowed for a Single Table in MySQL Instances?

The maximum size allowed for a single table depends on the maximum file size allowed by the OS.

Due to metadata overhead, the maximum size allowed for a single table is 2 TB.

## 6.2 Resource and Disk Management

### 6.2.1 How Long Does It Take to Create a DB Instance?

- RDS for MySQL and RDS for PostgreSQL instances:  
Generally, creating a DB instance (single or primary/standby) takes 5 to 7 minutes. The time required for creating a read replica depends on the data amount of the primary instance. More data will take longer to replicate. If the primary instance is empty, creating a read replica takes 7 to 8 minutes.

### 6.2.2 Which Types of Logs and Files Occupy RDS Storage Space?

The following logs and files occupy RDS storage space.

**Table 6-1** MySQL database file types

DB Engine	File Type
MySQL	Log files: database undo-log, redo-log, and binlog files
	Data files: database content files and index files
	Other files: ibdata, ib_logfile0, and temporary files

**Table 6-2** PostgreSQL database file types

DB Engine	File Type
PostgreSQL	Log files: database error log and transaction log files
	Data files: database content, index, replication slot data, transaction status data, and database configuration files
	Other files: temporary files

### Solution

1. If the original storage space is insufficient as your services grow, scale up storage space of your DB instance.
2. If data occupies too much storage space, run **DROP**, **TRUNCATE**, or **DELETE +OPTIMIZE TABLE** to delete useless historical table data to release storage space. If no historical data can be deleted, scale up your storage space.
3. If temporary files generated by sorting queries occupy too much storage space, optimize your SQL query statements.

- a. A large number of temporary files are generated if there are a large number of sorting queries executed by applications.
  - b. A large number of binlog files are generated and occupy space if there are large amounts of insert, delete, and update operations in a short period.
  - c. A large number of binlog files are generated if there are a large number of transactions and write operations.
4. Use Cloud Eye to monitor the size, usage, and utilization of storage space of your DB instance and set alarm policies.

## 6.2.3 Which Items Occupy the Storage Space of My RDS DB Instances?

Both your regular data (backup data not included) and the data required for the operation of your DB instances (such as system database data, rollback logs, redo logs, and indexes) take up storage space on your RDS DB instances. The storage space includes the file system overhead required for inode, reserved blocks, and database operations. The following RDS log files also occupy storage space:

- Binlog files generated by RDS for MySQL databases
- Logs files generated by RDS for PostgreSQL database servers

These files ensure the stability of RDS DB instances.

## 6.2.4 How Much Storage Space Is Required for DDL Operations?

Data Definition Language (DDL) operations may increase storage usage sharply. To ensure that services are running properly, do not perform DDL operations during peak hours.

If DDL operations are required, ensure that storage space is at least twice the tablespace size plus 10 GB.

For example, if your tablespace is 500 GB, ensure that storage space is at least 1,010 GB (500 GB x 2 + 10 GB).

## 6.3 Database Connection

### 6.3.1 What Should I Do If I Can't Connect to My RDS DB Instance?

#### Possible Causes

Try the following:

1. [Check whether the DB instance is available.](#)

For example, the system is faulty, the DB instance is abnormal, or the DB instance or a table is locked.

2. **(Common) Check whether the client connection is correct.**
  - If you connect to a DB instance over a private network, ensure that the DB instance and ECS are in the same region and VPC.
  - If you connect to a DB instance over a public network, bind an EIP to the DB instance and then connect to the DB instance through the EIP.
3. **Check the connection method.**

Run either of the following example commands to enable or disable SSL:

  - SSL enabled: `mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem`
  - SSL disabled: `mysql -h 172.16.0.31 -P 3306 -u root -p`
4. **Check whether the parameters in the connection command are correct.**

For example, check whether the following parameters are configured correctly: connection address, port number, username, password, and connection method.
5. **(Common) Check whether the network connectivity is normal**

For a private network connection:

  - a. Check whether the ECS and DB instance are in the same region and VPC.
  - b. Check security group rules.

To access DB instances in a different security group from the ECS, **add an inbound rule** for the security group.
  - c. On the ECS, check whether the DB instance port can be connected to.

For a public network connection:

  - a. Check security group rules.

To access DB instances in a security group from a public network, **add an inbound rule** for the security group.
  - b. Check network ACL rules.
  - c. Ping the ECSs in the same region to the DB instance.
6. **(Common) Check whether the number of connections to the DB instance reaches the upper limit.**

If there is an excessive number of database connections, applications may be unable to connect.
7. **(Common) Check whether the DB instance is in the Storage full state.**

If the DB instance is in the **Storage full** state, data read and write performance is affected.

## Fault Locating

1. **Check whether the DB instance is available.**

Check whether the DB instance is in the **Available** state.

**Possible cause:** The RDS system is faulty, the DB instance is abnormal, or the DB instance or a table is locked.

**Solution:** If the DB instance is abnormal, reboot it.
2. **Check whether the client connection is correct.**

Install an **engine client** whose version is at least as new as the DB instance version.

For details about how to connect to a DB instance over a private or public network, see [Can an External Server Access the RDS Database?](#)

**Table 6-3** Connection model

Connecti on method	Scenario	Example
Private network	A private IP address is provided by default. If your applications are deployed on an ECS that is in the same region and VPC as the DB instance, connect to the ECS and DB instance through a private IP address.	RDS for MySQL: <b>mysql -h &lt;private IP address&gt; -P 3306 -u root -p --ssl-ca=/tmp/ca.pem</b>
Public network	If you cannot access the DB instance using a private IP address, bind an EIP to the DB instance and then connect to the DB instance through the EIP.	RDS for MySQL: <b>mysql -h &lt;EIP&gt; -P 3306 -u root -p --ssl-ca=/tmp/ca.pem</b>

3. **Check the connection method.**

- SSL connection is recommended. Enable SSL on the **Connectivity & Security** page and upload the certificate to the ECS.

**mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem**

- Common connection: Disable SSL on the **Basic Information** page.

**mysql -h 172.16.0.31 -P 3306 -u root -p**

4. **Check the parameters in the command used to connect.**

Ensure that the connection address, port, username and password, and SSL connection method are correct, and try to connect to the DB instance again.

If you use a private connection with SSL enabled, run **mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem**.

- IP address

On the **Private Connection** tab of the **Connectivity & Security** page, obtain the floating IP address in the **Connection Information** area.

- Database Port

On the **Private Connection** tab of the **Connectivity & Security** page, obtain the database port in the **Connection Information** area.

- Root login credentials

Make sure you have entered the root password correctly.

- Certificate

Obtain the SSL certificate name from the directory where the command is executed.

If you use a public connection with SSL enabled, run the following example command: `mysql -h EIP -P 3306 -u root -p --ssl-ca=/tmp/ca.pem`

- IP address  
On the **Public Connection** tab of the **Connectivity & Security** page, obtain the EIP in the **Connection Information** area.
- Database Port  
On the **Public Connection** tab of the **Connectivity & Security** page, obtain the database port in the **Connection Information** area.
- Root login credentials  
Make sure you have entered the root password correctly.
- Certificate  
Obtain the SSL certificate name from the directory where the command is executed.

5. **Check the network connection.**

**Private network connection**

- a. Check whether the ECS and DB instance are in the same region and VPC.
- b. Check security group rules.
- c. On the ECS, check whether the DB instance port can be connected to.  
`telnet <IP address> <port number>`

**Public network connection**

- a. Check security group rules.
- b. Ping the DB instance on an ECS in the same region.  
If you cannot ping the RDS instance's EIP from an ECS, try pinging it from another ECS in the same region.

6. **Check whether there are too many connections to the DB instance.**

**Check method:**

- a. Run `show variables like '%max%connections%';` to view the number of instance connections.

```
mysql> show variables like '%max%connections%';
+-----+-----+
| Variable_name      | Value |
+-----+-----+
| extra_max_connections | 20    |
| max_connections    | 2500  |
| max_user_connections | 100000 |
+-----+-----+
3 rows in set (0.00 sec)
```

- **max\_connections:** the maximum number of clients that can be connected at the same time. If this parameter is set to **default**, the maximum number of clients depends on the amount of memory configured. For details, see [What Is the Maximum Number of Connections to an RDS DB Instance?](#)
- **max\_user\_connections:** the maximum number of concurrent connections allowed for a specific RDS for MySQL account.

- b. Check whether the total connections and current active connections have reached the upper limits by referring to [Viewing Monitoring Metrics](#). Determine whether to release the connections.

**Possible cause:** If there are too many database connections, applications may be unable to connect, and full and incremental backups may fail, affecting services.

**Solution:**

- a. Check whether applications are connected, optimize the connections, and release unnecessary connections.
  - b. If this parameter is set to **default**, you can scale up the DB instance to set **max\_connections** to a larger value. For details, see [Changing a DB Instance Class](#).
  - c. Check whether any metrics are abnormal and whether any alarms are generated on the Cloud Eye console. Cloud Eye monitors database metrics, such as the CPU usage, memory usage, storage space usage, and database connections, and allows you to set alarm policies to identify risks in advance if any alarms are generated. For details about the supported monitoring metrics, see [Configuring Displayed Metrics](#).
7. **Check whether the DB instance is in the Storage full state.**

**Check method:** View the storage space usage on the RDS console or Cloud Eye.

- On the RDS console  
Locate a DB instance and click its name to go to the **Basic Information** page. In the **Storage Space** area, view the storage space usage.
- On Cloud Eye  
Locate a DB instance and click **View Metric** in the **Operation** column. On the displayed page, view the storage space usage.

## 6.3.2 Can an External Server Access the RDS Database?

### DB Instance Bound with an EIP

For a DB instance that has an EIP bound, you can access it through the EIP.

### DB Instance Not Bound with an EIP

- Enable a VPN in a VPC and use the VPN to connect to the RDS DB instance.
- Create an RDS and an ECS in the same VPC and access RDS through the ECS.

## 6.3.3 What Do I Do If the Number of RDS Database Connections Reaches the Upper Limit?

The number of database connections indicates the number of applications that can be simultaneously connected to a database, and is irrelevant to the maximum number of users allowed by your applications or websites.

If there is an excessive number of database connections, applications may fail to be connected, and the full and incremental backups may fail, affecting services.

## Fault Locating

1. Check whether applications are connected, optimize the connections, and release unnecessary connections.
2. Check the specifications and scale them up if needed.
3. On the Cloud Eye console, view metrics of your DB instance to identify performance issues and set alarms for metric thresholds. Cloud Eye monitors metrics of different categories, including CPU, memory, storage, and connections. For details, see the *Cloud Eye User Guide*.

### 6.3.4 What Is the Maximum Number of Connections to an RDS DB Instance?

RDS does not have constraints on how many connections are supported. It depends on the default values and value ranges of the following parameters: **max\_connections** and **max\_user\_connections** for the MySQL DB engine and **max\_connections** for the PostgreSQL DB engine. You can customize these parameters in a parameter template.

#### Changing the Maximum Number of Connections

- RDS for MySQL
 

Or, you can query or change the maximum number of connections allowed using commands.

  - a. Querying the maximum number of connections
 

```
show global variables like 'max_connections';
```
  - b. Changing the value of **max\_connections** under **mysqld** in the **my.cnf** file
 

```
[mysqld]
max_connections = 1000
```
- RDS for PostgreSQL
 

You can query the maximum number of connections allowed using commands.

```
show max_connections;
```

#### Setting the Maximum Number of Connections to an Appropriate Value

- RDS for MySQL
  - In addition to the value of **max\_connections**, the maximum number of concurrent client connections allowed by RDS for MySQL is also limited by the maximum number of files that can be opened by a single process in the operating system. For example, if the maximum number of files that can be opened by each process is set to **100** in the operating system, the **max\_connections** parameter does not take effect even if it is set to **200**.
  - Check the maximum number of files that can be opened by a single process in the operating system. The default value is **1024**.
 

```
ulimit -n
```
  - Check the value of **open\_files\_limit**. **open\_files\_limit** indicates the maximum number of files that can be opened by a single process, which is read from the operating system during RDS for MySQL startup.
 

```
show variables like 'open_files_limit';
```



– Suggestions

The maximum number of RDS for MySQL connections can be modified to any amount allowed by your instance specifications. The maximum number of connections supported is closely related to the instance memory.

**max\_connections**: maximum number of concurrent connections to a DB instance. If this parameter is set to **default**, the maximum number of connections depends on the memory (unit: GB) of the DB instance. The formula is as follows:

**Estimated value of max\_connections = Available node memory / Estimated memory occupied by a single connection**

 NOTE

- Available node memory = Total memory – Memory occupied by the buffer pool – 1 GB (mysqld process/OS/monitoring program)
- Estimated memory usage of a single connection (single\_thread\_memory) = thread\_stack (256 KB) + binlog\_cache\_size (32 KB) + join\_buffer\_size (256 KB) + sort\_buffer\_size (256 KB) + read\_buffer\_size (128 KB) + read\_rnd\_buffer\_size (256 KB) ≈ 1 MB

The following table lists the default values of **max\_connections** for different memory specifications.

**Table 6-4** Max\_connections for different memory specifications

Memory (GB)	Connections
512	100,000
384	80,000
256	60,000
128	30,000
64	18,000
32	10,000
16	5,000
8	2,500
4	1,500
2	800

Set the maximum number of connections to an appropriate value because more connections consume more system resources.

- RDS for PostgreSQL  
Set **max\_connections** based on the complexity of your workloads.

## 6.3.5 How Can I Create and Connect to an ECS?

1. For details about how to create an ECS, see *Elastic Cloud Server User Guide*.
  - If you connect to an RDS DB instance through a private network, ensure that the ECS and DB instance are in the same VPC. If you connect to an RDS DB instance through a public network, the ECS and DB instance can be in different VPCs.
  - Configure a security group to allow the ECS to access the RDS DB instance through the IP address.
2. For details about how to connect to an ECS, see "Logging In to an ECS" in *Elastic Cloud Server User Guide*.

## 6.3.6 What Should I Do If an ECS Cannot Connect to an RDS DB Instance Through a Private Network?

Perform the following steps to identify the problem:

**Step 1** Check whether the ECS and RDS DB instances are located in the same VPC.

- If they are in the same VPC, go to [Step 2](#).
- If they are in different VPCs, create an ECS in the VPC in which the RDS DB instance is located.

**Step 2** Check whether the security group rules of the ECS instance are appropriate.

For MySQL DB instances, see the security group description in [Step 1: Create a DB Instance](#). Then, go to [Step 3](#).

For PostgreSQL DB instances, see the security group description in [Step 1: Create a DB Instance](#). Then, go to [Step 3](#).

**Step 3** On the ECS, check whether the RDS DB instance port can be connected.

The default port of RDS for MySQL is **3306**.

The default port of RDS for PostgreSQL is **5432**.

```
telnet <IP address> {port number}
```

- If the ECS can connect to the RDS DB instance port, the network between the ECS and the RDS DB instance is normal and no further action is required.
- If the ECS still cannot connect to the port, contact technical support.

----End

## 6.3.7 What Should I Do If a Database Client Problem Causes a Connection Failure?

Troubleshoot RDS connection failures caused by a client problem by checking the following items:

1. ECS Security Policy

In Windows, check whether the RDS instance port is enabled in the Windows security policy. In Linux, run **iptables** to check whether the RDS instance port is enabled in firewall settings.

2. Application Configuration  
Check whether the connection address, port parameter configuration, and JDBC connection parameter configuration are correct.
3. Username or Password  
Check whether the username or password is correct if an error similar to the following occurs during RDS DB connection:
  - [Warning] Access denied for user 'username'@'yourIp' (using password: NO)
  - [Warning] Access denied for user 'username'@'yourIp' (using password: YES)

 NOTE

If the problem persists, contact post-sales technical support.

### 6.3.8 What Should I Do If an RDS Database Problem Causes a Connection Failure?

Check whether any of the following problems occurred on the RDS DB instance.

1. The RDS DB instance is not properly connected.  
**Solution:** Check the connection. If you connect to the RDS DB instance through a private network, the ECS and DB instance must be in the same VPC and the DB instance can be accessed only through an ECS in the same VPC. If you connect to the RDS DB instance through a public network, the ECS and DB instance can be in different VPCs.
2. The maximum number of connections has been reached.  
**Solution:** Use RDS resource monitoring to check if the CPU usage and the number of current connections are abnormal. If either of them has reached the maximum, reboot, disconnect, or scale up the class of the RDS DB instance.
3. The DB instance is abnormal. For example, the RDS DB instance fails to be rebooted, the system is faulty, or the instance or table is locked.  
**Solution:** Reboot the RDS DB instance to see if the problem is resolved. If the problem persists, contact post-sales technical support.

### 6.3.9 Do Applications Need to Support Reconnecting to the RDS DB Instance Automatically?

It is recommended that your applications support automatic reconnections to the database. After a database reboot, your applications will automatically reconnect to the database to increase service availability and continuity.

To reduce resource consumption and improve performance, configure your applications to connect to the database using a persistent connection.

## 6.3.10 How Can I Connect to an RDS for PostgreSQL Database Through JDBC?

Although the SSL certificate is optional if you choose to connect to a database through Java database connectivity (JDBC), download an SSL certificate to encrypt the connections for security.

### Prerequisites

Familiarize yourself with:

- Computer basics.
- Java programming language.
- JDBC knowledge.


### Obtaining and Using JDBC

- JDBC driver download address: <https://jdbc.postgresql.org/download/>
- JDBC API: <https://jdbc.postgresql.org/documentation/>

### Connection with the SSL Certificate

#### NOTE

Download the SSL certificate and verify the certificate before connecting to databases.

In the **DB Information** area on the **Basic Information** page, click  in the **SSL** field to download the root certificate or certificate bundle.

**Step 1** Connect to the RDS for PostgreSQL DB instance through JDBC.

```
jdbc:postgresql://<instance_ip>:<instance_port>/<database_name>?sslmode=verify-  
full&sslrootcert=<ca.pem>
```

**Table 6-5** Parameter description

Parameter	Description
<instance_ip>	If you attempt to access the RDS DB instance through an ECS, set <i>instance_ip</i> to the floating IP address displayed on the <b>Basic Information</b> page of the DB instance to which you intend to connect.  If you attempt to access the RDS DB instance through an EIP, set <i>instance_ip</i> to the EIP that has been bound to the DB instance.
<instance_port>	Enter the database port displayed on the <b>Basic Information</b> page. Default value: <b>5432</b>
<database_name>	Enter the name of the database to which you intend to connect. Default value: <b>postgres</b>
sslmode	Enter the SSL connection mode. Default value: <b>verify-full</b>

Parameter	Description
sslrootcert	Enter the directory of the CA certificate for the SSL connection. The certificate should be stored in the directory where the command is executed.

Example script in Java:

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.Statement;

public class MyConnTest {
    final public static void main(String[] args) {
        Connection conn = null;
        // set sslmode here.
        // with ssl certificate and path.
        String url = "jdbc:postgresql://192.168.0.225:5432/my_db_test?sslmode=verify-
full&sslrootcert=/home/Ruby/ca.pem";

        try {
            Class.forName("org.postgresql.Driver");
            conn = DriverManager.getConnection(url, "root", "password");
            System.out.println("Database connected");

            Statement stmt = conn.createStatement();
            ResultSet rs = stmt.executeQuery("SELECT * FROM mytable WHERE columnfoo = 500");
            while (rs.next()) {
                System.out.println(rs.getString(1));
            }

            rs.close();
            stmt.close();
            conn.close();
        } catch (Exception e) {
            e.printStackTrace();
            System.out.println("Test failed");
        } finally {
            // release resource ....
        }
    }
}
```

----End

## Connection Without the SSL Certificate

### NOTE

You do not need to download the SSL certificate because the certificate verification on the server is not required.

**Step 1** Connect to the RDS for PostgreSQL DB instance through JDBC.

```
jdbc:postgresql://<instance_ip>:<instance_port>|<database_name>?sslmode=disable
```

**Table 6-6** Parameter description

Parameter	Description
<instance_ip>	If you attempt to access the RDS DB instance through an ECS, set <i>instance_ip</i> to the floating IP address displayed on the <b>Basic Information</b> page of the DB instance to which you intend to connect.
	If you attempt to access the RDS DB instance through an EIP, set <i>instance_ip</i> to the EIP that has been bound to the DB instance.
<instance_port>	Enter the database port displayed on the <b>Basic Information</b> page. Default value: <b>5432</b>
<database_name >	Enter the name of the database to which you intend to connect. Default value: <b>postgres</b>
sslmode	Enter the SSL connection mode. <b>disable</b> means data is not encrypted.

Example script in Java:

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.Statement;

public class MyConnTest {
    final public static void main(String[] args) {
        Connection conn = null;
        // set sslmode here.
        // no ssl certificate, so do not specify path.
        String url = "jdbc:postgresql://192.168.0.225:5432/my_db_test?sslmode=disable";
        try {
            Class.forName("org.postgresql.Driver");
            conn = DriverManager.getConnection(url, "root", "password");
            System.out.println("Database connected");

            Statement stmt = conn.createStatement();
            ResultSet rs = stmt.executeQuery("SELECT * FROM mytable WHERE columnfoo = 500");
            while (rs.next()) {
                System.out.println(rs.getString(1));
            }
            rs.close();
            stmt.close();
            conn.close();
        } catch (Exception e) {
            e.printStackTrace();
            System.out.println("Test failed");
        } finally {
            // release resource ....
        }
    }
}
```


----End

## 6.3.11 Why Cannot I Ping My EIP After It Is Bound to a DB Instance?

### Fault Location

1. Check security group rules.
2. Check network ACLs.
3. Ping the affected EIP from another ECS in the same region.

### Solution

1. Check security group rules.
  - a. Log in to the management console.
  - b. Click  in the upper left corner and select a region and a project.
  - c. Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - d. On the **Instances** page, click the target DB instance.
  - e. In the **Connection Information** area, click the security group.
  - f. Check whether the ECS NIC security group allows the inbound ICMP traffic.
2. Check network ACLs.
  - a. Check the network ACL status.
  - b. Check whether the NIC to which the EIP bound belongs to the subnet associated with the network ACL.
  - c. If the network ACL is enabled, add an ICMP rule to allow traffic.

#### NOTE

The default network ACL rule denies all incoming and outgoing packets. If the network ACL is disabled, the default rule still takes effect.

3. Ping the affected EIP from another ECS in the same region.

If the affected EIP can be pinged from another ECS in the same region, the virtual network is functional. In this case, contact technical support.

## 6.3.12 How Can I Obtain the IP Address of Enabled SQL audits of an Application?

### Scenario

EIPs obtained through tools are inaccurate. Therefore, applications still cannot be connected to RDS DB instances even though you have added IP addresses to a whitelist. This section describes how to obtain a local IP address.

### Procedure

- Step 1** Add IP addresses or IP address ranges that are allowed to access DB instances to the RDS whitelist.

**Step 2** Use the MySQL client to connect to an RDS for MySQL DB instance.

```
mysql -h host_name -P port -u username -p
```

Enter the password of the database account if the following information is prompted:

Enter password:

For example, if you run the following command as user **root** to connect to a DB instance:

```
mysql -h 172.16.0.31 -P 3306 -u root -p
```

**Enter password:**

**Step 3** Query process information.

```
show processlist
```

**Figure 6-1** shows the query result. The outbound IP address is the host IP address in the "show processlist" row of the Info field.

**Figure 6-1** IP query result

```
mysql> show processlist
-> ;
+-----+-----+-----+-----+-----+-----+-----+-----+
| Id      | User  | Host                | db    | Command | Time | State | Info                |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 286125391 | dctest | 121.199.31.143:14466 | NULL  | Query   | 0    | init  | show processlist   |
+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.01 sec)
```

**Step 4** View historical connection sources in audit logs if you have **enabled SQL audit**.

If this function is disabled, historical records cannot be viewed.

----End

### 6.3.13 Can I Access an RDS DB Instance Over an Intranet Connection Across Regions?

By default, RDS DB instances cannot be accessed over an intranet across regions. Cloud services in different regions cannot communicate with each other over an intranet. You can use EIP, Cloud Connect (CC), or Virtual Private Network (VPN) to connect to RDS instances across regions.

- You can access RDS instances across regions using EIP.
- CC allows you to connect VPCs in different regions, even if they are not owned by the same account.
- VPN uses an encrypted tunnel to connect VPCs in different regions and sends traffic over the Internet. It is inexpensive, easy to configure, and easy to use. However, the quality of VPN connections depends on the quality of your Internet connection.



## 6.3.14 Why Did the New Password Not Take Effect After I Reset the Administrator Password?

### Possible Causes

You may have restored from a backup before you reset the administrator password.


### Locating Method

Check whether the DB instance was restored after you reset the administrator password.

### Solution

Log in to the RDS console and reset the administrator password again. For details, see section [Resetting the Administrator Password](#).

## 6.3.15 How Do I Set the Encoding Format of the MySQL 8.0 Character Set?

1. Set `character_set_server` to `utf8` and `collation_server` to `utf8_general_ci`.
  - a. Log in to the management console.
  - b. Click  in the upper left corner and select a region and a project.
  - c. Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - d. On the **Instances** page, click the instance name.
  - e. In the navigation pane on the left, choose **Parameters**.
  - f. Search for `character_set_server` and `collation_server`, respectively, in the search box.
  - g. Set the parameters to `utf8` and `utf8_general_ci`, respectively, and click **Save**.
2. If you use a client of PHP 7.1.x, change the PHP version because it will fail to connect to MySQL 8.0 DB instances with the utf8mb4 character set.

## 6.3.16 What Should I Do If the ECS and RDS Are Deployed in Different VPCs and They Cannot Communicate with Each Other?

1. Change the VPC hosting the ECS to the same as that hosting the RDS.
2. Create a VPC peering connection.

## 6.3.17 How Do I View All IP Addresses Connected to a Database?

You can run the following SQL statement on the database to query the number of connected IP addresses:

```
SELECT substring_index(host, ':',1) AS host_name,state,count(*) FROM  
information_schema.processlist GROUP BY state,host_name;
```

### 6.3.18 Can I Access Standby RDS DB Instances?

No. You can directly access primary DB instances and read replicas. Standby DB instances are not visible to users and therefore you cannot access them directly.

RDS supports primary/standby failover and switchover. Data is synchronized between the primary and standby instances in real time.

### 6.3.19 How Do I Check the Connections to an RDS for MySQL Instance?

Use either of the following methods:

- Log in to the instance as user **root** and run the following command to view the threads running on it:  
**show full processlist;**
  - **Id:** Thread ID. You can use **kill id** to terminate a thread.
  - **User:** User used for connecting to the instance.
  - **Host:** IP address and port of the host that connects to the instance.
  - **db:** Database name.
  - **Command:** Connection status, which is usually **Sleep**, **Query**, or **Connect**.
  - **Time:** Connection duration, in seconds.
  - **State:** Status of the SQL statement being executed.
  - **Info:** SQL statement that is being executed.
  - **Memory\_used:** Memory usage of the current connection.
  - **Memory\_used\_by\_query:** Memory usage of the current query.
  - **CPU\_time:** Amount of time for which the current connection has been established. (Such information is not collected, so this column is left blank.)
  - **Trx\_executed\_time:** Execution time of the current transaction.
- On the **Instances** page, locate the instance and click **View Metric** in the **Operation** column.

View **Total Connections**. Generally, the primary and standby DB instances occupy two connections. If there are more than two connections, the instance is being connected and used by other users.

## 6.4 Database Migration

### 6.4.1 Why Do I Need to Use the mysqldump or pg\_dump Tools for Migration?

The mysqldump or pg\_dump tool is easy to use for data migration. However, when you use this tool, the server is stopped for a long period of time during data

migration. Only use these tools when there is not much data to migrate or if stopping the server for a long period of time is not an issue.

RDS is compatible with source database services. The procedure for migrating data from your database to RDS is similar to the procedure for migrating data from one database server to another.

## 6.4.2 What Should I Do When a Large Number of Binlog Files Cause Storage Space Insufficiency During an RDS MySQL Instance Migration?

During an RDS for MySQL DB instance migration, a large number of binlog files are generated in a short period of time, causing insufficient data disk space (disk usage: 91%) and affecting services.

### Solution

1. Clear expired data in a timely manner.
2. As your service data grows, the original storage space may be insufficient. If this happens, scale up storage space for your DB instance.
3. Cloud Eye monitors database metrics, such as the CPU usage, memory usage, storage space usage, and database connections, and allows you to set alarm policies to identify risks in advance.

## 6.4.3 What Types of DB Engines Does RDS Support for Importing Data?

- Exporting or importing data between DB engines of the same type is called homogeneous database export or import.
- Exporting or importing data between DB engines of different types is called heterogeneous database export or import. For example, import data from Oracle to DB engines supported by RDS.

Generally, data cannot be exported or imported between heterogeneous databases due to the different data formats involved. However, if the data formats are compatible, table data can, in theory, be migrated between them.

Third-party software is usually required for data replication to export and import between heterogeneous databases. For example, you can use a third-party tool to export table records from Oracle into a .txt file. Then, you can use LOAD statements to import the exported table records to a DB engine supported by RDS.

## 6.5 Database Permission

### 6.5.1 Why Does the Root User Not Have the Super Permissions?

RDS does not provide super permissions for the **root** user. The super permissions allow you to execute management commands, such as **reset master**, **set global**,

**kill**, and **reset slave**. These operations may cause primary/standby replication errors.

If you need to perform operations that require super permissions, RDS provides alternative methods.

- Scenario 1: If you cannot run the following command on an RDS instance to modify parameter values, you can modify parameter values through the RDS console.

**set global parameter name=*Parameter value*;**

If the script contains the **set global** command, delete the **set global** command and modify parameter values on the RDS console.

- Scenario 2: An error is reported after you run the following command because the **root** user does not have the super permissions. To solve this problem, delete **definer='root'** from the command.

**create definer='root'@'%' trigger(procedure)...**

You can import data using mysqldump. For details, see [Migrating Data to RDS for MySQL Using mysqldump](#).

## 6.5.2 RDS for MySQL Built-in Accounts

When you create an RDS for MySQL DB instance, RDS automatically creates certain system accounts (unavailable to users) for O&M operations. The system accounts include:

- `mysql.session`: used by plugins to access the server.
- `mysql.sys`: used to define objects in the `sys` schema.
- `rdsAdmin`: a management account with superuser permissions. It is used to query and modify instance information, rectify faults, migrate data, and restore data.
- `rdsRepl`: a replication account, used to synchronize data from the primary instance to the standby instance or read replicas.
- `rdsMetric`: a metric monitoring account used by watchdog to collect database status data.
- `rdsbackup`: a backup account used for background backup.
- `dsc_readonly`: used to anonymize data.

## 6.5.3 Does RDS for MySQL Support Multiple Accounts?

Yes, RDS for MySQL supports multiple accounts. You can assign different rights to these accounts through authorization commands to control access to different tables. Each table can be controlled independently.

For more details about MySQL permissions, see official [MySQL documents](#).

## 6.5.4 How Do I View Authorized Databases After a Local Client Is Connected to a DB Instance?

After connecting to the database on a local client, run the following command to grant permissions to view the database. In the command, *ip* indicates the local IP address.

```
show grants for root@'ip';
```

```
show grants for root@'%';
```

## 6.6 Database Storage

### 6.6.1 What Storage Engines Does RDS for MySQL Support?

The database storage engine is a core service for **storing, processing, and protecting data**. It can be used to control access permissions and rapidly process transactions to meet enterprise requirements.

#### InnoDB Storage Engine

For MySQL databases, only InnoDB supports backups and restorations and is therefore recommended.

#### Other Storage Engines

[Table 6-7](#) lists the storage engines not supported by MySQL 5.6 or later versions.

**Table 6-7** Unsupported storage engines

Storage Engine	Reason
MyISAM	<ul style="list-style-type: none"> <li>• MyISAM engine tables do not support transactions. They only support table-level locks. As a result, read and write operations conflict with each other.</li> <li>• MyISAM is not good at protecting data integrity. Data can be damaged or lost.</li> <li>• If data is damaged, MyISAM does not support data restoration provided by RDS for MySQL. Data can only be restored manually.</li> <li>• Data can be transparently migrated from MyISAM to InnoDB without changing code.</li> </ul>
FEDERATED	<ul style="list-style-type: none"> <li>• If primary/standby DB instances support FEDERATED, the same DML operations will be repeatedly executed on remote databases, and the data will become disordered.</li> <li>• For PITR restoration, after a full backup is restored, data on remote databases is not restored to the state it was in when the full backup was created. Accessing data during an incremental restoration will disorder FEDERATED table data.</li> </ul>

Storage Engine	Reason
MEMORY	<ul style="list-style-type: none"> <li>• If a memory table becomes empty after a restart, the database adds a DELETE event to the binlog when the table is opened. If a primary/standby DB instance uses memory tables and the standby instance (or a read replica) is restarted, a GTID is generated, which makes the standby inconsistent with that of the primary instance. As a result, the standby instance (read replica) has to be rebuilt.</li> <li>• Using memory tables may cause out-of-memory (OOM) errors and even service terminations.</li> </ul>

## 6.6.2 What Types of Storage Does RDS Use?

RDS uses Elastic Volume Service (EVS) disks for storage. For details, see *Elastic Volume Service User Guide*.

The RDS backup data is stored in OBS and does not occupy the database storage space. For details on the RDS instance storage configuration, see the *Object Storage Service User Guide*.

## 6.6.3 Does RDS for MySQL Support Stored Procedures and Functions?

Yes.

- Stored procedures and functions are a set of SQL statements that have been compiled and stored in databases. Invoking stored procedures and functions reduces the amount of data that needs to be transmitted between databases and application servers, which improve data processing efficiency.
- Differences between stored procedures or functions:
  - A function must have a return value, but a stored procedure does not.
  - The parameters of a stored procedure can be of the IN, OUT, and INOUT type, but the parameters of a function can only be of the IN type.

For details about how to create a stored procedure and a function, see the [official document](#).

## 6.6.4 What Should I Do If My Data Exceeds the Available Storage of an RDS for MySQL Instance?

### Symptom

There is not enough storage available for an RDS instance and the instance becomes read-only, so applications cannot write any data to the instance.

## Causes

1. Increased workload data
2. Too much data being stored
3. Too many RDS for MySQL binlogs generated due to a large number of transactions and write operations
4. Too many temporary files generated due to a large number of sorting queries executed by applications

## Solution

1. For insufficient storage caused by increased workload data, scale up storage space.  
If the original storage has reached the maximum, upgrade the specifications first.
2. If too much data is stored, delete unnecessary historical data.
  - a. If the instance becomes read-only, you need to contact technical support to cancel the read-only status first.
  - b. To clear up space, you can optimize tables with a high fragmentation rate during off-peak hours.  
To delete data of an entire table, run **DROP** or **TRUNCATE**. To delete part of table data, run **DELETE** and **OPTIMIZE TABLE**.
3. If binlog files occupy too much space, clear local binlogs.
4. If temporary files generated by sorting queries occupy too much storage space, optimize your SQL statements.

### 6.6.5 How Do I View the Storage Usage of My RDS Instance?

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instances** page, click the DB instance name.

**Step 5** On the **Basic Information** page, view the storage space usage in the **Storage Space** area.

----End

## 6.7 Client Installation

### 6.7.1 How Can I Install the MySQL Client?

MySQL provides client installation packages for different OSs on its official website. MySQL 5.7 is used as an example. You can download the [latest version](#) or [any other version](#) for your project. The following procedure illustrates how to

obtain the required installation package and install the MySQL client into a Red Hat Linux system.

## Procedure

### Step 1 Obtain the installation package.

Find the [link](#) to the required version on the download page. MySQL-client-5.7.31-1.el6.x86\_64.rpm is used as an example in the following figure.

**Figure 6-2** Download

MySQL Product Archives  
MySQL Community Server (Archived Versions)

Please note that these are old versions. New releases will have recent bug fixes and features!  
To download the latest release of MySQL Community Server, please visit MySQL Downloads.

Product Version: 5.7.31  
Operating System: Red Hat Enterprise Linux / Oracle Linux  
OS Version: Red Hat Enterprise Linux 6 / Oracle Linux 6 (x86\_64-bit)

RPM Bundle	Date	Size	Download
(mysql-5.7.31-1.el6.x86_64-rpm-bundle.tar)	Jun 3, 2020	467.1M	<a href="#">Download</a>
RPM Package, MySQL Server	Jun 3, 2020	161.7M	<a href="#">Download</a>
RPM Package, Client Utilities	Jun 3, 2020	24.6M	<a href="#">Download</a>
RPM Package, Development Libraries	Jun 3, 2020	3.7M	<a href="#">Download</a>
RPM Package, Development Libraries	Jun 3, 2020	131.0M	<a href="#">Download</a>

### Step 2 Upload the installation package to the ECS.

1. When you create an ECS, select an OS, such as Red Hat 6.6, and bind an EIP to it.
2. Use a remote connection tool to connect to the ECS through the bound EIP and upload the installation package to the ECS.

### Step 3 Run the following command to install the MySQL client:

```
sudo rpm -ivh MySQL-client-5.7.31-1.el6.x86_64.rpm
```

#### NOTE

- If there are any conflicts during the installation, add the **replacefiles** parameter to the command and try to install the client again. Example:  
rpm -ivh --replacefiles MySQL-client-5.7.31-1.el6.x86\_64.rpm
- If a message is displayed prompting you to install a dependency package, you can add the **nodeps** parameter to the command and install the client again. Example:  
rpm -ivh --nodeps MySQL-client-5.7.31-1.el6.x86\_64.rpm

----End

## 6.7.2 How Can I Install a PostgreSQL Client?

PostgreSQL provides [client installation methods](#) for different OSs on its official website.

The following describes how to install a PostgreSQL 12 client in CentOS.



## Procedure

### Step 1 Log in to an ECS.

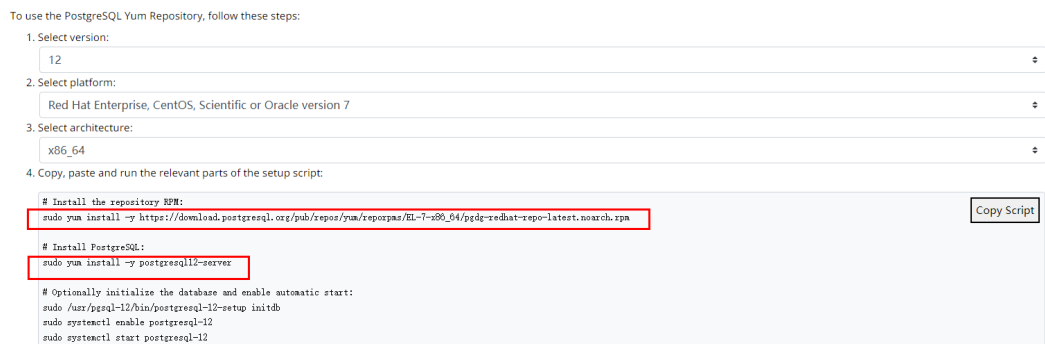
1. When you create an ECS, select an OS like CentOS 7 and bind an EIP to it.
2. Use a remote connection tool to connect to the ECS through the EIP.

### Step 2 Open the [client installation page](#).

### Step 3 Select a DB engine version, OS, and OS architecture, and run the following commands on the ECS to install a PostgreSQL client.

```
sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporepms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
sudo yum install -y postgresql12-server
```

**Figure 6-3** Installing a client



- Select a DB engine version that is consistent with that of your RDS for PostgreSQL instance.
- Select an OS that is consistent with that of the ECS.
- Select an OS architecture that is consistent with that of the ECS.

**Figure 6-4** Installing the RPM package

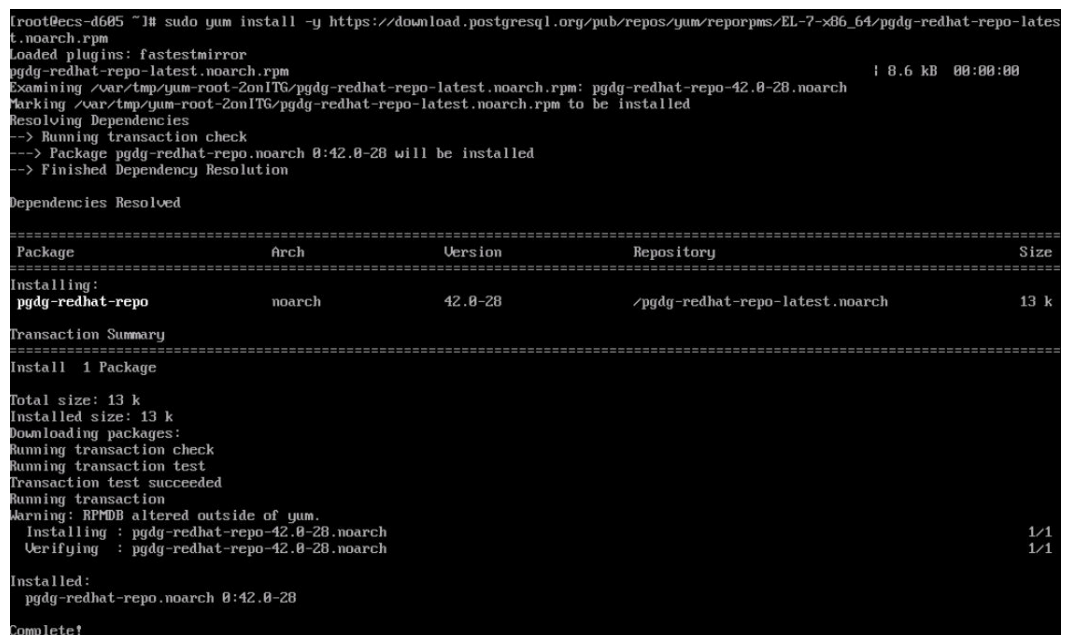


Figure 6-5 Client installed

```
Total 467 kB/s | 14 MB 00:00:30
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Importing GPG key 0x442DF0F8:
Userid : "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
Fingerprint: 60c9 e2b9 1a37 d136 fe74 d176 1f16 d2e1 442d f0f8
Package : pgdg-redhat-repo-42.0-20.noarch (@pgdg-redhat-repo-latest.noarch)
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libicu-50.2-4.e17_7.x86_64 1/4
  Installing : postgresql12-libs-12.13-1PGDG.rhel7.x86_64 2/4
  Installing : postgresql12-12.13-1PGDG.rhel7.x86_64 3/4
  Installing : postgresql12-server-12.13-1PGDG.rhel7.x86_64 4/4
  Verifying : postgresql12-libs-12.13-1PGDG.rhel7.x86_64 1/4
  Verifying : postgresql12-12.13-1PGDG.rhel7.x86_64 2/4
  Verifying : postgresql12-server-12.13-1PGDG.rhel7.x86_64 3/4
  Verifying : libicu-50.2-4.e17_7.x86_64 4/4

Installed:
  postgresql12-server.x86_64 0:12.13-1PGDG.rhel7

Dependency Installed:
  libicu.x86_64 0:50.2-4.e17_7 postgresql12.x86_64 0:12.13-1PGDG.rhel7 postgresql12-libs.x86_64 0:12.13-1PGDG.rhel7

Complete!
```

**Step 4** Connect to the RDS for PostgreSQL instance.

Figure 6-6 Connection successful

```
[root@ecs-d605 ~]# psql -h [redacted] -d postgres -U root
Password for user root:
psql (12.13, server 12.11)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=>
```

----End

## 6.8 Database Usage

### 6.8.1 Does MySQL 8.0 Support Full-Text Search?

Yes. MySQL 8.0 supports full-text search. The keyword is FULLTEXT. Run the following SQL statements to perform a test.

- Creating a table

```
CREATE TABLE ARTICLE (
  id int unsigned NOT NULL AUTO_INCREMENT,
  title varchar(200) DEFAULT NULL,
  Content text,
  PRIMARY KEY (id),
  FULLTEXT KEY title (title,content),
  FULLTEXT KEY fulltext_article (title,content)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

- Creating an index  
ALTER TABLE ARTICLE ADD FULLTEXT INDEX fulltext\_article (title,content);
- Querying an index  
SHOW INDEX FROM ARTICLE;

### 6.8.2 How Do I Use the mysqlbinlog Tool?

This section describes how to use the mysqlbinlog tool to locally parse binlogs.

The basic unit of binlog is the binlog event. Servers write binlog files in binary format. Therefore, if you want to display the binlog content in text format, you

need to use the `mysqlbinlog` tool to parse the binlog. Generally, this tool is stored in the same directory as `mysqld`.

Invoking method: `mysqlbinlog [options] log_file ...`

Example: `mysqlbinlog masterbin.000001`

Example of binlog content:

```
# at 141#210309 9:28:36 server id 123 end_log_pos 245Query thread_id=3350
exec_time=11 error_code=0
```

- **at 141:** starting position of the event in the binlog file.
- **#210309 9:28:36:** timestamp information, indicating that the binlog file is written at 09:28:36 on March 9, 2021 (UTC).
- **Query thread\_id:** thread ID.

Common `mysqlbinlog` parameters:

- **--start-position:** position where the decoding starts.
- **--start-datetime:** time where the decoding starts.
- **--stop-position:** position where the decoding stops.
- **--stop-datetime:** time where the decoding stops.
- **--skip-gtids:** `gtid_log_event` is not printed.
- **--short-form:** Only statements are displayed.
- **--result-file:** SQL file to which binlog decoding results are written.

### 6.8.3 How Do I View Session IDs and Login and Logout Time of a Database?

- View database login and logout time in SQL audit logs. For details about how to enable SQL audit, see [Enabling the SQL Audit Function](#).
- To view sessions, run the `show processlist` command in the database.

### 6.8.4 Does the OPTIMIZE TABLE Operation Lock Tables on an RDS DB Instance?

When the `OPTIMIZE TABLE` operation is performed on an RDS DB instance, the tables are locked only for a short period of time.

During the table locking period, DML operations can be performed but DDL operations cannot. DML will recreate tables, which consumes CPU and disk resources. If there are a large number of concurrent DML operations, the table will be locked for longer.

To avoid impacting services, perform the `OPTIMIZE TABLE` operation during off-peak hours.

## 6.9 Backup and Restoration

## 6.9.1 How Long Does RDS Store Backup Data For?

Automated backup data is kept based on the backup retention period you specified.

There is no limit for the manual backup retention period. You can delete manual backups as needed.

The backup data is stored in OBS and does not occupy the database storage space.

## 6.9.2 How Do I Clear RDS Backup Space?

The RDS backup space stores automated backups, manual backups, and SQL audit logs.

- **Automated full and incremental backups**  
Automated backups cannot be manually deleted. You need to change the backup retention period by referring to [Configuring an Automated Backup Policy](#). Backups that have expired will be automatically deleted.
- **Manual full backups**  
You can manually delete manual backups. For details, see [Deleting a Manual Backup](#).
- **SQL audit logs**  
You need to change the retention period by referring to . Audit logs that have expired will be automatically deleted.  
You can also disable SQL audit and select check box "I acknowledge that after audit log is disabled, all audit logs are deleted."

## 6.9.3 Can My Database Be Used in the Backup Window?

A backup window is a user-specified time during which RDS DB instances are backed up. With these periodic data backups, RDS allows you to restore DB instances to a point in time within the backup retention period.

- During the backup window, you can still use your instance except rebooting it on the console.
- When starting a full backup task, RDS first tests connectivity to your instance. If either of the following conditions is met, the test fails and a retry is performed. If the retry fails, the backup task fails.
  - DDL operations are being performed on the DB instance.
  - The backup lock fails to be obtained from the DB instance.

## 6.9.4 How Do I View My Backup Storage Usage?

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instances** page, click the DB instance name.

**Step 5** On the **Basic Information** page, view the backup space usage in the **Backup Space** area.

----End

## 6.9.5 How Can I Back Up an RDS Database to an ECS?

You can back up data to an ECS the same way you export SQL statements. The ECS service does not have restrictions on the types of data to be backed up as long as the data complies with local laws and regulations.

You can store RDS backup data on an ECS, but using an ECS is not recommended.

You are advised to use RDS automated backup and manual backup to back up data to OBS for higher data reliability and service assurance.

## 6.9.6 Will Backups Be Retained After My RDS Instance Is Deleted?

If your RDS instance is deleted, its manual backups are retained by default and will be billed based on the OBS pricing details. If you do not need the backups anymore, **delete them manually**. If your instance is frozen, its backups are not billed.

Automated backups, binlog backups, and their related files are automatically deleted.

## 6.9.7 Why Has My Automated Backup Failed?

The following figure shows the possible reasons for automated backup failures.

**Figure 6-7** Reasons why automated backup fails



- The network environment may be unstable due to problems such as network delay or interruptions.  
If RDS detects any of these problems, it triggers another automated backup half an hour later. Alternatively, you can perform a manual backup immediately.
- If multiple tasks are being executed simultaneously, there can be problems such as excessive task wait times or interruptions.  
If RDS detects any of these problems, it triggers another automated backup half an hour later. Alternatively, you can perform a manual backup immediately.
- The DB instance is abnormal probably because it is faulty or being modified.  
If RDS detects any of these problems, it triggers another automated backup half an hour later. Alternatively, you can perform a manual backup immediately.
- The backup speed depends on how many tables there are in the databases.  
If the number of tables exceeds 500,000, the backup will fail.
- A parameter change was incorrect.  
If your DB instance becomes faulty after you modify parameters of a parameter template and apply the template to the instance, check whether the modified parameters are set to correct values and whether there are any associated parameters that need to be changed, or reset the parameters to their defaults and reboot the DB instance.
- An error occurred during data import.  
For example, system table records get lost due to inappropriate data import.
  - For RDS for MySQL, you can import data again by referring to [Migrating Data to RDS for MySQL Using mysqldump](#).
  - For RDS for PostgreSQL, you can import data again by referring to [Migrating Data to RDS for PostgreSQL Using psql](#).

### 6.9.8 Why Is a Table or Data Missing from My Database?

RDS does not delete or perform any operations on any user data. If this problem occurs, check if there have been any misoperations and restore the data from backup files, if necessary.

Check for misoperations: If the SQL audit function has been enabled, you can view data execution records in audit logs.

Restore data using backup files:

- Use the RDS restoration function.
- Import the backup data to RDS through an ECS.

### 6.9.9 How Do I Restore a Local Database Backup to RDS?

You can use the DRS migration function to restore a local database backup to RDS.

For more information, see [Backups and Restorations](#).

## 6.9.10 Does RDS for PostgreSQL Support Table PITR?

No.

You can use a manual or an automated backup to restore data to the status when the backup was created. This operation restores the data of the entire DB instance. For details, see [Backups and Restorations](#).

## 6.9.11 Can I Dump Backup Files to OBS Buckets?

Incremental backups cannot be directly dumped to your OBS buckets. If you want to dump incremental backups, download merged binlogs and dump them using OBS Browser+.

Full backups cannot be directly dumped to your OBS buckets. If you want to dump full backups, download full backups locally and dump them using OBS Browser+.

## 6.9.12 Does RDS for MySQL Support Table-Level Backup to a Specified OBS Bucket?

RDS for MySQL does not support table-level backup to a specified OBS bucket.

RDS supports full backups and incremental backups (binlog backups). Both of them are stored in OBS.

## 6.9.13 Can I Delete the RDS for MySQL Backup Policy?

Sorry, you cannot delete the RDS for MySQL backup policy.

Once the backup policy is enabled, it cannot be disabled. You can change the backup retention days and backup cycle on the RDS console. The backup cycle can be changed to one day. For details, see [Configuring an Automated Backup Policy](#).

# 6.10 Database Monitoring

## 6.10.1 Which DB Instance Monitoring Metrics Do I Need to Pay Attention To?

You need to pay attention to CPU, memory, and storage space usage.

You can configure the system to report alarms based on service requirements and take measures to handle any reported alarms.

### Configuration examples:

- Configure RDS to report alarms to Cloud Eye if its CPU utilization reaches or exceeds a specific value (for example, 90%) multiple times (for example, 3 times) within a set period (for example, 5 minutes).
- Configure RDS to report alarms to Cloud Eye if its memory utilization reaches or exceeds a specific value (for example, 90%) multiple times (for example, 4 times) within a set period (for example, 5 minutes).

- Configure RDS to report alarms to Cloud Eye if its storage utilization reaches or exceeds a specific value (for example, 85%) multiple times (for example, 5 times) within a set period (for example, 5 minutes).

 **NOTE**

For details on Cloud Eye alarm configuration, see "Creating an Alarm Rule" in the *Cloud Eye User Guide*.

**Measures:**

- If a CPU or memory alarm is reported, you can scale up the vCPUs or memory by changing the DB instance class.

For details, see [Changing a DB Instance Class](#).

- If a storage space usage alarm is reported, you can:
  - Check the storage space consumption to see if any space can be freed up by deleting data from DB instances or by dumping the data to another system.
  - Scale up the storage space.

For details, see [Scaling up Storage Space](#).

## 6.10.2 How Can I Calculate the Memory Usage of an RDS DB Instance?

Click the target RDS DB instance. On the **Advanced O&M** page, you can view its memory usage.

The formula for calculating the memory usage is as follows:

Memory usage = (Total memory – (Available memory + Buffer memory + Cache memory))/Total memory

## 6.10.3 How Do I Set an Alarm Rule for the Replication Delay Between Primary and Standby DB Instances?

You can set an alarm rule for the replication delay by referring to the following:

- [Setting Alarm Rules](#)
- [Setting Alarm Rules](#)

## 6.11 Capacity Expansion and Specification Change

### 6.11.1 Are My RDS DB Instances Still Available During Storage Scale-up and Instance Class Change?

Currently, you can scale up storage space and change the vCPU or memory of a DB instance.

- When storage space is being scaled up, RDS DB instances are still available and services are not affected. However, you cannot delete or reboot DB instances that are being scaled.



- During the change of the vCPU or memory, the network is intermittently disconnected for one or two times in seconds. For primary/standby DB instances, a failover may occur and services may be briefly interrupted. Changing the vCPU or memory takes 5 to 15 minutes.  
After you change the vCPU or memory, the DB instances will reboot and services will be interrupted. Therefore, you are advised to change instance classes during off-peak hours.

## 6.11.2 Why Does the DB Instance Become Faulty After the Original Database Port Is Changed?

### Symptom

- The DB instance is in **Faulty** state after the original database port is changed.
- The DB instance cannot be connected using the new database port.

### Possible Causes

The submitted database port is occupied.

### Procedure

Change the database port to the new port again. For details, see [Changing a Database Port](#).

- If the database port is changed successfully, the previous change failed because the submitted database port was occupied.
- If the original database port still fails to be changed, contact technical support.

## 6.11.3 Can I Change the VPC that My RDS DB Instance Belongs To?

No, you cannot directly change the VPC on the RDS console.

However, you can change the VPC by restoring a full backup to a new DB instance. For operation details, see [Restoring from Backup Files to DB Instances](#).

## 6.12 Database Parameter Modification

### 6.12.1 What Inappropriate Parameter Settings Cause Unavailability of the RDS for PostgreSQL Database?

In the following cases, inappropriate parameter settings cause the database to be unavailable:

- Parameter value ranges are related to DB instance specifications.  
The maximum values of **shared\_buffers** and **max\_connections** are related to the DB instance physical memory. If you set these parameters inappropriately, the database will be unavailable.

- Parameter association is incorrect.
  - If **log\_parser\_stats**, **log\_planner\_stats**, or **log\_executor\_stats** is enabled, you must disable **log\_statement\_stats**. Otherwise, the database is unavailable.
  - **max\_connections**, **autovacuum\_max\_workers**, and **max\_worker\_processes** must meet the following requirements. Otherwise, the database is unavailable.  
**max\_connections** value + **autovacuum\_max\_workers** value + **max\_worker\_processes** value + 1 < 8388607

 NOTE

For additional details, visit the [PostgreSQL official website](#).

Solution:

1. Log in to the RDS console and query the logs to locate the incorrectly configured parameters.
2. On the **Configuration** page, change parameters to default values and reboot the database.
3. Configure the incorrect parameter values and restore other parameters to their original default values.

## 6.12.2 How Can I Change the Time Zone?

You can set the time zone only on the RDS console. Different DB engines have different time zone policies.

- RDS for MySQL and RDS for PostgreSQL allow you to select a time zone when you create a DB instance and change the time zone after the instance is created.


---

**NOTICE**

- If the time zone of your RDS for MySQL instance is different from that of the region where your workloads are deployed, or if the DST and standard time are switching in your country, you need to adjust the time zone of the instance.
- After the time zone parameter is modified, you need to reconnect to the instance for the modification to take effect.

---

To change the time zone for an RDS for MySQL or RDS for PostgreSQL DB instance, perform the following steps:

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instances** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Parameters**.

**Step 6** Search for a time zone parameter in the search box, for example, **time\_zone**.

- The time zone parameter for RDS for MySQL is **time\_zone**.
- The time zone parameter for RDS for PostgreSQL is **timezone**.

**Step 7** Select a time zone, and click **Save**.

**Step 8** In the displayed dialog box, click **OK**.

----End

## Time Zone Parameters

- **system\_time\_zone**: operating system (OS) time zone. This parameter cannot be changed and it has no impact on the database time zone.
- **time\_zone**: database time zone. You can modify this parameter to change the time zone for your DB instance.

### 6.12.3 How Do I Configure a Password Expiration Policy for RDS for MySQL DB Instances?

In MySQL 5.6, you can run **ALTER USER *username* PASSWORD EXPIRE** to set the password expiration policy.

In MySQL 5.7 and 8.0, you can set the global variable **default\_password\_lifetime** to control the default validity period of a user password.

The value of **default\_password\_lifetime** indicates how many days until a password expires. The default value is **0**, indicating that the created user password will never expire.

```
mysql> show variables like 'default_password_lifetime';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| default_password_lifetime | 0 |
+-----+-----+
1 row in set (0.00 sec)
```

## Changing the Global Automatic Password Expiration Policy

Change the value of the **default\_password\_lifetime** parameter on the RDS console.

## Checking the Password Expiration Date of All Users

Run the following command:

```
mysql> select
user,host,password_expired,password_last_changed,password_lifetime from
user;
```

```
mysql> select user,host,password_expired,password_last_changed,password_lifetime from user;
+-----+-----+-----+-----+-----+
| user          | host      | password_expired | password_last_changed | password_lifetime |
+-----+-----+-----+-----+-----+
| mysql.session | localhost | N                | 2020-01-17 15:02:23   | NULL              |
| mysql.sys     | localhost | N                | 2020-01-17 15:02:23   | NULL              |
| rdsAdmin      | localhost | N                | 2020-01-17 15:02:30   | 0                 |
| root          | %        | N                | 2020-03-05 14:23:54   | NULL              |
| rdsRepl       | 192.168.% | N                | 2020-01-17 15:02:45   | 0                 |
| rdsMetric     | 192.168.% | N                | 2020-01-17 15:02:30   | 0                 |
| rdsBackup     | localhost | N                | 2020-01-17 15:02:30   | 0                 |
| u_test01      | %        | N                | 2020-03-05 14:28:10   | 30                |
| u_test02      | %        | N                | 2020-03-05 14:28:38   | NULL              |
| jeffrey       | localhost | N                | 2020-03-05 15:23:17   | NULL              |
+-----+-----+-----+-----+-----+
10 rows in set (0.00 sec)
```

## Checking the Password Expiration Policy of a Specified User

Run the following command:

```
mysql> show create user jeffrey@'localhost';
```

```
mysql> show create user jeffrey@'localhost';
+-----+-----+-----+-----+-----+
| CREATE USER FOR jeffrey@localhost |
+-----+-----+-----+-----+-----+
| CREATE USER 'jeffrey'@'localhost' IDENTIFIED WITH 'mysql_native_password' AS '*1269F151658F0C925558311940C8B5486087F' REQUIRE NONE PASSWORD_EXPIRE DEFAULT ACCOUNT UNLOCK |
+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```


**EXPIRE DEFAULT** indicates that the password follows the global expiration policy.

## Configuring the Password Expiration Policy for a Specified User

- Configuring the password expiration policy during user creation  
**create user 'script'@'localhost' identified by '\*\*\*\*\*' password expire interval 90 day;**
- Configuring the password expiration policy after user creation  
**ALTER USER 'script'@'localhost' PASSWORD EXPIRE INTERVAL 90 DAY;**
- Setting the password to be permanently valid  
**CREATE USER 'mike'@'%' PASSWORD EXPIRE NEVER;**  
**ALTER USER 'mike'@'%' PASSWORD EXPIRE NEVER;**
- Setting the password to follow the global expiration policy  
**CREATE USER 'mike'@'%' PASSWORD EXPIRE DEFAULT;**  
**ALTER USER 'mike'@'%' PASSWORD EXPIRE DEFAULT;**

## 6.12.4 How Do I Change the RDS Transaction Isolation Level?

You can change the transaction isolation level by setting the **tx\_isolation** parameter on the RDS console.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instances** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Parameters**. On the **Parameters** tab page, locate **tx\_isolation** and select the desired isolation level from the drop-down list in the **Value** column. The following values are available for you to choose from:

- **READ-UNCOMMITTED**
- **READ-COMMITTED**
- **REPEATABLE-READ**
- **SERIALIZABLE**

**Step 6** Click **Save**. In the displayed dialog box, click **Yes**.


----End

## 6.12.5 Does RDS for PostgreSQL Support the test\_decoding Plugin?

PostgreSQL 10, PostgreSQL 11, and PostgreSQL 13 support test\_decoding. For more information about test\_decoding, see [test\\_decoding introduction](#).

To use test\_decoding, set **wal\_level** to **logical**.

**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner and select a region and a project.

**Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

**Step 4** On the **Instances** page, click the target DB instance.

**Step 5** In the navigation pane on the left, choose **Parameters**. On the **Parameters** tab page, locate **wal\_level** and change its value to **logical**.

**Step 6** Click **Save**. In the displayed dialog box, click **Yes**.


----End


## 6.12.6 How Do I Use the utf8mb4 Character Set to Store Emojis in an RDS for MySQL DB Instance?

To store emojis in an RDS for MySQL DB instance, ensure that:

- The client outputs the utf8mb4 character set.
- The connection supports the utf8mb4 character set. If you want to use a JDBC connection, download MySQL Connector/J 5.1.13 or a later version and leave **characterEncoding** undefined for the JDBC connection string.
- Configure the RDS DB instance as follows:
  - Setting **character\_set\_server** to **utf8mb4**

Parameter Name <a href="#">↗</a>	Effective upon Reboot <a href="#">↗</a>	Value	Allowed Values	Description
character_set_server	Yes	<input type="text" value="utf8mb4"/>	utf8, latin1, gbk, utf8mb4	The server's default character set.

- Log in to the management console.
- Click  in the upper left corner and select a region and a project.
- Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

- iv. On the **Instances** page, click the instance name.
- v. In the navigation pane on the left, choose **Parameters**. On the **Parameters** tab page, locate **character\_set\_server** and change its value to **utf8mb4**.
- vi. Click **Save**. In the displayed dialog box, click **Yes**.
- Selecting **utf8mb4** for database character set
  - i. Log in to the management console.
  - ii. Click  in the upper left corner and select a region and a project.
  - iii. Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
  - iv. On the **Instances** page, click the instance name.
  - v. On the **Databases** page, click **Create Database**. In the displayed dialog box, enter a database name and remarks, select the character set **utf8mb4**, and authorize permissions for users. Then, click **OK**.
- Setting the character set of the table to **utf8mb4**

```
([...]) [ ... ]> create table emoji_01 (id int auto_increment primary key, content varchar(255)) default charset utf8mb4;
Query OK, 0 rows affected (0.01 sec)

([...]) [ ... ]> show create table emoji_01 \G
***** 1. ROW *****
      Table: emoji_01
      Create Table: CREATE TABLE 'emoji_01' (
        'id' int(11) NOT NULL AUTO_INCREMENT,
        'content' varchar(255) DEFAULT NULL,
        PRIMARY KEY ('id')
      ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4
      1 row in set (0.00 sec)
```


## FAQs

If you have set **characterEncoding** to **utf8** for the JDBC connection string, or the emoji data cannot be inserted properly after you have performed the above operations, you are advised to set the connection character set to **utf8mb4** as follows:

```
String query = "set names utf8mb4";
stat.execute(query);
```

### 6.12.7 Can I Use SQL Commands to Modify Global Parameters?

Sorry, you cannot use SQL commands to modify global parameters, but you can modify specific parameters on the RDS console.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and a project.
- Step 3** Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
- Step 4** On the **Instances** page, click the target DB instance.
- Step 5** In the navigation pane on the left, choose **Parameters**.
- Step 6** Change the value of the target parameter and click **Save**.

**Step 7** In the displayed dialog box, click **OK**.

----End

## 6.12.8 How Do I Set Case Sensitivity for RDS for MySQL Table Names?

You can set case sensitivity for table names while creating an instance, or change the value of the case sensitivity parameter after the instance is created.

### NOTICE

To change the value of **lower\_case\_table\_names**:

- Ensure that each table name is unique and in correct case and there is no backup delay.
- Perform the following operations for DB instances associated with read replicas:
  1. Change the value of **lower\_case\_table\_names** for read replicas, for example, from **1** to **0**.
  2. Manually reboot the primary DB instance.
  3. Change the value of **lower\_case\_table\_names** for the primary DB instance, for example, from **1** to **0**.
  4. Manually reboot the primary DB instance again.

- If your instance runs MySQL 5.6 or 5.7, you can change the value of **lower\_case\_table\_names** after the instance is created.
- You can set case sensitivity for table names when creating an RDS for MySQL 5.6, 5.7, or 8.0 instance on the console or using APIs.

The case sensitivity of table names for created RDS for MySQL 8.0 instances cannot be changed.

- Set **Table Name Case Sensitivity** on the RDS console by referring to [Buy a DB Instance](#).

## 6.12.9 Can I Enable Query Caching for My RDS for MySQL Instance?

Parameters related to query caching cannot be set on the console.

You are not advised to enable query caching because:

- Query caching helps improve query speed only when you frequently access the same SQL statement, but consumes additional resources and reduces the SQL execution speed in other scenarios.
- Function test results show that the query speed of an instance without enabling query caching is faster than that when this function is enabled.
- Query caching is no longer maintained in the MySQL community.

## 6.13 Network Security

## 6.13.1 What Security Protection Policies Does RDS Have?

### Network

- RDS runs your DB instances in a VPC, ensuring that the DB instances are isolated from other services.
- RDS uses security groups to ensure that only trusted sources can access your DB instances.
- RDS supports SSL connections to encrypt data during transmission.

### Management

You can use the Identity and Access Management (IAM) service to manage RDS permissions.

## 6.13.2 How Can Data Security Be Ensured During Transmission When I Access RDS Through an EIP?

When you access RDS through an EIP, workload data will be transmitted on the Internet.

To prevent any potential data breaches, you are advised to use SSL to encrypt data transmitted on the Internet.

You can also use Direct Connect or VPN to encrypt data transmission.

## 6.13.3 How Can I Prevent Untrusted Source IP Addresses from Accessing RDS?

- If you enable public accessibility, your EIP DNS and database port may be vulnerable to hacking. To protect information such as your EIP, DNS, database port, database account, and password, you are advised to set the range of source IP addresses in the RDS security group to ensure that only trusted source IP addresses can access your DB instances.
- To prevent your database password from being cracked, set a strong password and periodically change it.

## 6.13.4 How Do I Configure a Security Group to Enable Access to RDS DB Instances?

- When you attempt to connect to a DB instance through a private network, check whether the ECS and RDS DB instance are in the same security group.
  - If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No security group rules need to be configured.
  - If the ECS and RDS DB instance are in different security groups, you need to configure security group rules for them, separately.
    - RDS DB instance: Configure an **inbound rule** for the security group with which the DB instance is associated.



- ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.
- When you attempt to connect to a DB instance through an EIP, you need to configure an **inbound rule** for the security group associated with the DB instance.

## 6.13.5 How Can I Import the Root Certificate to a Windows or Linux OS?

### Importing the Root Certificate to the Windows OS

1. Click **Start** and choose **Run**. In the displayed **Run** dialog box, enter **MMC** and press **Enter**.
2. On the displayed console, choose **File > Add/Remove Snap-in**.
3. In the left **Available snap-ins** pane of the displayed **Add or Remove Snap-ins** dialog box, select **Certificates** and click **Add**.
4. In the displayed **Certificates snap-in** dialog box, select **Computer account** and click **Next**.
5. In the displayed **Select Computer** dialog box, click **Finish**.
6. In the **Add or Remove Snap-ins** dialog box, click **OK**.
7. On the console, double-click **Certificates**.
8. Right-click **Trusted Root Certification Authorities** and choose **All Tasks > Import**.
9. In the displayed **Certificate Import Wizard** dialog box, click **Next**.
10. Click **Browse** to change the file type to **All Files (\*.\*)**.
11. Locate the downloaded root certificate ca.pem file and click **Open**. Then, click **Next**.

---

**NOTICE**

You must change the file type to **All Files (\*.\*)** because **.pem** is not a standard certificate extension name.

---

12. Click **Next**.
13. Click **Finish**.
14. Click **OK** to complete the import of the root certificate.

### Importing the Root Certificate to the Linux OS


You can use a connection tool (such as WinSCP or PuTTY) to upload the certificate to any directory on a Linux OS.

## 6.13.6 How Can I Identify the Validity Period of an SSL Root Certificate?

When you connect to an RDS for MySQL DB instance using an SSL connection, run the following command to check whether the certificate has expired:

```
show status like '%ssl_server%';
```

Update the root certificate to the latest version before it expires:

1. In the **DB Information** area on the **Basic Information** page, click  in the **SSL** field to download the root certificate or certificate bundle.
2. Reboot the DB instance for the new certificate to take effect.
3. Connect to the DB instance using the new certificate or certificate bundle.

### NOTE

If a certificate is about to expire, replace it with an officially issued certificate to improve system security.

## 6.13.7 What Are the Possible Causes for Data Corruption?

- **Data tampering**  
Lots of security measures are provided to ensure that only authenticated users have permissions to perform operations on database table records. Database tables can be accessed only through specific database ports.  
Verifying package during primary/standby synchronization can prevent data tampering. RDS for MySQL uses the InnoDB storage engine to prevent data from being damaged.
- **DB instance servers may be powered off suddenly, causing database page corruption and database rebooting failures.**  
If a primary DB instance becomes faulty, RDS switches to the standby DB instance within 1 to 5 minutes to provide services for you. Databases cannot be accessed during a failover. You must configure automatic reconnection between your applications and RDS to make sure that your applications are available after the failover.

## 6.14 Version Upgrade

### 6.14.1 Does RDS for MySQL Support Version Upgrades?

- **Major version upgrades**  
Major versions cannot be upgraded on the RDS console. You can use Data Replication Service (DRS) to migrate databases from RDS for MySQL 5.6 to RDS for MySQL 5.7 smoothly. **Before using DRS to upgrade a major version, you need to prepare a DB instance of the target version.**  
On the **Instances** page, click the target DB instance. On the displayed **Basic Information** page, click **Migrate Database** in the upper right corner of the page.

**Table 6-8** MySQL database version information

Source Database Version	Destination Database Version	Migration Type
RDS for MySQL/Self-built MySQL/MySQL in other clouds <ul style="list-style-type: none"> <li>• 5.5.x</li> <li>• 5.6.x</li> <li>• 5.7.x</li> <li>• 8.0.x</li> </ul>	RDS for MySQL <ul style="list-style-type: none"> <li>• 5.6.x</li> <li>• 5.7.x</li> <li>• 8.0.x</li> </ul>	Version upgrade

### 6.14.2 Does RDS for MySQL Support Version Downgrades?

RDS for MySQL does not support version downgrades on the management console.

You can [use mysqldump to migrate data](#), or delete the DB instance and create a new one.

# A Change History

---

Released On	Description
2024-04-15	This issue is the first official release.