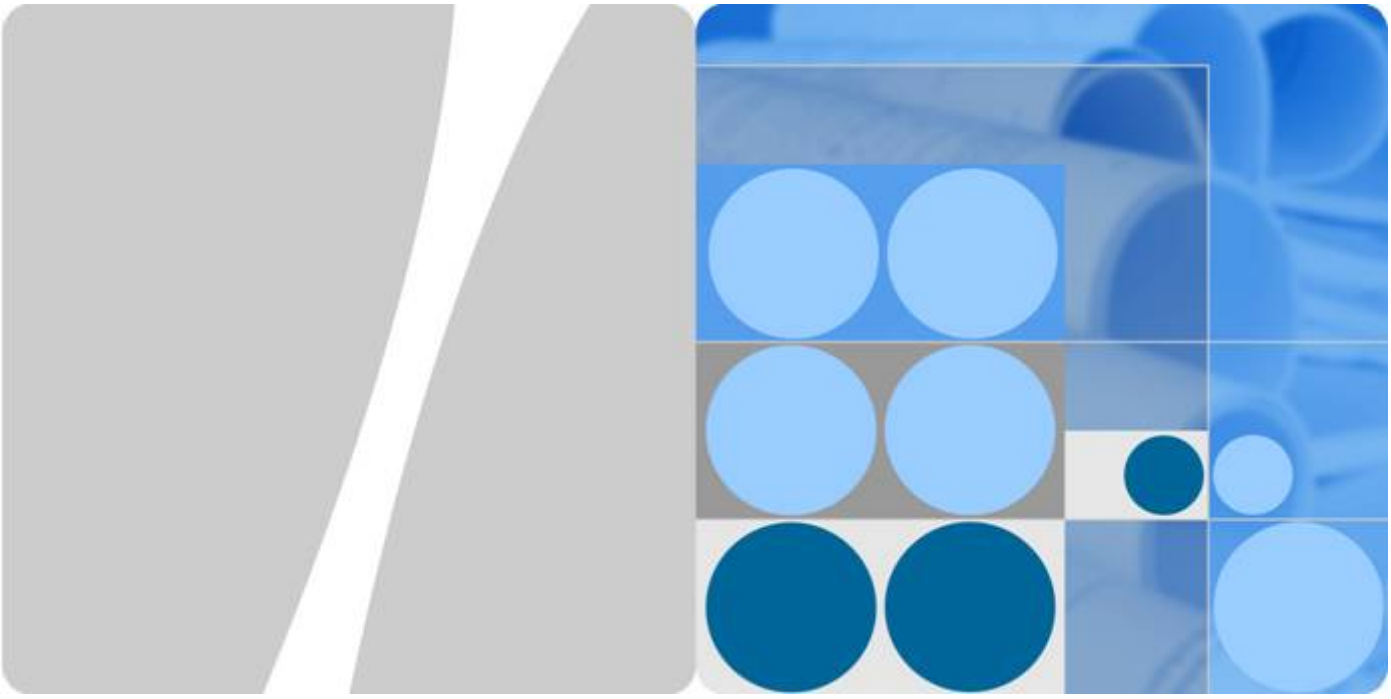


Relational Database Service

FAQs

Issue 28

Date 2021-01-18

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Contents

1 Product Consulting

1.1 What Precautions Should Be Taken When Using RDS?

1. DB instances' operating systems (OSs) are invisible to you. Your applications can access a database only through the IP address and port.
2. The backup files stored in OBS and the ECS used by RDS are invisible to you. They are visible only in the RDS instance management system.
3. Precautions after purchasing RDS:

   After purchasing RDS DB instances, you do not need to perform basic database O&M operations, such as applying HA and security patches. However, you must still pay attention to:

   a. Whether the CPU, input/output operations per second (IOPS), and space are insufficient for the RDS DB instances. If any of these becomes insufficient, you will need to 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.

1.2 What Is the Availability of RDS DB Instances?

Formula for an RDS DB instance availability:

DB instance availability = (1 – Failure duration/Total service duration) × 100%

1.3 Can I Use a Template to Create DB Instances?

Currently, you cannot use a template to create DB instances.

1.4 How Long Does It Take to Create a DB Instance?

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 DB instance. A larger data amount indicates a longer read replica creation time. If the primary DB instance is empty, creating a read replica takes 7 to 8 minutes.

If the duration is exceeded, a fault may occur during the creation. Please contact customer service.

1.5 What Are the Differences Between RDS and Other Database Solutions?

Table 1-1 Differences between RDS and other database solutions

Function Item	RDS	Self-Built Database Service
Service availability	For details, see Elastic Cloud Service User Guide.	Requires self-guarantee, primary/standby relationship setup, and RAID setup.
Data reliability	For more information, see the *Elastic Volume Service User Guide*.	Requires self-guarantee, primary/standby relationship setup, and RAID setup.
System security	Defends against Anti-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.
Database backup	Automated backups	You must find backup storage space to back up the database by yourself and periodically check whether backup data can be restored.
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.	The hosting cost is high.

Function Item	RDS	Self-Built Database Service
Maintenance cost	Not required.	Full-time Database Administrators (DBAs) are required for maintenance, leading to high manpower costs.
Deployment and scaling	Supports elastic scaling, fast deployment, and on-demand enabling.	Requires procurement, deployment, and coordination of hardware.
Resource utilization	Bills users based on the resources actually used, resulting in high resource utilization.	Peak resource utilization is considered, leading to low resource usage.

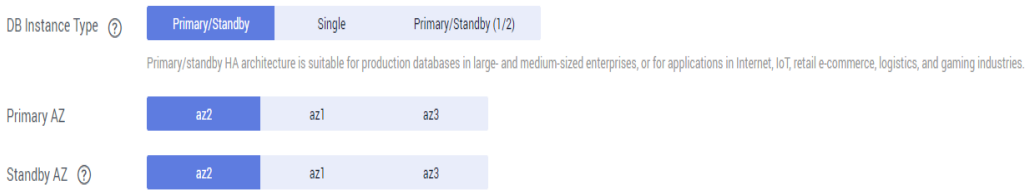
1.6 Will My RDS DB Instances Be Affected by Other Users' DB Instances?

No. Your RDS DB instances and resources are isolated from other users' DB instances.

1.7 Does RDS Support Cross-AZ High Availability?

Yes. RDS supports cross-AZ high availability. When you create primary/standby DB instances, you can select different AZs for them.

Figure 1-1 Cross-AZ high availability



1.8 Can RDS Primary/Standby DB Instances Be Changed to Single DB Instances?

No. Only RDS single DB instances can be changed to primary/standby DB instances.

1.9 What Are the Browsers Supported By RDS?

See **browsers supported by RDS**.

1.10 What Should I Do If Garbled Characters Are Displayed After SQL Query Results Are Exported to an Excel File?

The default code is utf8. You need to convert the default code to Unicode.

1.11 How Do I Create an AD Domain?

Active Directory, which is short for AD, is a directory service on Windows Standard Server, Windows Enterprise Server, and Windows Datacenter Server. (Active Directory cannot run on the Windows Web Server, but it can manage the computers running the Windows Web Server.) Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

Procedure

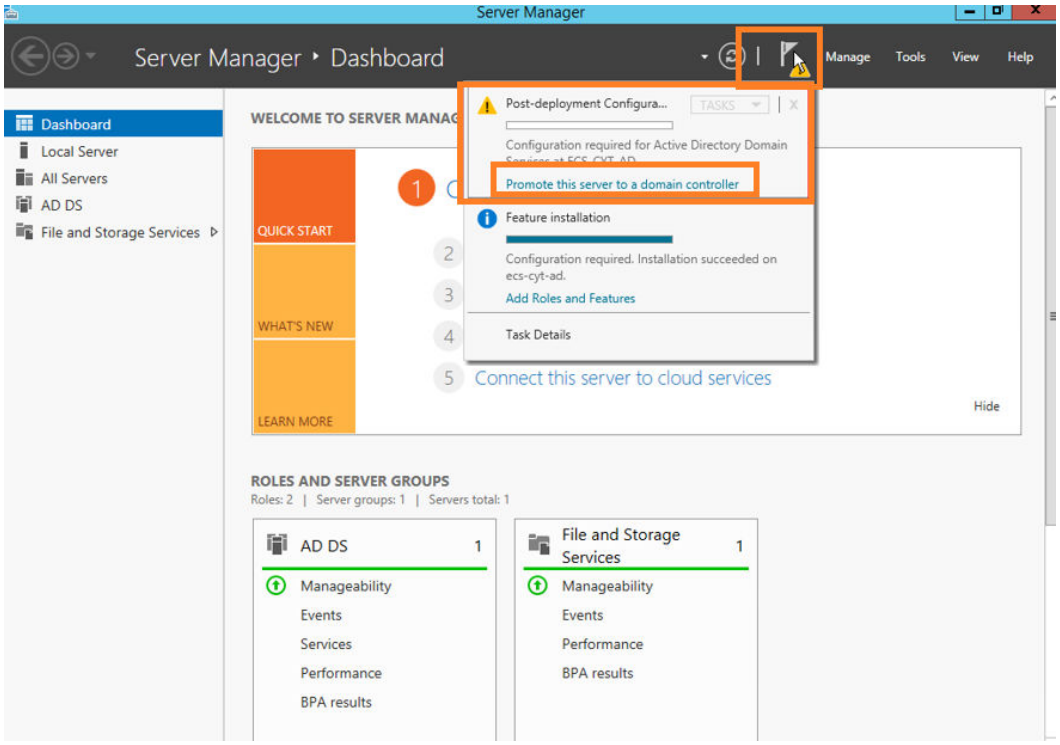
This section describes how to use Windows Server 2012 R2 to create a domain server.

NOTE

1. When you configure an AD domain information during the DB instance creation, do not configure or disable Group Policy Object (GPO) for your domain controller server. Otherwise, the DB instance creation will fail.
2. If GPO is required, you need to buy an ECS and set up a new domain controller server with GPO disabled. Then, establish trust between your domain controller server and the new domain controller server. For details, contact customer service.

Step 1 Install an AD domain controller.

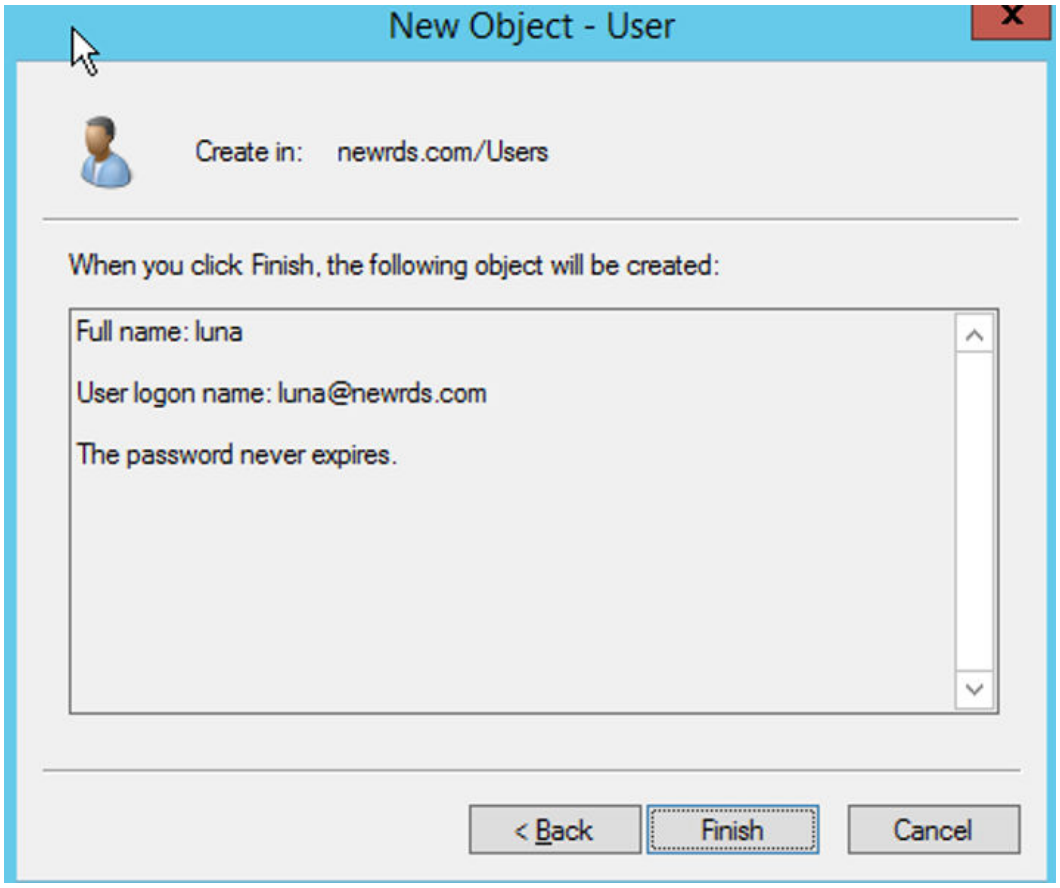
1. In Server Manager, choose **Manage** > **Add Roles and Features**.
2. In the **Add Roles and Features Wizard** dialog box, click **Next** until the **Select server roles** page is displayed. Select **Active Directory Domain Services** and click **Add Features** in the displayed box.
3. Click **Next** until the **Confirm installation selections** page is displayed. Click **Install** to start the role installation process.
4. After the installation is complete, a yellow triangle icon is displayed. Click **Promote this server to a domain controller**. The **Active Directory Domain Services Configuration Wizard** window is displayed.



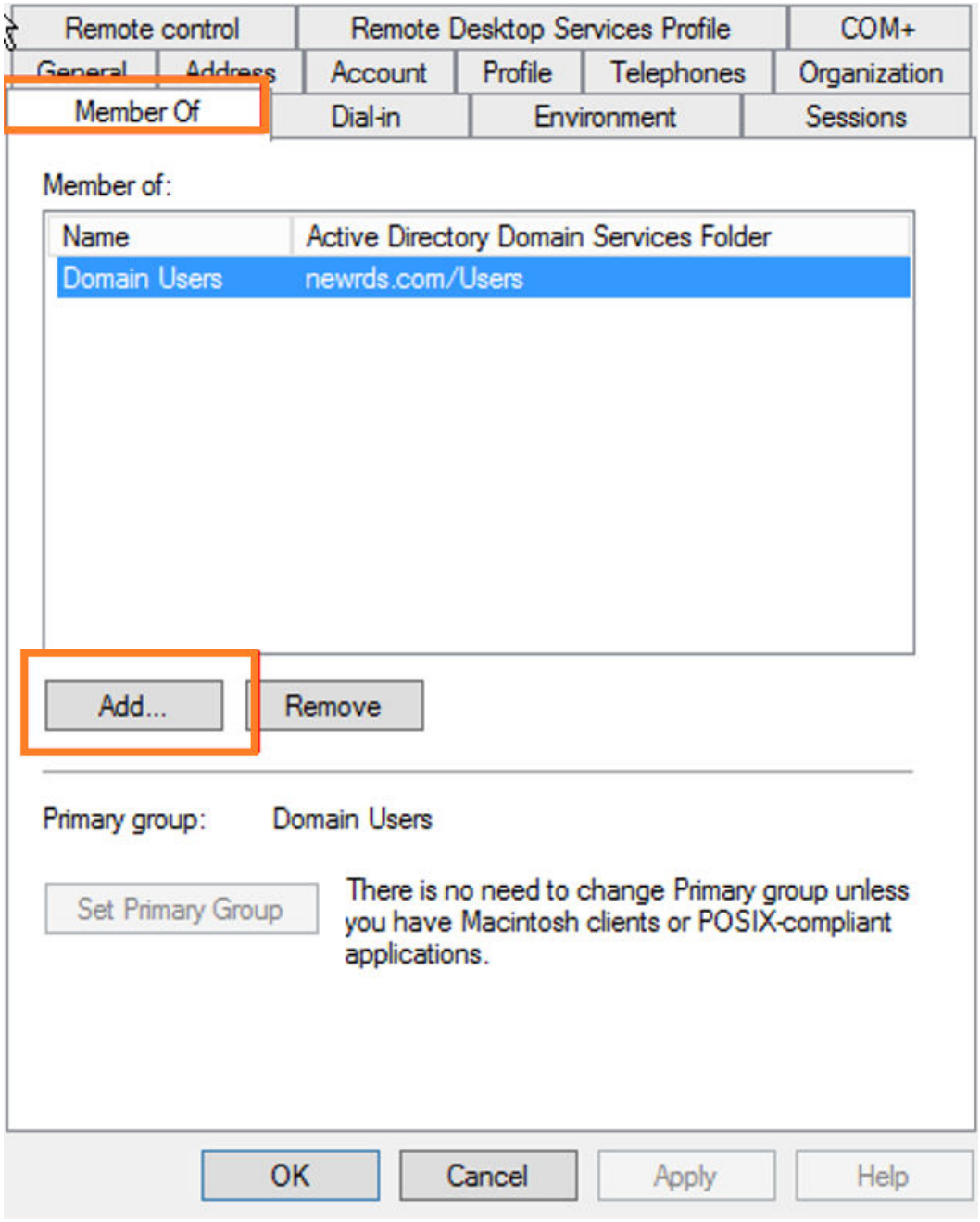
5. On the **Deployment Configuration** page, select **Add a new forest** and set a domain name, such as newrds.com.
6. Click **Next**. On the displayed page, enter the DSRM password (non-domain user).
7. Click **Next** until the **Prerequisites Check** page displayed. Click **Install**. After the installation is complete, the server automatically reboots.
8. Modify the DNS configuration of the network interface. Set the IP address of the active DNS server to the server's private IP address, such as 192.168.0.133.

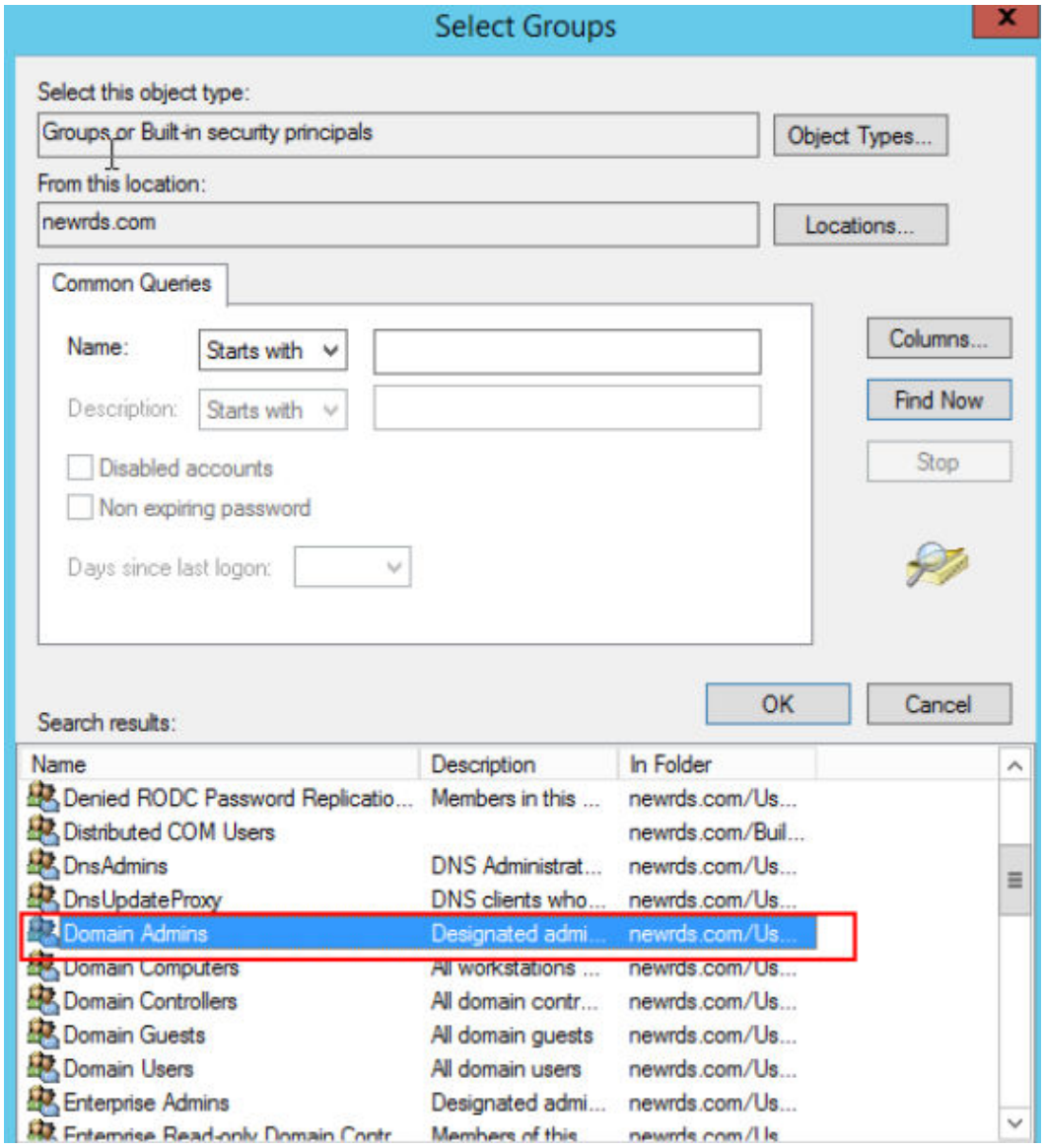
Step 2 Create and add a domain account.

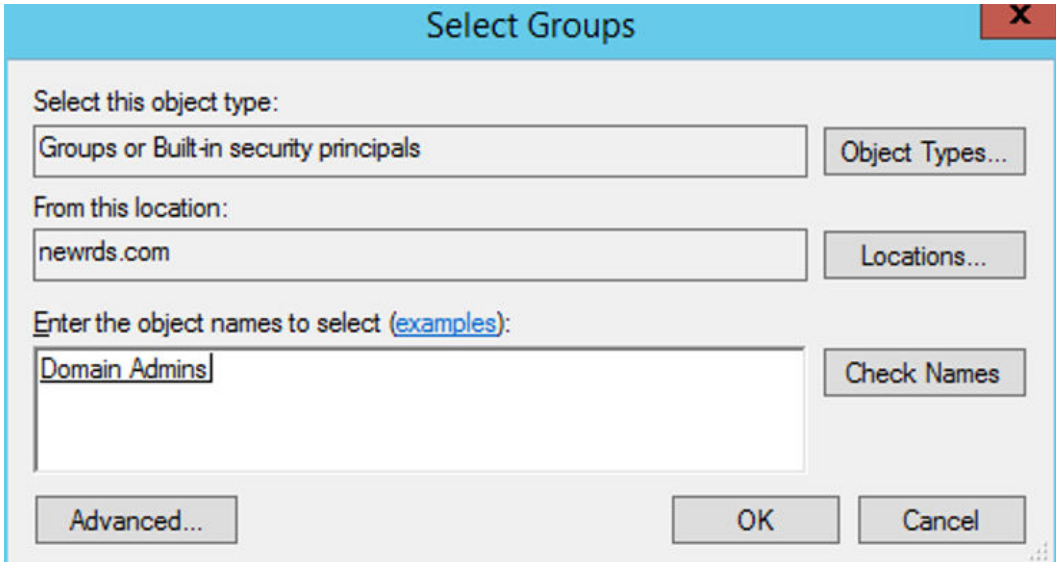
1. Open **Active Directory Users and Computers**, right-click on the **Users** and choose **New** > **User**. Enter the username and click **Next**.
2. Enter the first name, last name, and user login name, such as luna@newrds.com.
3. Enter the password and then confirm it. Deselect all check boxes (do not change the password at the first login).
4. After the user is added, a figure similar to the following is displayed. You can add domain accounts to user groups for permission control.

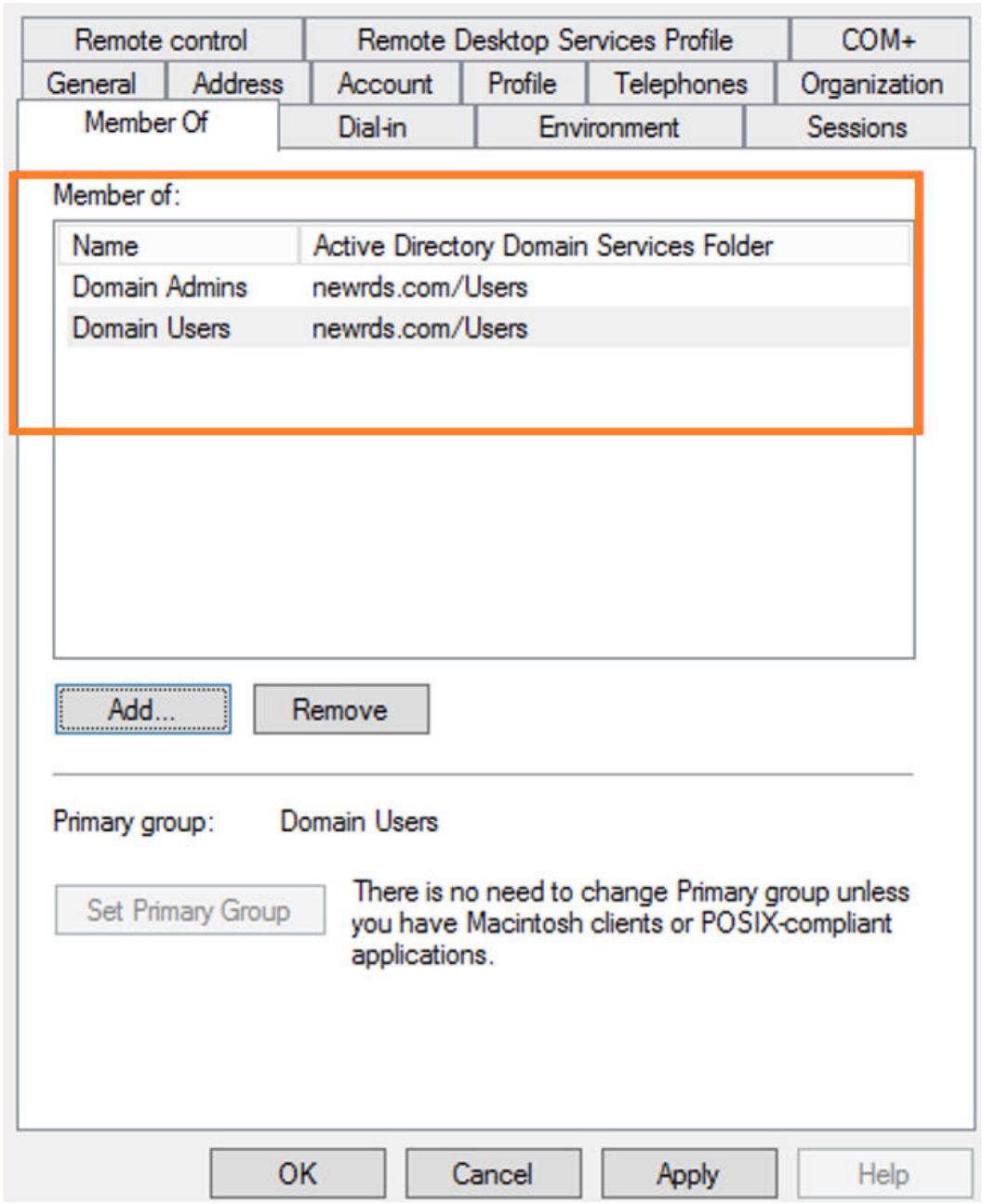


5. Add the domain account for logging in to RDS to the Active Directory Admin group.









Step 3 Add an RDS DB instance to the domain.

On the instance creation page, click **Configure** to configure the AD domain and then complete the DB instance creation. After the instance is created, the AD domain can be used.

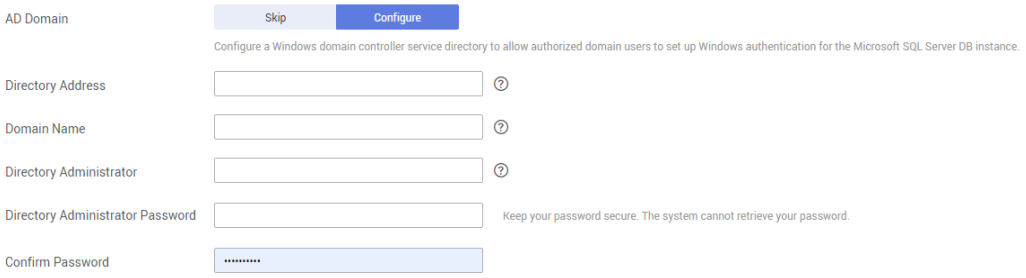


Table 1-2 AD domain parameters

Parameter	Description
Directory Address	Enter the IP address of the ECS that supports the AD domain. For example: 192.168.x.x. **NOTE** Ensure that the ECS IP address can connect to the RDS DB instance. If you encounter any network problems, contact customer service.
Domain Name	A fully qualified domain name, such as DBStest.com, must: 1. Be the same as the ECS domain name. 2. Be no more than 48 characters long. 3. Only include letters, digits, dots (.), and hyphens (-). 4. Include a valid top-level domain name which contains at least 2 characters long and contains only dots (.) and letters.
Directory Administrator	You are advised to enter the domain administrator username.
Directory Administrator Password	Password of the directory administrator. Keep this password secure. The system cannot retrieve it.

----End

1.12 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, the table locking duration will be longer. Therefore, you are advised to perform the OPTIMIZE TABLE operation during off-peak hours.

1.13 What Can I Do About Websites Responding Slower After Using RDS?

To solve this problem, you are advised to perform the following operations:

- Check the performance status of RDS DB instances on the RDS console.
- Check and compare the current database connection status of the local database and the RDS DB instance. This problem may be related to applications.

1.14 Can I Set the Synchronize Model Between Primary DB Instances and Read Replicas?

The synchronize model displayed on the RDS console indicates the data synchronization method between primary and standby DB instances. Semi-synchronous and asynchronous are supported. The semi-synchronous model improves data security and asynchronous model improves performance.

The default synchronize model between primary DB instances and read replicas is asynchronous and cannot be changed.

1.15 How Does a Cloud Database Perform a Primary/Standby Switchover?

RDS provides primary/standby DB instances for high availability. The system will perform a primary/standby failover in case of a failure.

Failover (Automatic)

It is also called out-planned handover. If the primary DB instance fails, the system will automatically switch to the standby DB instance within 5 minutes. No human intervention is required. The connection IP address remains unchanged. DB instances cannot be accessed during the failover. You need to configure automatic reconnections between applications and RDS DB instances to ensure near-continuous availability.

Switchover (Manual)

It is also called out-planned handover. When a DB instance is running properly, you can manually perform a primary/standby switchover as required.

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 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

Primary/standby switchover may cause service interruption for some seconds or minutes (determined by the replication delay). If the primary/standby synchronization delay is too long, a small amount of data may get lost. To prevent traffic congestion, you are advised to perform switchover during off-peak hours.

Step 6 If you have enabled the operation protection function, click **Start Verification** in the displayed dialog box. On the displayed page, click **Send Code**, enter the obtained verification code, and click **Verify** to close the page.

Two-factor authentication is required to improve the security of your account and cloud product. For details about how to enable operation protection, see the *Identity and Access Management User Guide*.

Step 7 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 8 After a switchover is successful, you can view and manage the DB instance on the **Instance Management** page.

- During the switchover process, 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

1.16 Does Primary/Standby Switchover Have Impact on Services?

Primary/standby switchover may cause service interruption for some seconds or minutes (determined by the replication delay). If the primary/standby synchronization delay is too long, a small amount of data may get lost. To prevent traffic congestion, you are advised to perform switchover during off-peak hours.

1.17 Can Multiple ECSs Connect to the Same RDS DB Instance?

Multiple ECSs can connect to the same RDS DB instance as long as the capability limits of a database are not exceeded.

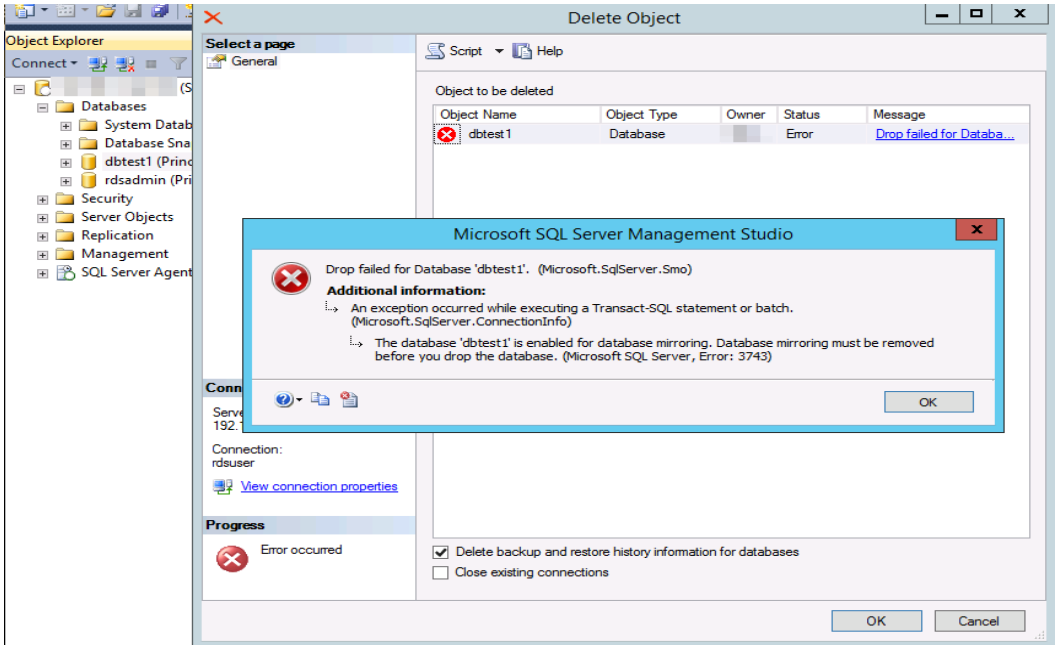
1.18 Why an Error is Reported When I Attempt to Delete a Database from RDS SQL Server Primary/Standby DB Instances?

Symptom

An error shown in **Figure 1-2** is reported on SQL Server Management Studio when a database is being deleted from RDS SQL Server primary/standby DB instances.

The database 'xxxx' is enabled for database mirroring.Database mirroring must be removed before you drop the database. Error: 3743

Figure 1-2 Error information



Possible Causes

According to the error information, the SQL Server DB instance type is primary/standby and database mirroring is enabled for the standby DB instance. As a result, the database cannot be deleted.

Solution

Before deleting the database, run the following commands to disable the mirroring:

Use master

go

ALTER DATABASE *[Database_Name]* **SET PARTNER OFF;**

GO

After the database mirroring is disabled, the database can be deleted.

1.19 Can Primary and Standby RDS DB Instances Be Deployed in the Same AZ?

An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. Some regions support both single AZs and multiple AZs and some only support single AZs.

To achieve higher reliability, RDS will automatically deploy your primary and standby instances in different physical servers even if you deploy primary and standby DB instances in the same AZ. If you attempt to create primary/standby DB instances in the same AZ in a Dedicated Computing Cluster (DCC) and there is only one physical server available, the creation will fail.

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 the same (default setting), the primary and standby DB instances are deployed in the same AZ.
- If they are different, the primary and standby DB instances are deployed in different AZs to ensure failover support and high availability.

1.20 Can I Set the Time Zone on RDS Databases?

Yes, you can set the time zone on the RDS console.

1.21 Can I Encrypt the Disk After Purchasing an RDS DB Instance?

Sorry, but you cannot. Once the DB instance is created, you cannot modify the disk encryption status or change the key. The backup data stored in OBS will not be encrypted.

To encrypt the disk for a created DB instance, you can restore the DB instance from the backup data to a new DB instance and then enable disk encryption for the new DB instance. Alternatively, use DRS to migrate data from the created DB instance to a DB instance with the disk encrypted.

1.22 Does RDS for MySQL Support Encryption Functions?

Yes. For the encryption functions supported by RDS for MySQL, visit **https://dev.mysql.com/doc/refman/5.7/en/encryption-functions.html**.

1.23 Does a Self-Built MySQL Database on an ECS Support Primary/Standby Replication?

Yes. You can use DRS to perform primary/standby replication by referring to **Real-Time Synchronization**.

1.24 Are There Any Restrictions After GTID Is Enabled for a MySQL DB Instance?

By default, GTID is enabled on RDS for 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. You can refer to **Upgrading the Minor Version** to upgrade the minor version.

1.25 Will Different RDS DB Instances Share CPU and Memory Resources?

No, RDS DB instances are independent from each other and will not share CPU and memory resources.

1.26 Does RDS Support 3-AZ Deployment?

So far, RDS does not support 3-AZ deployment.

A DB instance is the minimum management unit and an independently running database.

Table 1-3 DB instance types

DB Instance Type	Description
Single	Uses a single-node architecture and is more cost-effective than primary/standby DB instances.

DB Instance Type	Description
Primary/Standby	Uses an HA architecture with one master node and one slave node.
Read replica	Uses a single-node architecture (without a standby node).
Cluster	Uses the Microsoft Always On architecture with one master node, one slave node, and up to five read-only nodes. It features higher availability, reliability, and scalability.

2 Resource and Disk Management

2.1 How Do I View the Storage Space Occupied by My Database?

You can use the Data Admin Service (DAS) to view the storage space occupied by your database.

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** to go to the RDS console. The RDS console is displayed.

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

Alternatively, click the target DB instance on the **Instance Management** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

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

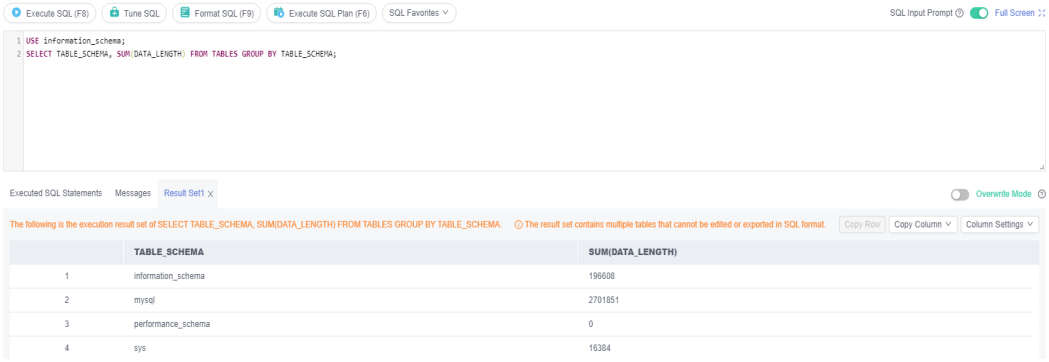
Step 6 On the top menu bar, choose **SQL Operations** > **SQL Window**.

Step 7 Run the following SQL statements in the SQL window to view the space occupied by your database. **Figure 2-1** shows the query result.

```
USE information_schema;

SELECT TABLE_SCHEMA, SUM(DATA_LENGTH) FROM TABLES GROUP BY TABLE_SCHEMA;
```


Figure 2-1 Execution result



----End

2.2 Which Types of Logs and Files Occupy RDS Storage Space?

The following logs and files occupy RDS storage space.

Table 2-1 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 2-2 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

Table 2-3 Microsoft SQL Server database file types

DB Engine	File Type
Microsoft SQL Server	Log files: database error log, transaction log, and trace files
	Data files: database content 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 due to a large number of sorting queries executed by applications.
   b. A large number of binlog files are generated and occupy space due to large amounts of add, delete, and modify operations in a short period.
   c. A large number of binlog files are generated due to 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.

2.3 Does RDS Support Scaling Down Storage Space of DB Instances?

No.

2.4 Which Items Occupy the Storage Space of My RDS DB Instances?

Both your common data (excluding backup data) and the data required for the operation of your DB instances (such as system database data, rollback logs, redo logs, and indexes) occupies the storage space on your purchased RDS DB instances. The following RDS log files also occupy storage space:

- Binlog log files generated by MySQL databases
- Logs files generated by PostgreSQL database servers
- Log files, including Microsoft SQL Server logs, default Microsoft SQL Server Trace logs, and Microsoft SQL Server Agent logs, generated by Microsoft SQL Server databases.

These files ensure the stable running of RDS DB instances.

2.5 What Overhead Does the Storage Space Have After I Applied for an RDS DB Instance?

The storage space you applied for will contain the system overhead required for inode, reserved block, and database operation.

2.6 How Much Storage Space Is Required for DDL Operations?

Data Definition Language (DDL) operations may increase storage space 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 10 GB greater than or equal to twice the size of the tablespace. For example, if your tablespace is 500 GB, ensure that storage space is greater than or equal to 1010 GB (500 GB x 2 + 10 GB).

2.7 How Do I Release DB Instances in Expired or Frozen State?

You can release resources in **Expired** or **Frozen** state as required.

For operation details, see **Releasing Resources**.

2.8 How Many DB Instances Can Run on RDS?

There are no limitations on the number of DB instances running on RDS.

2.9 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. A maximum of 0.5 million tables can be backed up. Excessive tables will generate errors. The backup speed is affected by the number of tables in a database.

- MySQL allows you to create numerous databases and tables. For details, see the official MySQL documentation.
- PostgreSQL allows you to create numerous databases and database accounts.
- Microsoft SQL Server allows you to create a maximum of 100 databases and numerous database accounts.

3 Database Connection

3.1 What Should I Do If I Fail to Connect to an RDS DB Instance?

Possible Causes

Locate the fault from the following aspects:

1. **Check whether the DB instance is available.**

   For example, if 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 connect to the DB instance:
   - 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.**

   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 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.

For 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 fail to be connected.

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.

8. **View the common connection error messages**

Find corresponding solutions based on connection error messages.

Fault Locating

Figure 3-1 Locating instance connection failures

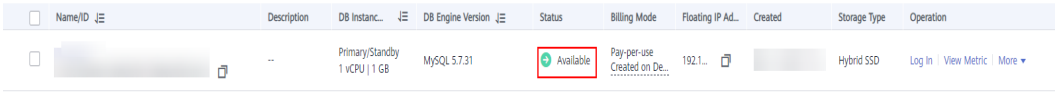
1. **Check whether the DB instance is available.**

   Check method: 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.

   Figure 3-2 Checking DB instance status



2. **Check whether the client connection is correct.**

   You are advised to install an **engine client** whose version is later than or equal to 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 3-1 Connection model

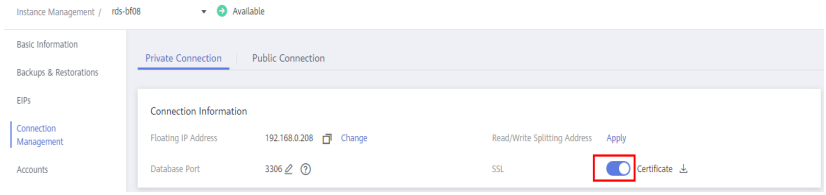
Connect Through	Scenarios	Example
Private network	A floating IP address is provided by default. If your applications are deployed on an ECS that is in the same region and VPC as the DB instance, you are advised to connect to the ECS and DB instance through a floating IP address.	Take MySQL as an example: **mysql -h** < *floating IP address* > **-P 3306 -u root -p --ssl-ca=/tmp/ca.pem**
Public network	If you cannot access the DB instance over a private (floating) IP address, you are advised to bind an EIP to the DB instance and then connect to the DB instance through the EIP. For EIP pricing details, see **EIP billing details**.	Take MySQL as an example: **mysql -h** < *EIP*> **-P 3306 -u root -p --ssl-ca=/tmp/ca.pem**

3. **Check the connection method.**

   - SSL connection is recommended. Enable SSL on the **Connection Management** page and upload the certificate to the ECS.

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

Figure 3-3 Enabling SSL



- Common connection: Disable SSL on the **Connection Management** page.

  mysql -h 172.16.0.31 -P 3306 -u root -p

4. **Check whether the parameters in the connection command are correct.**

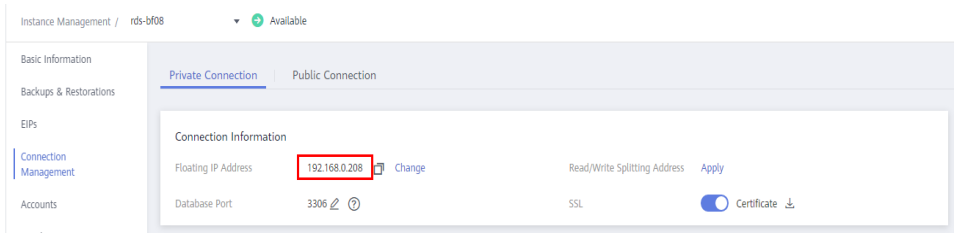
   Ensure that the connection address, port, username and password are correct, and try to connect to the DB instance again.

   If you use a private connection with SSL enabled, run the following example command: **mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem**. Obtain the parameters as follows:

   - Floating IP Address

     On the **Private Connection** tab of the **Connection Management** page, obtain the floating IP address in the **Connection Information** area.

     Figure 3-4 Floating IP address

   - Database Port

     On the **Private Connection** tab of the **Connection Management** page, obtain the database port in the **Connection Information** area.

   - Username and password

     Enter the username and password of the **root** user.

   - Certificate

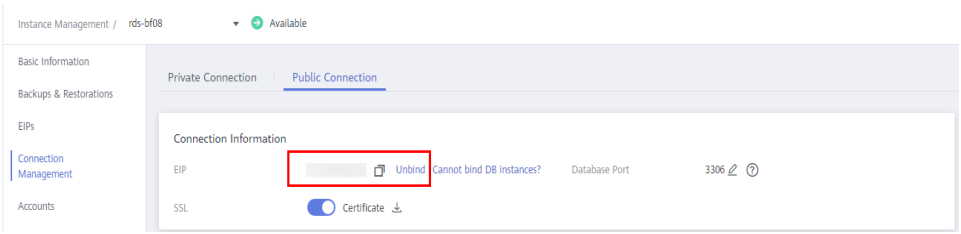
     Obtain the SSL certificate name from the directory where the command is executed.

   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**. Obtain the parameters as follows:

   - EIP

     On the **Public Connection** tab of the **Connection Management** page, obtain the EIP in the **Connection Information** area.

Figure 3-5 EIP



- Database Port

  On the **Public Connection** tab of the **Connection Management** page, obtain the database port in the **Connection Information** area.

- Username and password

  Enter the username and password of the **root** user.

- Certificate

  Obtain the SSL certificate name from the directory where the command is executed.

5. **Check whether the network connection is normal.**

   Private network connection

   a. Check whether the ECS and DB instance are in the same region and VPC.

      - If the ECS and DB instance are in different regions, they cannot communicate with each other. Select a region near to your service area to reduce network latency and experience faster access.
      - If the ECS and RDS DB instance are in different VPCs, see **What Should I Do If the ECS and RDS Are Deployed in Different VPCs and They Cannot Communicate with Each Other?**

   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.

      telnet *<IP address> <port number>*

      - If the connection is normal, the network is normal.
      - If the connection fails, **create a service ticket** to customer service for assistance.

   Public network connection

   a. Check security group rules.

      To access DB instances in a different security group from the ECS, **add an inbound rule** for the security group.

   b. Check network ACL rules.

      i. Go to the **Network ACLs**.

      ii. Check whether the NIC bound to the EIP is in the subnet associated with the network ACL.

      iii. Check whether the network ACL is enabled.

      If the network ACL is enabled, **add an ICMP rule to allow traffic**.

The default network ACL rule denies all inbound and outbound packets. After the network ACL is disabled, the default rule still takes effect.

c. Ping the ECSs in the same region to the DB instance.

If you cannot ping the EIP on the original ECS, select another ECS in the same region and ping the EIP again. If the ping is successful, the network is normal. If the ping failed, **create a service ticket**.

6. **Check whether the number of connections to the DB instance reaches the upper limit.**

Check method: Check whether the total connections and current active connections have reached the upper limit by referring to **View monitoring metrics**. If the maximum number of database connections specified in **What Is the Maximum Number of Connections to an RDS DB Instance?** has been reached, release unnecessary connections.

Possible cause: If there are excessive database connections, applications may fail to be connected, and the full and incremental backups may fail, affecting service running.

Solution:

a. Check whether applications are connected, optimize the connections, and release unnecessary connections.

b. 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 supported monitoring metrics, see **Configuring Displayed Metrics**.

c. If the DB instance specifications are too small, scale to larger specifications. For details, see **Changing DB Instance Specifications**.

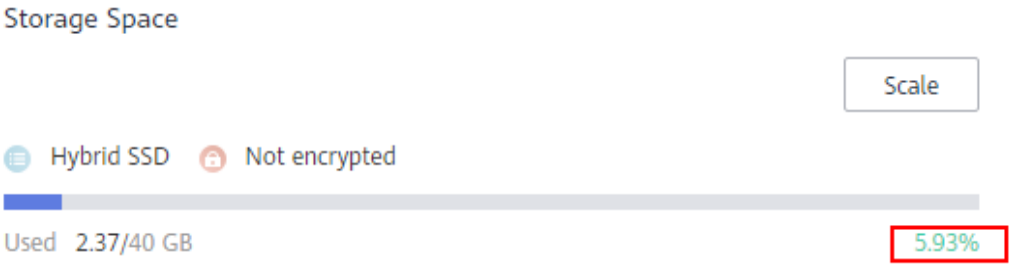
7. (Common) Check whether the DB instance is in the **Storage full** state.

Check method: View the storage space usage on the RDS console or Cloud Eye.

– On the RDS console

Click a DB instance to go to the **Basic Information** page. In the **Storage Space** area, view the storage space usage.

Figure 3-6 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.

Possible cause: When the DB instance status is **Storage full**, the DB instance needs to preserve at least 15% of its capacity to work properly.

Solution:

a. As your service data grows, the original storage space may be insufficient. You are advised to scale up storage space.

   For operation details, see **Scaling Up Storage Space**.

b. Shorten the local retention period of binlogs.

   For operation details, see **Setting a Local Retention Period for MySQL Binlogs**.

c. Process expired data files in a timely manner.

d. 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 supported monitoring metrics, see **Configuring Displayed Metrics**.

8. **View common connection error messages.**

   When you run commands to connect to a DB instance, the possible errors and and solutions are provided in the following:

   - ERROR 2013: Lost connection to MySQL server during query

     If the values of **wait_timeout** and **interactive_timeout** are too small, MySQL client will automatically disconnect the timeout empty connection. For details, see **MySQL Client Automatically Disconnected from a DB Instance**.

   - ERROR 1045 (28000): Access denied for user 'root'@'192.168.0.30' (using password:YES)

     Check whether the password is correct, whether the ECS has the permission to connect to the DB instance, and whether the MySQL client can ping the DB instance's floating IP address. For details, see **MySQL DB Instance Inaccessible**.

   - ERROR 1226 (42000): User 'test' has exceeded the 'max_user_connections' resource (current value:10)

     Check whether the number of connections to the DB instance is limited. For details, see **MySQL DB Instance Inaccessible**.

   - ERROR 1129 (HY000): Host '192.168.0.111' is blocked because of many connection errors; unblock with 'mysqladmin flush-hosts'

     Check whether the number of failed MySQL client connection attempts (not caused by incorrect passwords) exceeds the value of **max_connection_errors**. For details, see **MySQL DB Instance Inaccessible**.

   - [Warning] Access denied for user 'username'@'yourIp' (using password: NO)

If this error message is displayed when you attempt to connect to a MySQL or PostgreSQL DB instance, check whether the username or password is correct.

- [Warning] Access denied for user 'username'@'yourIp' (using password: YES)

  If this error message is displayed when you attempt to connect to a MySQL or PostgreSQL DB instance, check whether the username or password is correct.

- Login failed for user 'username'

  If this error message is displayed when you attempt to connect to a Microsoft SQL Server DB instance, check whether the username or password is correct.

9. If the problem persists, **create a service ticket**.

3.2 Can an External Server Access the RDS Database?

DB Instance Bound with an EIP

For a DB instance that has been bound with an EIP, you can access it through the EIP.

For operation details, see:

- **Connecting to a DB Instance Through a Public Network**
- **Connecting to a DB Instance Through a Public Network**
- **Connecting to a DB Instance Through a Public Network**

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.

For operation details, see:

- **Connecting to a DB Instance Through a Public Network**
- **Connecting to a DB Instance Through a Public Network**
- **Connecting to a DB Instance Through a Public Network**

3.3 How Do I Troubleshoot 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 service running.

Fault Locating

1. Check whether applications are connected, optimize the connections, and release unnecessary connections.
2. Check whether the specifications are small and scale them as needed.
3. 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, see the *Cloud Eye User Guide*.

3.4 What Is the Maximum Number of Connections to an RDS DB Instance?

RDS does not have constraints on the number of connections. This number is determined by the default value and value range of the DB engine. For example, you can set **max_connections** and **max_user_connections** in a parameter template to configure the maximum number of connections for an RDS MySQL DB instance.

For more information, see the number of connections supported by each specification in the **Relational Database Service Performance White Paper**.

About max_connections

The max_connections is closely related to storage space (unit: GB) of the DB instance.

Estimated 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 3-2 Max_connections for different memory specifications

Memory (GB)	Connections
512	100,000
384	80,000
256	60,000
128	30,000

Memory (GB)	Connections
64	18,000
32	10,000
16	5,000
8	2,500
4	1,500
2	800

3.5 How Can I Create and Connect to an ECS?

1. For details about how to create an ECS, see the *Elastic Cloud Server User Guide*.
   - The ECS is used for connecting to an RDS DB instance and must be located in the same VPC as the RDS DB instance.
   - Configure a correct security group to allow the ECS to access the RDS DB instance through the private address.
2. For details on how to connect to the ECS, see the "Logging in to an ECS" section in the *Elastic Cloud Server User Guide*.

3.6 What Should I Do If an ECS Cannot Connect to an RDS DB Instance?

Perform the following steps to identify the problem:

Step 1 Check whether the ECS and RDS DB instance 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 a security group has been added to the ECS.

- If a security group has been added, check whether its configuration rules are suitable.

  For MySQL DB instances, see the security group description in **Buying an RDS MySQL DB Instance**. Then, go to **Step 3**.

  For PostgreSQL DB instances, see the security group description in **Buying an RDS PostgreSQL DB Instance**. Then, go to **Step 3**.

  For Microsoft SQL Server DB instances, see the security group description in **Buying an RDS Microsoft SQL Server DB Instance**. Then, go to **Step 3**.
- If no security group has been added, go to the VPC console from the ECS details page and click **Security Groups** to add a security group.

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**.

The default RDS for Microsoft SQL Server port number is **1433**.

```
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.
- If the ECS cannot connect to the port, contact technical support.

Step 4 If you originally use the common connection and later change the SSL connection for security reasons, you should use the SSL login. Otherwise, the following error will be reported:

mysql: [Warning] Using a password on the command line interface can be insecure.

ERROR 2026 (HY000): SSL connection error: protocol version mismatch

Check whether the connection mode is a common connection or an SSL connection.

If you use the SSL connection, check whether the SSL connection is enabled.

For details about a common connection and an SSL connection, see **Connecting to a DB Instance**.

----End

3.7 What Should I Do If a Database Client Problem Causes a Connection Failure?

Identify an RDS connection failure caused by a client problem from the following aspects.

1. ECS Security Policy

   In Windows, check whether the RDS instance port is enabled in the Windows security policy. In Linux, run the **iptables** command to check whether the RDS DB 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. Incorrect User Name or Password

   Check whether the user name 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)
   - Login failed for user 'username'

NOTE

If the problem persists, contact post-sales technical support.

3.8 What Should I Do If an RDS Database Problem Causes a Connection Failure?

Check whether any of the following problems occur on the RDS DB instance.

1. The RDS DB instance is not properly connected.

   Solution: Check the connection. The RDS DB instance must be accessed only through an ECS in the same VPC.

2. The maximum number of connections has been reached.

   Solution: Check whether the CPU usage and the number of current connections are normal by using the RDS resource monitoring function. If either of them reaches the maximum, reboot, disconnect, or scale up the specifications of the DB instance.

3. 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.

3.9 How Do My Applications Access an RDS DB Instance in a VPC?

Ensure that the ECS in which your applications are located is in the same VPC as the RDS DB instance. If the ECS and the RDS DB instance are in different VPCs, modify the VPC route table and network access control list (ACL) to ensure that the ECS can access the RDS DB instance.

3.10 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.

In addition, you are advised to set your applications to connect to the database using a long connection to reduce resource consumption and improve performance.

3.11 How Can I Connect to a MySQL Database Through JDBC?

If you are connecting to a MySQL database through Java database connectivity (JDBC), the SSL certificate is optional. For security reasons, you are advised to

download the SSL certificate to encrypt the connection. SSL is disabled by default for MySQL DB instances. You can enable SSL by referring to **Configuring an SSL Connection**. SSL encrypts connections to databases but it increases the connection response time and CPU usage. Therefore, you are advised not to enable SSL.

Prerequisites

You must be familiar with:

- Computer basics
- Java programming language
- JDBC basic knowledge

Connection with the SSL Certificate

NOTE

The JDBC connection is an SSL connection. The SSL certificate needs to be downloaded and verified for 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 MySQL DB instance through JDBC.

jdbc:mysql://*<instance_ip>*:*<instance_port>*/*<database_name>*?**sslmode=verify-full&sslrootcert=***<ca.pem>*

Table 3-3 Parameter description

Parameter	Description
<instance_ip>	If you are accessing the RDS DB instance through an ECS, ***instance_ip*** indicates the floating IP address displayed on the **Basic Information** page of the DB instance to which you intend to connect.
	If you are accessing the RDS DB instance through an EIP, ***instance_ip*** indicates the EIP that has been bound to the DB instance.
<instance_port>	Indicates the database port displayed on the **Basic Information** page. The default port is **3306**.
<database_name>	Indicates the name of the database to which you intend to connect. The default database name is **mysql**.
sslmode	Indicates the SSL connection mode. The default mode is verify-full.
sslrootcert	Indicates 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;
import java.sql.SQLException;

public class MyConnTest {
    final public static void main(String[] args) {
        Connection conn = null;
         Statement stat = null;
        // set sslmode here.
        // with ssl certificate and path.
        String url = "jdbc:mysql://192.168.0.225:3306/my_db_test?sslmode=verify-
full&sslrootcert=/home/Ruby/ca.pem";

        try {
            Class.forName("com.mysql.jdbc.Driver");
            conn = DriverManager.getConnection(url, "root", "password");
            System.out.println("Database connected");

            Statement stmt = conn.createStatement();
              String sql = "SELECT * FROM mytable WHERE columnfoo = 500";
            ResultSet rs = stmt.executeQuery sql);
            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

The JDBC connection is an SSL connection, but 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 MySQL DB instance through JDBC.

jdbc:mysql://*<instance_ip>*:*<instance_port>*/*<database_name>***?sslmode=require**

Table 3-4 Parameter description

Parameter	Description
<instance_ip>	If you are accessing the RDS DB instance through an ECS, ***instance_ip*** indicates the floating IP address displayed on the **Basic Information** page of the DB instance to which you intend to connect.

Parameter	Description
	If you are accessing the RDS DB instance through an EIP, ***instance_ip*** indicates the EIP that has been bound to the DB instance.
<instance_port>	Indicates the database port displayed on the **Basic Information** page. The default port is **3306**.
<database_name>	Indicates the name of the database to which you intend to connect. The default database name is **mysql**.
sslmode	Indicates the SSL connection mode. **require** indicates that data needs to be 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:mysql://192.168.0.225:3306/my_db_test?sslmode=require";
        try {
            Class.forName("com.mysql.jdbc.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

3.12 How Can I Connect to a PostgreSQL Database Through JDBC?

If you are connecting to a PostgreSQL database through Java database connectivity (JDBC), the SSL certificate is optional. For security reasons, you are advised to download the SSL certificate to encrypt the connection.

Prerequisites

You must be familiar with:

- Computer basics
- Java programming language
- JDBC basic knowledge

Obtaining and Using JDBC

- JDBC driver download address: **https://jdbc.postgresql.org/download.html**
- JDBC Interface: **https://jdbc.postgresql.org/documentation/head/index.html**

Connection with the SSL Certificate

NOTE

The JDBC connection is an SSL connection. The SSL certificate needs to be downloaded and verified for 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 PostgreSQL DB instance through JDBC.

jdbc:postgresql://*<instance_ip>***:***<instance_port>***/***<database_name>***?sslmode=verify-full&sslrootcert=***<ca.pem>*

Table 3-5 Parameter description

Parameter	Description
<instance_ip>	If you are accessing the RDS DB instance through an ECS, ***instance_ip*** indicates the floating IP address displayed on the **Basic Information** page of the DB instance to which you intend to connect.
	If you are accessing the RDS DB instance through an EIP, ***instance_ip*** indicates the EIP that has been bound to the DB instance.
<instance_port>	Indicates the database port number displayed on the **Basic Information** page. The default port number is **5432**.

Parameter	Description
<database_name>	Indicates the name of the database to which you intend to connect. The default database name is **postgres**.
sslmode	Indicates the SSL connection mode. The default mode is verify-full.
sslrootcert	Indicates 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

The JDBC connection is an SSL connection, but 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 PostgreSQL DB instance through JDBC.

jdbc:postgresql://*<instance_ip>***:***<instance_port>***/***<database_name>***?sslmode=disable**

Table 3-6 Parameter description

Parameter	Description
<instance_ip>	If you are accessing the RDS DB instance through an ECS, ***instance_ip*** indicates the floating IP address displayed on the **Basic Information** page of the DB instance to which you intend to connect.
	If you are accessing the RDS DB instance through an EIP, ***instance_ip*** indicates the EIP that has been bound to the DB instance.
<instance_port>	Indicates the database port number displayed on the **Basic Information** page. The default port number is **5432**.
<database_name>	Indicates the name of the database to which you intend to connect. The default database name is **postgres**.
sslmode	Indicates the SSL connection mode. **disable** indicates that 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

3.13 Why Can't 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 **Instance Management** 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.

   Table 3-7 Security group rules

Direction	Type	Protocol/Port Range	Source IP Address
Inbound	IPv4	Any: Any	0.0.0.0/0 0.0.0.0/0 indicates all IP addresses.
Inbound	IPv4	ICMP: Any	0.0.0.0/0 0.0.0.0/0 indicates all IP addresses.

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. After 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 such a case, contact customer service for technical support.

3.14 How Can I Obtain the IP Address of an Application?

Scenarios

EIPs obtained through tools are inaccurate. Therefore, applications may fail to be connected to DB instances even though you have added IP addresses to a whitelist. This section describes how to obtain IP addresses of applications.

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 MySQL DB instance.

mysql -h *host_name* **-P** *port* **-u** *username* **-p**

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

Enter password:

For example, 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 3-7 shows the query result. The outbound IP address is the host IP address in the "show processlist" row of the Info field.

Figure 3-7 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)
```

----End

3.15 What Should I Do If an RDS Microsoft SQL Server DB Instance Failed to Be Connected?

Fault Location

- Check whether the ECS can connect to the RDS DB instance.

  If the ECS cannot connect to the RDS DB instance, check whether the ECS and RDS DB instance are located in the same VPC and security group.
- Check whether the IP address and port number are correct.

  Use a colon to separate an IP address and a port number.
- Check whether the RDS service is running properly.
- Check whether the username and password are correct. You can reset the password.
- Reboot the RDS DB instance and check whether it can be connected through an ECS.

Solution

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 **Basic Information** and **Backups & Restorations** pages, check connection and backup information.

Step 5 On the **Basic Information** page, check the administrator.

Step 6 Download an SQL Server Management Studio installation package and install it on an ECS.

Step 7 Connect to the RDS DB instance through an ECS.

----End

3.16 What Can I Do If the Connection Test Failed?

Fault Location

1. Check security group rules.
2. Check network ACLs.
3. Check the NIC information of ECSs.
4. Check the disconnected ports.

Solution

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 **Connection Information** area on the **Basic Information** page, view the VPC where the RDS DB instance is located.

Step 5 Check whether the RDS DB instance to which distributed transactions are added is in the same VPC as ECS.

- If they are in the same VPC, see **What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs?**
- If they are in different VPCs:
  - Public access: Bind an EIP to the DB instance by referring to **Binding and Unbinding an EIP**.
  - Private access: Create a VPC peering connection by referring to **VPC Peering Connection Overview** to establish a network connection between two VPCs.
  - Change the VPC hosting the ECS to the same as that hosting the RDS by referring to **Changing a VPC**.

----End

3.17 Can I Access an RDS DB Instance Over an Intranet Across Regions?

Sorry, but you cannot. RDS DB instances in different regions cannot communicate with each other over an intranet. For low network latency and quick resource access, select the nearest region.

3.18 Is an SSL Connection to a DB Instance Interrupted After a Primary/Standby Switchover or Failover Occurs?

For DB instances connected through SSL, a primary/standby switchover or failover does not interrupt the connection because the SSL certificate is still valid for both the primary and standby DB instances.

3.19 Can RDS DB Instances in Different VPCs Communicate with Each Other Over an Intranet?

No, they can't.

You can use VPC peer connections to enable communication over an intranet. For details, see **VPC Peering Connection Creation Procedure**.

3.20 Whether the Bandwidth Is Limited When an ECS Connects to an RDS DB Instance?

No, the bandwidth is not limited.

3.21 Are There Any Potential Risks If There Are Too Many Connections to MySQL DB Instances?

If there are a large number of MySQL connections, the service side may fail to connect to databases, and the full and incremental backups of DB instances may fail, affecting service running.

Solution

1. Check whether the service side is connected to databases, optimize the instance connections, and release unnecessary connections.
2. Cloud Eye monitors database metrics, such as the CPU, memory, storage usage, and number of connections, and allows you to set alarm policies to identify risks in advance if any alarms are generated.

3.22 Does MySQL Support SSL Connections?

MySQL supports SSL connections. Different from other vendors, RDS for MySQL enables the SSL connection on the database server by default. When you use a client to connect to MySQL DB instances, you can determine whether to enable SSL as required.

For details about SSL, see **Connecting to a DB Instance Through a Public Network**.

3.23 Why Does the New Password Not Take Effect After I Reset the Administrator Password?

Possible Causes

You reset the administrator password after the backup is created. Therefore, the original administrator password takes effect after data is restored from the backup.

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 **Resetting the Administrator Password**.

3.24 Does RDS Have Restrictions on the Frequency of Querying Connections?

No.

3.25 Does RDS for SQL Server Support Periodic Password Changes?

No, RDS for SQL Server does not support periodic password changes.

You can change the password by **resetting the password**.

3.26 Shall I Be Logged Out After the Connection to SQL Server Timed Out?

No, you won't be logged out after the connection timed out. You can modify the **remote query timeout** parameter by referring to **Modifying Parameters** to adjust the duration a remote operation can take before SQL Server times out.

3.27 How Do I Set the Encoding Format to Connect to the MySQL 8.0 Character Set?

Solution

1. Set **character_set_server** to **utf8** and **collation_server** to **utf8_general_ci**.
2. If the client uses PHP 7.1.x, it will fail to connect to the utf8mb4 character set of MySQL 8.0. You are advised to use another PHP version.

3.28 What Should I Do If the ECS and RDS Are Deployed in Different VPCs and They Cannot Communicate with Each Other?

Solution

1. Change the VPC hosting the ECS to the same as that hosting the RDS by referring to **Changing a VPC**.
2. Create a VPC peering connection by referring to **VPC Peering Connection Overview**.

3.29 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;

3.30 Can I Access Standby RDS DB Instances?

Sorry, you can't. 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.

3.31 How Do I Implement Fine-Grained Permission Control on RDS Access?

You can implement fine-grained permission control on RDS access by referring to **Creating a Custom Policy**.

3.32 What Should I Do If No EIPs Are Available When I'm Attempting to Bind an EIP?

The possible cause is that all available EIPs have been bound to other applications. You can unbind an EIP by referring to **Binding and Unbinding an EIP** or purchase a new EIP.

4 Database Migration

4.1 Why Do I Need to Use the mysqldump and 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. Therefore, use these tools when the data amount is small or if the server is allowed to stop for a long period of time, during which the data can be migrated.

RDS is compatible with original 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.

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 MySQL instance migration, a large number of binlog files are generated in a short period of time. As a result, the data disk space is insufficient (91%), affecting service running.

Solution

1. Clear expired data in a timely manner.
2. As your service data grows, the original storage space may be insufficient. You are advised to scale up storage space.

   For operation details, see **Scaling Up Storage Space**.
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 if any alarms are generated.

   For operation details, see **Configuring Displayed Metrics**.

4.3 Does RDS Support Cross-Region Migration?

You can use the Data Replication Service (DRS) to migrate databases across regions on the cloud.

On the **Instance Management** page, click the target DB instance. On the displayed **Basic Information** page, click **Migrate Database** in the upper right corner of the page.

For more information, see **Real-Time Migration** in the *Data Replication Service User Guide*.

4.4 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.

  Data cannot be exported or imported between heterogeneous databases due to different data formats. However, if the data formats are compatible, table data can also be imported theoretically.

  Generally, third-party software is 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 in .txt format. Then, you can use Load statements to import the exported table records to the DB engines supported by RDS.

4.5 How Many Migration Methods Does RDS for MySQL Support?

RDS for MySQL supports the following two data migration methods:

- Using mysqldump. For details, see **Migrating Data to RDS for MySQL Using mysqldump**
- Using DRS. You can migrate on-premises databases to RDS for MySQL by performing the following:

  On the **Instance Management** page, click the target DB instance. On the displayed **Basic Information** page, click **Migrate Database** in the upper right corner of the page.

  For more information, see **Before You Start** in the *Data Replication Service User Guide*.

5 Database Permission

5.1 Why Does the Root User Not Have the Super Permission?

Most relational database cloud service platforms do not provide the super permission for the **root** user. The super permission allows users to execute many management commands, such as reset master, set global, kill, and reset slave. These operations may cause primary/standby replication errors. To ensure stable running of DB instances, RDS does not provide the super permission for the **root** user.

If you require the super permission, RDS can provide service capabilities or use other methods to bypass the super permission constraints.

For example:

1. You cannot run the following command on a database to modify parameter values. You can modify parameter values only on the RDS console.

   set global parameter name=*Parameter value*;

   If the script contains the **set global** command and causes the super permission loss, delete the **set global** command and modify parameter values through the RDS console.

2. An error is reported after you run the following command because the **root** user does not have the super permission. You can delete **definer='root'** from the command to solve the problem.

   create definer='root'@'%' trigger(procedure)...

   You can import data using mysqldump. For operation details, see **Migrating MySQL Data Using mysqldump**.

3. You can create PostgreSQL plugins by referring to **Managing a Plugin**.

5.2 How Do I Grant the RDS FullAccess Permission to a Sub-user?

RDS FullAccess is a region-level permission. You need to assign permissions for region-specific projects.

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, you need to switch to a region where you have been authorized to use RDS.

5.3 RDS System Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions. For details about RDS system permissions, see **Table 5-1**.

Table 5-1 RDS system policies and permissions

Policy Name/ System Role	Scope	Permission Description	Permission Type	Dependency
RDS FullAccess	Region-specific projects	Full permissions for RDS	Policy	None
RDS ReadOnlyAccess		Read-only permissions for RDS		None
RDS ManageAccess		Database administrator permissions for all operations except deleting RDS resources		None
RDS Administrator		Full permissions for RDS	Role	This role must be used together with the Tenant Guest and Server Administrator roles in the same project.

5.4 Does RDS for MySQL Support Multiple Accounts?

Yes, RDS for MySQL supports multiple accounts. Users can assign different rights to these accounts through authorization commands to control access to different tables. Each table is independent of each other.

Performance is not affected when multiple accounts access tables. Concurrent access of multiple sessions increases system resource overhead. For details, see the number of connections in **MySQL 5.7 Test Data**.

For more details about MySQL permissions, see official **MySQL documents**.

5.5 What Are the Differences Between RDS ManageAccess and DAS Permissions?

Permission	Description
RDS ManageAccess	Permissions used to manage RDS DB instances
DAS permissions	Permissions used on Data Admin Service (DAS). DAS enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency.

5.6 Can Multiple Users Log in to DAS at the Same Time? Will the Passwords Be Locked If I Entered Wrong Passwords for Several Consecutive Times?

Multiple users can log in to DAS at the same time. The passwords will not be locked after several failed attempts.

If you forget the password of your database account when using RDS, you can reset the password. On the **Instance Management** page of the RDS console, locate the target DB instance and choose **More** > **Reset Password** in the **Operation** column.

5.7 How Do the Login Name Permissions of RDS for SQL Server 2017 Enterprise Edition Primary/Standby DB Instances Synchronized to Its Read Replicas?

- The Login Name permissions created by the primary DB instance are automatically synchronized to read replicas every minute. Wait for about one minute until the synchronization is complete, you can use the Login Name permission or changing password permission on read replicas.

- You can add, delete, or modify the Login Name on read replicas because the Login Name permissions are automatically synchronized to read replicas every minute. The additional Login Names and permissions on the read replicas are not deleted due to the time difference. You can delete them from read replicas manually.
- If a database account exists on both the primary DB instance and replicas, the account password is synchronized to read replicas from the primary instance. Changing the Login Name permissions on read replicas will not take effect.

5.8 After a Primary Instance Account Is Deleted and Recreated on RDS for SQL Server, Will the Permissions Be Automatically Synchronized?

Yes. After a primary instance account is deleted and recreated on RDS for SQL Server, permissions and modifications on the primary instance will be automatically synchronized to the standby DB instance and read replicas.

6 Database Storage

6.1 Does RDS for MySQL Support TokuDB?

Currently, the official MySQL does not support TokuDB.

Therefore, RDS for MySQL does not support TokuDB, either.

6.2 Is RDS for MySQL Compatible with MariaDB?

MariaDB is a branch of the MySQL source code. It is maintained by the open source community and uses the GPL authorization. One of the reasons for developing MariaDB is that Oracle has acquired MySQL and has a potential risk of shutting down MySQL. Therefore, the community develops MariaDB to avoid this risk.

MariaDB is compatible with MySQL. There is no difference for front-end applications such as PHP, Perl, Python, Java, .NET, MyODBC, Ruby, and MySQL C connector.

6.3 What Storage Engines Does the RDS for MySQL Support?

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.

For MySQL databases, only the InnoDB storage engine supports backup and restoration functions and is therefore recommended.

For versions later than MySQL 5.6.40 and 5.7.22, some storage engines are no longer supported.

RDS for MySQL now does not support MyISAM due to the following reasons:

- MyISAM engine tables do not support transactions and support only table-level locks. As a result, read and write operations conflict with each other.

- MyISAM has a defect in protecting data integrity, which may cause database data damage or even data loss.
- If data is damaged, MyISAM does not support data restoration provided by RDS for MySQL and requires manual restoration.
- Data can be transparently migrated from MyISAM to InnoDB, which does not require code modification for tables.

RDS for MySQL now does not support FEDERATED due to the following reasons:

- Same DML operations are repeatedly executed on remote databases, causing data disorder.
- During the PITR restoration, data on remote databases is not restored to the status when the full backup is created after the full restoration phase is complete. Applying data during the incremental restoration will disorder FEDERATED table data.

RDS for MySQL now does not support MEMORY due to the following reasons:

- If a memory table becomes empty after a restart, the database generates a DELETE event to the binlog when the table is opened. If primary/standby DB instances use memory tables and the standby database (or read-only database) is restarted, a GTID is generated, which is inconsistent with that of the primary database. As a result, the standby database is rebuilt.
- Using memory tables may cause out-of-memory (OOM) and even service termination.

6.4 What Is the RDS DB Instance Storage Configuration?

RDS uses EVS disks for data storage. For EVS details, see *Elastic Volume Service User Guide*.

The RDS DB instance backup data is stored in OBS and does not occupy the database storage space. For details on the RDS DB instance storage configuration, see the *Object Storage Service User Guide*.

6.5 Does RDS for MySQL Support Stored Procedures and Functions?

Yes.

1. Stored procedures and functions are a set of SQL statements that have been compiled and stored in databases. Invoking stored procedures and functions reduces data transmission between databases and application servers, and improves data processing efficiency.
2. 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 Can I Change the Storage Type of an RDS DB Instance from Common I/O to Ultra-high I/O?

No. After an RDS DB instance is created, the storage type cannot be changed.

Table 6-1 Items that cannot be changed

Item	Change Direction
Storage type	• From common I/O to ultra-high I/O • From ultra-high I/O to common I/O • From high I/O to common I/O The preceding descriptions are examples only. The storage type cannot be changed.

6.7 Why Does My Primary RDS DB Instance Become Read-Only?

If your storage space usage reaches up to 95% of the total storage, your primary RDS DB instance becomes read-only automatically. It becomes readable and writable after the storage space usage is less than 85% of the total storage. For details about the causes and solutions of insufficient storage space, see **What Should I Do If My Data Exceeds the Database Storage Space of an RDS DB Instance?**

6.8 What Should I Do If My Data Exceeds the Database Storage Space of an RDS DB Instance?

Scenario

The database storage space of an RDS DB instance is exhausted, and applications cannot read data from or write data to databases, interrupting services.

Cause

1. Data occupies a great amount of storage space.
2. A large number of binlog files are generated due to a large number of transactions and write operations.
3. A large number of temporary files are generated due to a large number of sorting queries executed by applications.

Solution

1. 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.
2. If binlog files occupy too much storage space, contact technical support to delete local binlog files to release storage space.
3. If temporary files generated by sorting queries occupy too much storage space, optimize your SQL query statements.
4. If the preceding solutions are invalid, implement database and table sharding.

7 Database Performance

7.1 What Should I Do When the CPU Usage of My RDS MySQL DB Instance Is High?

If the CPU usage is high or close to 100% when you use RDS for MySQL, data read/write processing is slow, connections cannot be obtained, and errors are reported, affecting your service running.

Solution

1. View the slow SQL logs to check whether any slowly executed SQL queries exist and view their performance characteristics (if any) to locate the cause.

   For details on viewing MySQL logs, see section **Viewing and Downloading Slow Query Logs**.
2. View the CPU usage metric of your RDS DB instance to facilitate problem locating.

   For details, see **Configuring Displayed Metrics**.
3. Create read replicas to offload read pressure on primary DB instances.
4. When multiple associated tables are queried, indexes must be created for the associated fields.
5. Do not use the SELECT statement to scan all tables. You can specify fields or add the where condition.
6. You can use the Data Admin Service (DAS) to identify SQL statements that are executed frequently, consume a large amount of resources, or take a long time to execute. You can optimize the database according to the diagnosis suggestions to ensure the stability of the database performance.

   For details, see **SQL Tuning**.

7.2 What Should I Do If an RDS DB Instance Is Abnormal Due to Full Storage Space?

You can scale up storage space if it is no longer sufficient for your requirements. If the DB instance is in the **Storage full** status and data cannot be written to the database, the DB instance will be abnormal, affecting service running.

Solution

1. As your service data grows, the original storage space may be insufficient. You are advised to scale up storage space.

   For operation details, see **Scaling Up Storage Space**.
2. Shorten the local retention period of binlogs.

   For operation details, see **Setting a Local Retention Period for MySQL Binlogs**.
3. Process expired data files in a timely manner.
4. Cloud Eye monitors database metrics, such as the CPU, memory, storage usage, and number of connections, and allows you to set alarm policies to identify risks in advance if any alarms are generated.

   For operation details, see **Configuring Displayed Metrics**.

7.3 What Is the Maximum Number of IOPS Supported by RDS?

The IOPS supported by RDS depends on the I/O performance of EVS disks. For details, see **Disk Types and Disk Performance** in the *Elastic Volume Service Product Introduction*.

7.4 How Do I Improve the Query Speed of My RDS Database?

The following are some suggestions provided for you to improve the database query speed:

- View the slow query logs to check whether any slowly executed SQL queries exist and view their performance characteristics (if any) to locate the cause.
- View the CPU usage of your RDS DB instance to facilitate problem locating.
- Create read replicas to offload read pressure on the primary DB instance.
- Add indexes for associated fields in multi-table association queries.
- Specify a field or add a where clause, avoiding full table scanning through the SELECT statement.

8 Client Installation

8.1 How Can I Install the MySQL Client?

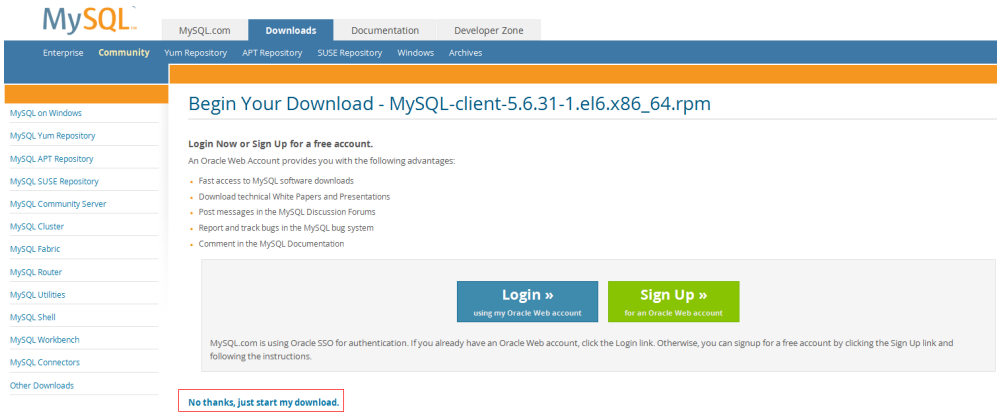
MySQL provides client installation packages for different OSs on its official website. MySQL 5.6 is used as an example. Click **here** to download the MySQL 5.6 client installation package or click **here** to download other versions of the packages. The following procedure uses Red Hat Linux OS as an example to illustrate how to obtain the required installation package and install the MySQL client.

Procedure

Step 1 Obtain the installation package.

Find the **link** to the required version on the download page. MySQL-client-5.6.31-1.el6.x86_64.rpm is used as an example in the following figure.

Figure 8-1 Procedure



NOTE

Click **No thanks, just start my download.** to download the installation package.

Step 2 Upload the installation package to the ECS.

NOTE

When you create an ECS, select an OS, such as Red Hat 6.6, and bind an EIP to it. Then, upload the installation package to the ECS using a remote connection tool, and use PuTTY to connect to the ECS.

Step 3 Run the following command to install the MySQL client:

```
sudo rpm -ivh MySQL-client-5.6.31-1.el6.x86_64.rpm
```

NOTE

- If any conflicts occur during the installation, add the **replacefiles** parameter to the command and try to install the client again. Example:
  ```
  rpm -ivh --replacefiles MySQL-client-5.6.31-1.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-5.6.31-1.el6.x86_64.rpm
  ```

----End

8.2 How Can I Install the PostgreSQL Client?

PostgreSQL provides **client installation packages** and the required dynamic shared library packages for different OSs on its official website.

RDS for PostgreSQL provides the **client installation package** of PostgreSQL Enhanced Edition 11 and the **installation package of dynamic shared library**. Use the client to connect to Enhanced Edition DB instance.

NOTICE

Ensure that the database client matches the DB engine version of your RDS PostgreSQL DB instances.

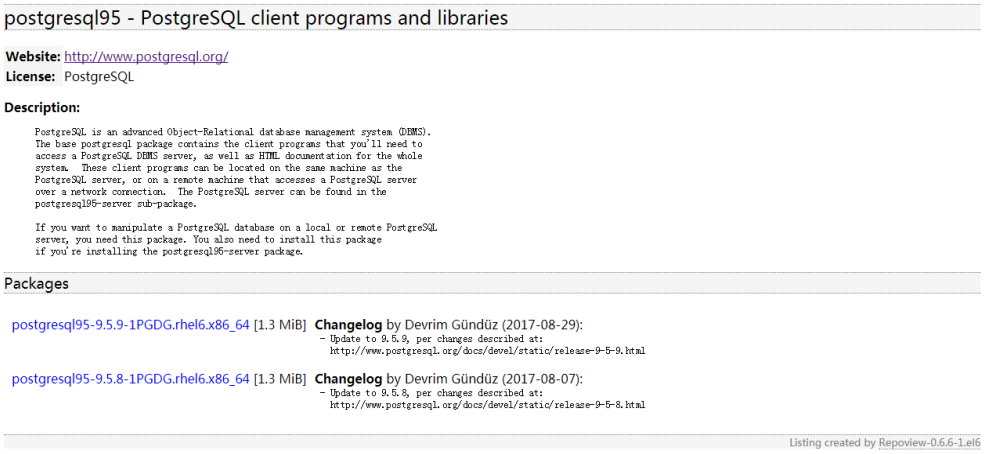
This following uses latest **PostgreSQL 9.5** in Red Hat Linux 6 as an example to describe how to obtain the required installation package and complete the installation.

Procedure

Step 1 Obtain the PostgreSQL client installation package.

Find the **link** to the required version on the download page. postgresql95 is used as an example in the following figure.

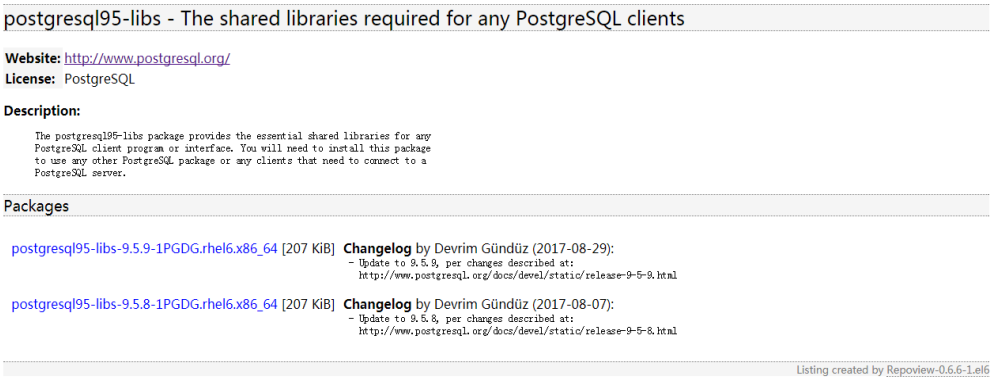
Figure 8-2 Downloading the PostgreSQL client installation package



Step 2 Obtain the dynamic shared library package required for the PostgreSQL client.

Find the **link** to the required version on the download page. postgresql95-libs is used as an example in the following figure.

Figure 8-3 Downloading the dynamic shared library package



Step 3 Upload the installation and dynamic shared library packages to the ECS.

NOTE

When you create an ECS, select an OS, such as Red Hat 6.6, and bind an EIP to it. Then, upload the installation and dynamic shared library packages to the ECS using a remote connection tool, and use PuTTY to connect to the ECS.

Step 4 Run the following command to install the PostgreSQL client:

```
sudo rpm -ivh postgresql95-9.5.7-1PGDG.rhel6.x86_64.rpm postgresql95-libs-9.5.7-1PGDG.rhel6.x86_64.rpm
```

NOTE

- If any conflicts occur during the installation, add the **replacefiles** parameter to the command and try to install the client again. Example:
  ```
  rpm -ivh --replacefiles postgresql95-9.5.7-1PGDG.rhel6.x86_64.rpm postgresql95-libs-9.5.7-1PGDG.rhel6.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 postgresql95-9.5.7-1PGDG.rhel6.x86_64.rpm postgresql95-libs-9.5.7-1PGDG.rhel6.x86_64.rpm
  ```

----End

8.3 How Can I Install SQL Server Management Studio?

The Microsoft SQL Server official website provides the SQL Server Management Studio installation package. SQL Server Management Studio applications can run in the Windows OS only.

Procedure

Step 1 Obtain the SQL Server Management Studio installation package.

Visit the **Microsoft website** and download the installation package, for example, download the installation package of SQL Server Management Studio 18.0.

Step 2 Upload the installation package to the ECS.

Step 3 Double-click the installation package and complete the installation as instructed.

----End

9 Backup and Restoration

9.1 How Long Does RDS Store Backup Data?

Automated backup data is kept based on the backup retention period you specified. There is no limit on the manual backup retention period. You can delete manually backup files as needed.

The backup data is stored in OBS and does not occupy the database storage space.

9.2 Where Are RDS Backup Files Stored?

RDS backup files are stored in OBS and do not occupy the database storage space. RDS provides free backup storage space of the same size as your purchased storage space. You can download the backup data on the RDS console.

For more information about the storage configuration, see the *Object Storage Service User Guide*.

9.3 Can My Database Be Used in the Backup Window?

A backup window is a user-specified time segment during which backup of RDS DB instances is performed. With these periodic data backups, RDS allows you to restore DB instances to the backups during a retention period. This backup process does not affect services. However, you cannot reboot DB instances on the RDS console.

9.4 How Is RDS for MySQL Backup Data Charged?

All the RDS full and incremental backup data is stored in OBS. RDS provides free backup storage space of the same size as your purchased storage space. For example, if the storage space you selected when buying a DB instance is 200 GB, charging initiates only after the backup storage space usage exceeds 200 GB. The first 200 GB is free of charge for storage. The backup data is stored in the

standard storage class using the multi-AZ deployment and is billed by the hour. For pricing details, see **Billing**.

9.5 How Can I Back Up RDS Databases 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. However, you are advised not to use an ECS as the database backup space. You are advised to store RDS backup data to OBS for high data reliability and service assurance.

9.6 How Do I Restore Backup Files on HUAWEI CLOUD to a Local Database?

You can use the OBS client to download backup files to a local device and then restore them locally.

9.7 Are Manual Backups Still Charged After My RDS DB Instances Have Been Deleted?

Yes. Manual backups are retained by default after your DB instances are deleted. The manual backups are charged based on the OBS pricing details.

9.8 Will the Backup Data File Be Retained After the RDS DB Instance Is Deleted?

After the RDS DB instance is deleted, its backup files are automatically deleted. If you want to retain data, complete a manual backup before deleting the DB instance.

9.9 How Can I Retrieve the Databases and Tables Deleted by Mistake?

HUAWEI CLOUD Data Admin Service (DAS) is a professional tool that simplifies database management.

You can use DAS to retrieve the data that is deleted by mistake and roll it back to the original status. You are also advised to enable SQL audit to record database operations.

Scenarios

- Audit core data changes, collect change statistics, and view sensitive information. For example, you can use this function to query bank statements, statistics on new orders, and key configuration changes.

- Roll back the misoperation to the state before it is operated. For example, you can use the rollback function when the WHERE condition is not added during DBA configuration update, configuration data is deleted by mistake, or a large amount of dirty data and ripple effects are generated due to program bugs.

Operation Entrance

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** to go to the RDS console. The RDS console is displayed.

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

Alternatively, click the target DB instance on the **Instance Management** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

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

----End

Procedure

For operation details, see **Data Tracking and Rollback** in the *Data Admin Service User Guide*.

9.10 How Are Unsynchronized Backups Generated for RDS SQL Server DB Instances?

Unsynchronized backups are generated only for Microsoft SQL Server 2017 Enterprise Edition DB instances. If a primary DB instance fails, the standby DB instance is promoted to the new primary instance. During the failover process, a small amount of data may not be synchronized and a differential backup is created for user-created databases on the original primary DB instance. You can use the unsynchronized backup and the last backup to restore data.

NOTE

To obtain the unsynchronized backup, download it from the RDS console. To obtain the last backup, contact customer service.

9.11 Why Has My Automated Backup Failed?

Automated backup failures may be caused by the following reasons:

1. The network environment is unstable, due to issues such as network delay or interruption. RDS will detect these problems and trigger an automated

backup after half an hour. You can also perform a manual backup before then.

2. Multi-task executions are complicated, resulting in problems such as task waiting or interruption. RDS will detect these problems and trigger an automated backup half an hour later. You can also perform a manual backup in time.
3. A DB instance status is unavailable, possibly because the DB instance is faulty or being modified. RDS will trigger an automated backup after the DB instance status becomes available. You can also perform a manual backup before then.
4. A parameter change is incorrect. For example, a DB instance may be faulty after a parameter template containing incorrectly changed parameters apply to it. You can check whether original and current values are correct, check whether any related parameters also need to be changed, reset the parameter template, or reboot the DB instance.
5. An error has occurred during data import.

   For example, system table records get lost due to inappropriate data import.

   For MySQL, you can import data again by referring to **Migrating MySQL Data Using DRS**.

   For PostgreSQL, you can import data again by referring to **Migrating PostgreSQL Data Using DRS**.

   For Microsoft SQL Server, you can import data again by referring to **Migrating SQL Server Data Using DRS**.

   If the problem persists, contact technical support.

9.12 What Happens to Database Backups After an RDS DB Instance Is Deleted?

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

9.13 Will My Backups Be Deleted If I Delete My Cloud Account?

If your cloud account is deleted, both your automated and manual backups are deleted.

9.14 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 whether a misoperation has been performed. Restore the data using backup files, if necessary.

Possible solutions are as follows:

- Use the RDS restoration function to restore data.
- Import the backup data to RDS through an ECS.

9.15 Does RDS Support Remote Backups?

No, RDS does not support remote backups.

9.16 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 operation details, see **Migrating Data to the Cloud**.

9.17 How Do I Use Differential Backup Provided by RDS for MySQL?

A differential backup indicates the data records on the standby DB instance is more than those on the primary DB instance. In this case, the standby DB instance is automatically rebuilt to back up the extra data.

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 **Full Backups** page, locate the target backup to be downloaded and click **Download** in the **Operation** column.

Step 5 Decompress the downloaded backup, find the DML or DDL statements, and determine whether to execute them based on service requirements.

----End

9.18 Does RDS for PostgreSQL Support Table-Level Restoration?

No.

RDS for PostgreSQL only supports instance-level restoration. You can use a manual or an automated backup to restore data to the status when the backup was created. For operation details, see **Working with Backups**.

9.19 Do Incremental and Full Backups Support Dump?

Incremental backups cannot be dumped. If you want to dump incremental backups, download merged binlogs and dump them using OBS Browser.

Full backups cannot be dumped. If you want to dump full backups, download full backups locally and dump them using OBS Browser.

9.20 Does RDS for MySQL Support Table-Level Backup to a Specified OBS Bucket?

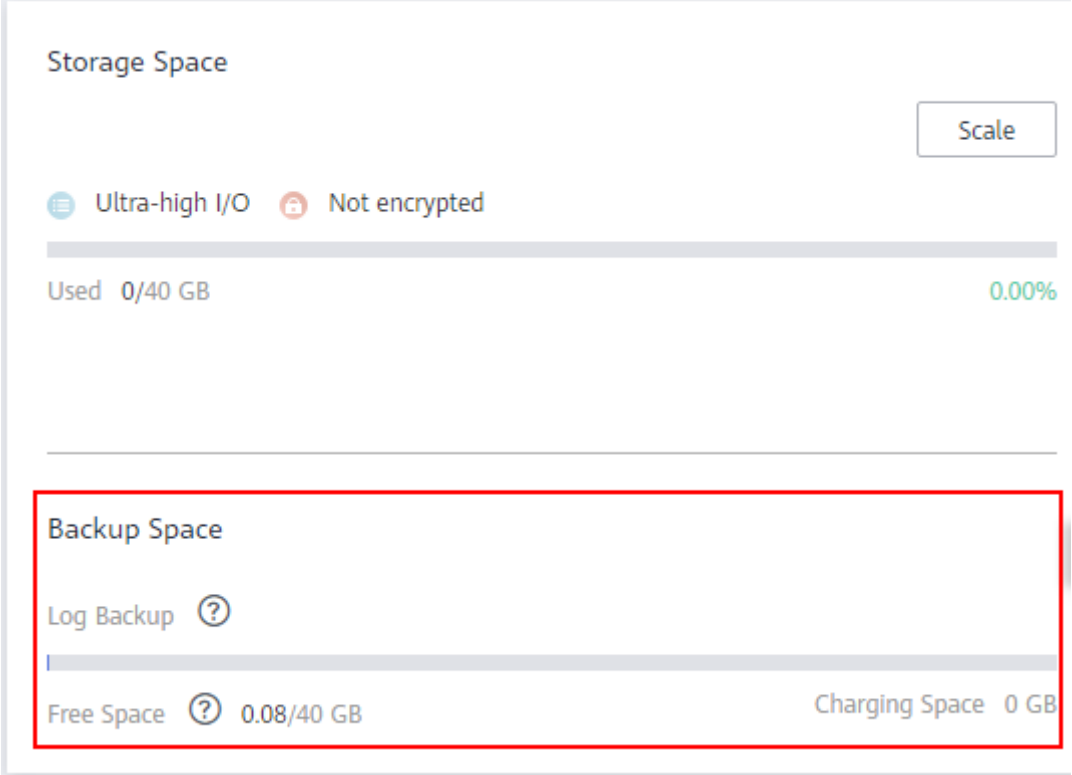
RDS for MySQL does not support table-level backup to a specified OBS bucket.

RDS supports full backups and incremental backups (binlog backups). Both of them are stored in OBS.

9.21 How Do I View My Backup Storage Usage?

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.
4. On the **Instance Management** page, click the target DB instance.
5. On the **Basic Information** page, view the backup space usage in the **Backup Space** area.

Figure 9-1 Backup space



9.22 Can RDS Directly Read Binlog Backup Files?

No, RDS does not directly read binlog files. You can download or view binlog backup files from the RDS console. For details, see **Downloading a Binlog Backup File**.

9.23 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. For operation details, see **Configuring an Automated Backup Policy**.

10 Read Replicas and Read/Write Splitting

10.1 Does RDS Support Read/Write Splitting?

Database	Read/Write Splitting	Database Proxy	Description
RDS for MySQL	Supported	Supported	You can **configure read/write splitting** after read replicas are created. Through a read/write splitting address, write requests are automatically routed to the primary DB instance and read requests are routed to read replicas by user-defined weights. • For details about the MySQL read replicas, see **Introducing Read Replicas**. • To apply for the read/write splitting permission, submit a service ticket by choosing **Service Tickets > Create Service Ticket** in the upper right corner of the management console.

Database	Read/Write Splitting	Database Proxy	Description
RDS for PostgreSQL	Supported	Not supported	After read replicas are created, 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. For details about PostgreSQL read replicas, see **Introduction to Read Replicas**.
RDS for SQL Server	Supported only by 2017 Enterprise Edition	Not supported	After read replicas are created, 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. For details about SQL Server read replicas, see **Introduction to Read Replicas**.

10.2 Can I Purchase Read Replicas Together with DB Instances?

You can purchase read replicas only together with MySQL DB instances billed in the yearly/monthly mode.

10.3 Can I Create or Delete a Database for a Read Replica?

Sorry, read replicas do not support database creation and deletion.

10.4 Does MySQL Support Sharding and Read/Write Splitting?

Yes. RDS supports sharding and read/write splitting.

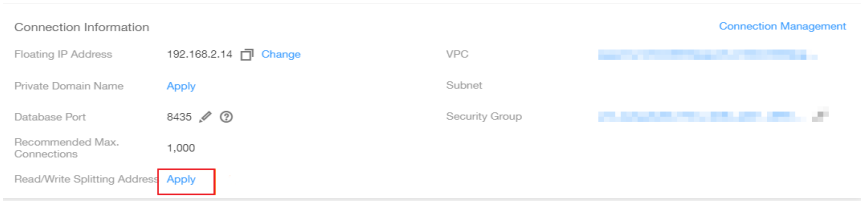
- Distributed Database Middleware (DDM) provides the sharding function to remove the capacity and performance bottlenecks of databases.

- A maximum of five read replicas can be created for a MySQL primary DB instance. Read replicas and DB instances are connected through separated IP addresses.

  After enabling the read/write splitting function, you can use a unified read/write splitting address, which can be obtained on the **Read/Write Splitting** page.

  For detailed operations, see **Configuring Read/Write Splitting**.

  Figure 10-1 Read/write splitting

10.5 Can I Apply for Multiple Read/Write Splitting Addresses for an RDS MySQL DB Instance?

Sorry, you can't. After read/write splitting is enabled, a read/write splitting address is automatically assigned. You can use the read/write splitting address to connect to the primary DB instance, but to connect to read replicas, you can only use the IP addresses of the read replicas.

10.6 How Do I Configure a Read/Write Splitting Address?

After a read replica is created, you can **enable read/write splitting** and connect to the DB instance through a read/write splitting address.

- After read/write splitting is enabled, an additional address called read/write splitting address is automatically provided. You need to switch your applications to this address for read/write splitting.
- After read/write splitting is enabled, databases can be connected through a read/write splitting address.

  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.

11 Database Monitoring

11.1 Which DB Instance Monitoring Metrics Do I Need to Pay Most Attention To?

You need to pay the most attention to CPU, memory, and storage space usage.

To stay aware of these metrics, you can configure the system to report alarms to Cloud Eye as needed. You can then take measures to clear 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 the "Alarm Rule Management" section 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.

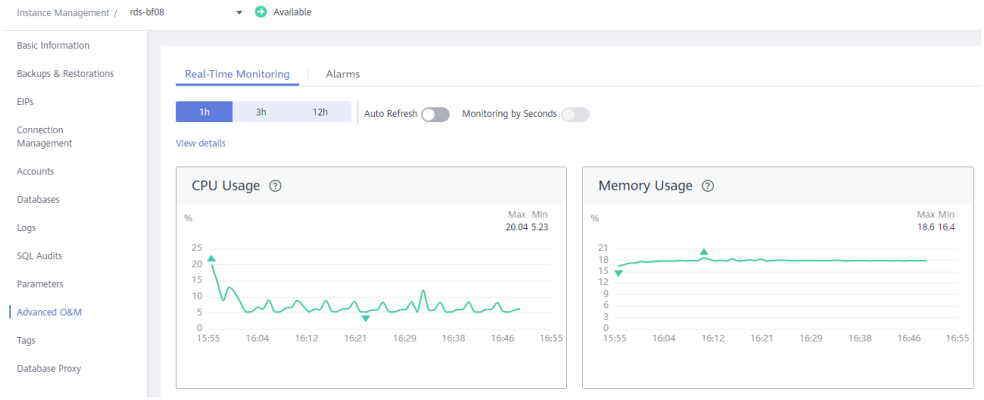
  For details, see section **Changing a DB Instance Class**.
- If a storage space usage alarm is reported, perform either of the following operations:
  - Check the storage space consumption to see whether any space can be freed up by deleting data from DB instances or dumping the data to another system.

- Scale up the storage space.
  For details, see section **Scaling Up Storage Space**.

11.2 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 the memory usage of the DB instance.

Figure 11-1 Instance monitoring



The formula for calculating the memory usage is as follows:

Memory usage = (Total memory – (Available memory + Buffer memory + Cache memory))/Total memory

You can run **cat /proc/meminfo** to view the total memory, available memory, buffer memory, and cache memory.

11.3 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 for MySQL DB Instances**
- **Setting Alarm Rules for PostgreSQL DB Instances**
- **Setting Alarm Rules for Microsoft SQL Server DB Instances**

12 Capacity Expansion and Specification Change

12.1 Are My RDS DB Instances Available When Scaling?

Currently, you can scale up storage space and change the CPU or memory of a DB instance.

- When scaling storage space, RDS DB instances are available and services are not affected. However, you cannot delete or reboot DB instances that are being scaled.
- When changing the CPU or memory of DB instances, the network is intermittently disconnected for one or two times within seconds. (For Microsoft SQL Server 2017 Enterprise Edition, you need to stop services first and then change the CPU or memory of DB instances.) For primary/standby DB instances, a failover may occur and services may be interrupted for a short period of time.

12.2 Will Services Be Interrupted When RDS Instance Classes Are Changed?

Yes.

When you change the RDS DB instance classes, DB instances will be rebooted and services will be interrupted. Therefore, select off-peak hours to perform this operation.

12.3 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 original DB port to the new port again. For details, see **Changing the Database Port**.

- If the original database port is changed successfully, the previous change failed because the submitted database port is occupied.
- If the original database port still fails to be changed, contact technical support.

13 Database Parameter Modification

13.1 What Inappropriate Parameter Settings Cause Unavailability of the PostgreSQL Database?

In the following cases, inappropriate parameter settings cause unavailability of the database:

- 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 the parameters inappropriately, the database is 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 details on parameter descriptions, visit the **PostgreSQL official website**.

Solution:

1. Log in to the RDS console and query the logs to locate the incorrectly configured parameter.
2. On the **Configuration** page, change parameters to default values and reboot the database.
3. Set the incorrectly configured parameter to a correct value and other parameters to the original values.

13.2 How Can I Change the Time Zone?

Different DB engines have different time zone policies.

MySQL and PostgreSQL allows you to select a time zone when you create a DB instance and change the time zone after the instance is created.

SQL Server allows you to select a time zone when you create a DB instance but you cannot change the time zone after the instance is created.

To change the time zone for a MySQL or 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 **Instance Management** page, click the target DB instance.

Step 5 On the **Parameters** page, locate the time zone parameter and change its value. Then, click **Save**. In the displayed dialog box, click **Yes**.

- For MySQL, the time zone parameter is **time_zone**.
- For PostgreSQL, the time zone parameter is **timezone**.

----End

13.3 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. For operation details, see **Modifying Parameters**.

13.4 How Do I Ensure that the Character Set of an RDS MySQL Database Is Correct?

UTF-8 supports 4 byte characters, while MySQL utf8 supports only 3 byte characters. Emojis, uncommon Chinese characters, and newly added Unicode characters cannot be stored using MySQL utf8 character set. MySQL released the utf8mb4 character set in 2010 and added the utf8mb4 code since 5.5.3 to compatible with the 4-byte unicode. You only need to change utf8 to utf8mb4. No other conversion is required.

HUAWEI CLOUD Data Admin Service (DAS) is a professional database management tool. You can view the database and system character sets through the DAS console.

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 **Log In** in the **Operation** column.

Alternatively, click the target DB instance on the **Instance Management** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

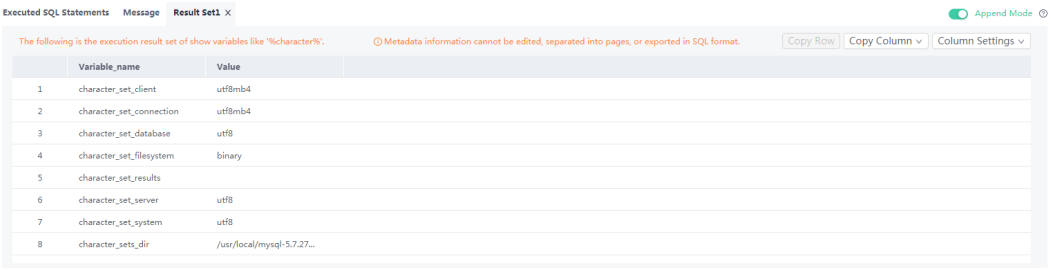
Step 5 On the displayed login page, enter the correct username and password and click **Log In**.

Step 6 On the top menu bar, choose **SQL Operation** > **SQL Window**.

Step 7 Run the following SQL statement in the SQL window to view the database character set:

show variables like '%character%';

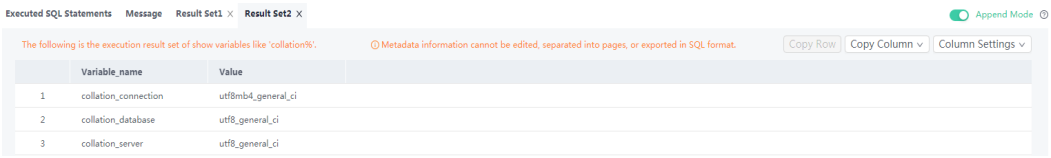
Figure 13-1 SQL execution result



Step 8 Run the following SQL statement in the SQL window to view the database coding:

show variables like 'collation%';

Figure 13-2 SQL execution result



Step 9 Change the character set to utf8mb4.

1. Run the following SQL statement to change the database character sets.

   ALTER DATABASE DATABASE_NAME DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

2. Run the following SQL statement to change the table character sets.

   ALTER TABLE TABLE_NAME DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

NOTE

The SQL statement just changes the character sets of tables. The character sets of fields in the tables are not changed.

3. Run the following SQL statement to change all the field character sets in tables:

   ALTER TABLE TABLE_NAME CONVERT TO CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

NOTE

- **character_set_client**, **character_set_connection**, and **character_set_results** are the settings of the client.
- **character_set_system**, **character_set_server**, and **character_set_database** are the settings of the server.
- The priorities of the parameters on the server are as follows: **character_set_database** > **character_set_server** > **character_set_system**.
- To change **character_set_server** and **set names**, see **How Do I Use the utf8mb4 Character Set to Store Emoji in an RDS for MySQL DB Instance?**

----End

13.5 Does RDS for PostgreSQL Support the test_decoding Plugin?

PostgreSQL 10 and PostgreSQL 11 support test_decoding. For more information about test_decoding, see **test_decoding introduction**.

NOTE

To use test_decoding, you need to set **wal_level** to **logical**.

13.6 What Should I Do If Modifications to RDS PostgreSQL Parameters Do Not Take Effect After a DB Instance Reboot?

You are advised to adjust the **shard_buffer** value and then reboot the DB instance. For details about how to modify parameters, see **Modifying Parameters**.

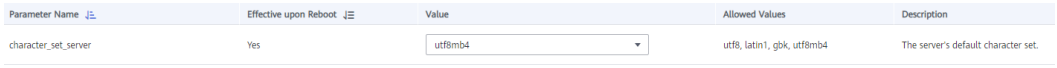
13.7 How Do I Use the utf8mb4 Character Set to Store Emoji in an RDS for MySQL DB Instance?

Configuration

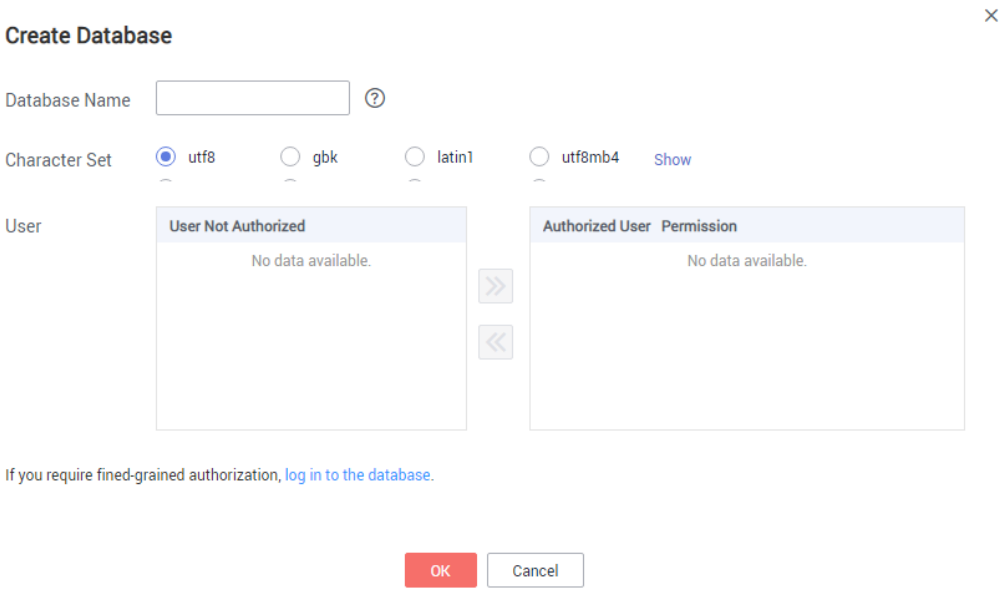
To store emoji in an RDS for MySQL DB instance, you must:

- Ensure that the client outputs the utf8mb4 character set.

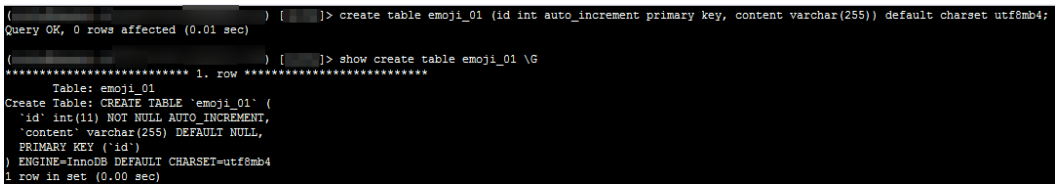
- Ensure that the connection supports the utf8mb4 character set. For example, the JDBC connection requires MySQL Connector/J 5.1.13 or later versions. In the JDBC connection string, you are advised not to configure the **characterEncoding** option.
- Configure the RDS DB instance as follows:
  - Set **character_set_server** to **utf8mb4**.



  - Select **utf8mb4** for **Character Set**.



  - Set the character set of the configuration table to **utf8mb4**.



Setting the Session Character Set Through set names

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 operations in **Configuration**, you are advised to set the connection character set to **utf8mb4** as follows:

```
String query = "set names utf8mb4";
stat.execute(query);
```

13.8 Where Should I Store the NDF Files for Microsoft SQL Server?

When you add NDF files of the custom database and the tempdb database, do not place them in C drive. If you place them in the C drive, the system disk space

will be exhausted and services may be interrupted. You need to store the NDF auxiliary file of the custom database in **D:\RDSDBDATA\DATA** and the NDF auxiliary file of the tempdb database in **D:\RDSDBDATA\Temp**.

13.9 Can I Change the VPC to Which My RDS DB Instance Belongs?

No, you cannot directly change the VPC on the RDS console.

However, you can change the VPC by restoring the full backup to a new DB instance. For operation details, see **Restoring a DB Instance from a Backup**.

13.10 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.

13.11 How Do I Modify the Character Set Collation of RDS for SQL Server?

- An instance-level collation can be specified only during instance creation. After the DB instance is created, the collation cannot be modified. To modify the instance-level character set collation, you need to create a DB instance and then restore data to the created DB instance.
- A database-level collation is specified during database creation. If it is not specified, the instance-level collation is automatically used. You can modify the database-level collation as user **rdsuser** at any time.

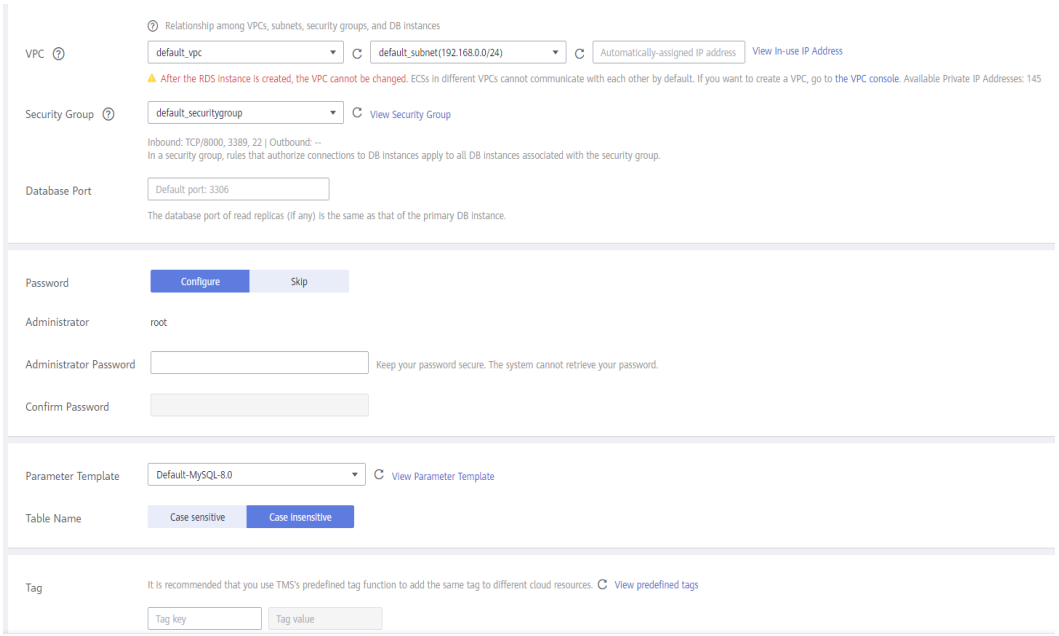
13.12 How Do I Set Case Sensitivity for RDS MySQL Table Names?

For existing DB instances, the case sensitivity for table names cannot be modified.

You can set the case sensitivity for table names during the DB instance creation using either of the following methods. Currently, only MySQL 8.0 supports case sensitivity settings for table names.

- Set **Table Name Case Sensitivity** on the RDS console by referring to **Buying a DB Instance**.

Figure 13-3 Database configuration



- Set **lower_case_table_names** by invoking an API to create a DB instance by referring to **Creating a DB Instance**.

  Value range:

  – **0**: Table names are fixed and case sensitive.

  – **1**: Table names are stored in lowercase and are case insensitive.

14 Log Management

14.1 How Long Is the Delay of RDS MySQL Slow Query Logs?

Generally, the delay is 5 minutes. If the size of slow query logs reaches 10 MB within 5 minutes, the logs will be uploaded to OBS.

14.2 How Do I View All SQL Logs Executed by MySQL?

You can use the visualized database management service Data Admin Service (DAS) to quickly search for target SQL execution records. You can also use the SQL audit function of RDS to query all SQL operation records.

Querying SQL Logs Through DAS

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 **Log In** in the **Operation** column.

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

Step 6 On the top menu bar, choose **SQL Operations** > **SQL History**.

Step 7 On the displayed page, search for execution information about the target SQL statement by time range, database name, or keyword.

- To access the **Database Management**, click a database name.
- To copy and use your required SQL statements, click the SQL statement in the **SQL Statement** column.

- To directly execute a SQL statement, click **Open in SQL Window** in the **Operation** column.

----End

Querying SQL Logs Through RDS

Step 1 Log in to the management console.

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

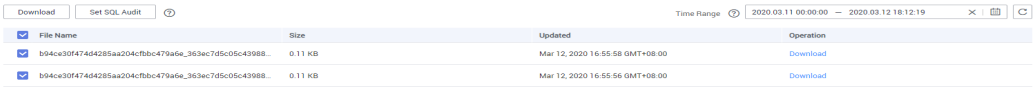
Step 3 Click **Service List**. Under **Database**, click **Relational Database Service**. The RDS console is displayed.

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, 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 one SQL audit log.

Figure 14-1 Downloading SQL audit logs



Step 6 The following figure shows the SQL audit log content. For field descriptions, see **Table 14-1**.

Figure 14-2 MySQL audit logs

```
"6","408543","1159","Connect",2020-03-20T03:35:05 UTC,"","","","","","[redacted]","",""
"7","408543","0","Quit",2020-03-20T03:35:05 UTC,"","","","","","[redacted]","",""
"8","408544","1159","Connect",2020-03-20T03:35:20 UTC,"","","","","","[redacted]","",""
"9","408544","0","Quit",2020-03-20T03:35:20 UTC,"","","","","","[redacted]","",""
"10","408546","1159","Connect",2020-03-20T03:35:35 UTC,"","","","","","[redacted]","",""
"11","408546","0","Quit",2020-03-20T03:35:35 UTC,"","","","","","[redacted]","",""
"12","408547","1159","Connect",2020-03-20T03:35:50 UTC,"","","","","","[redacted]","",""
"13","408547","0","Quit",2020-03-20T03:35:50 UTC,"","","","","","[redacted]","",""
```

Table 14-1 Audit log field description

Parameter	Description
record_id	ID of a single audit log record.
connection_id	ID of the session executed by the record, which is the same as the ID in the **show processlist** command output.
connection_status	Session status, which is usually the returned error code of a statement. If the statement is successfully executed, the value **0** is returned.

Parameter	Description
name	Recorded type name. Generally, DML and DDL operations are QUERY, connection and disconnection operations are CONNECT and QUIT, respectively.
timestamp	Recorded UTC time.
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 **localhost** for local login and 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

14.3 What's the Slow Query Threshold for Microsoft SQL Server?

The slow query threshold is 5 seconds.

14.4 How Can I Obtain Microsoft SQL Server Error Logs Using Commands?

Step 1 Log in to the Microsoft SQL Server client as user **rdsuser**.

Step 2 Run the following statement to query error logs:

EXECUTE master.dbo.rds_read_errorlog
FileID,LogType,FilterText,FilterBeginTime,FilterEndTime

- *FileID*: indicates the ID of an error log. The value **0** indicates the latest logs.
- *LogType*: indicates the log type. The value **1** indicates error logs and value **2** indicates agent logs.
- *FilterText*: indicates a keyword, which can be **NULL**.
- *FilterBeginTime*: indicates the start time in queries, which can be **NULL**.

- *FilterEndTime*: indicates the completion time in queries, which can be **NULL**.

Example:

EXEC master.dbo.rds_read_errorlog 0,1,'FZYUN','2018-06-14 14:30','2018-06-14 14:31'

Figure 14-3 shows the query results.

Figure 14-3 Example query results

	LogDate	ProcessInfo	Text
1	2018-06-14 14:30:47.490	spid64	Starting up database 'FZYUN032020'.
2	2018-06-14 14:30:47.430	spid64	CHECKDB for database 'FZYUN029029' finished wit...
3	2018-06-14 14:30:47.400	spid64	Starting up database 'FZYUN029029'.
4	2018-06-14 14:30:47.330	spid64	CHECKDB for database 'FZYUN029027' finished wit...
5	2018-06-14 14:30:47.290	spid64	Starting up database 'FZYUN029027'.
6	2018-06-14 14:30:47.220	spid64	CHECKDB for database 'FZYUN02' finished without...
7	2018-06-14 14:30:47.180	spid64	Starting up database 'FZYUN02'.
8	2018-06-14 14:30:47.110	spid64	CHECKDB for database 'FZYUN' finished without e...
9	2018-06-14 14:30:47.080	spid64	Starting up database 'FZYUN'.
10	2018-06-14 14:30:46.840	spid64	Starting up database 'FZYUN032020'.

----End

14.5 Can I Export Statistics on RDS Slow Query Logs?

Sorry, statistics on RDS slow query logs cannot be exported.

14.6 Does the SQL Audit Function Affect Database Performance?

The SQL audit function is disabled by default. Enabling this function may decrease the performance by 10%. After you enable the SQL audit function, all SQL operations will be recorded in log files for your download and query.

14.7 How Long Can RDS Error Logs Be Retained?

RDS error logs are retained for 30 days. You can query the error log records of the last 30 days.

14.8 Can I Optimize Slow SQL Statements from the DAS Console?

Yes, **SQL tuning** helps you locate the SQL statements that are executed frequently, executed slowly, and consume large volumes of resources. You can optimize the SQL statements according to the diagnosis suggestions to ensure the stability of the database performance.

14.9 How Do I View Deadlock Logs of RDS for MySQL?

Database deadlock logs are not recorded in error logs. To view deadlock logs, use Data Admin Service (DAS), a visualized and professional database management tool, to quickly execute SQL statements.

Procedure

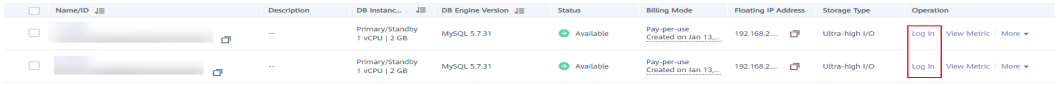
Step 1 Log in to the management console.

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 **Log In** in the **Operation** column.

Figure 14-4 Logging in to a database



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

Step 6 Select the target database and choose **SQL Operations** > **SQL Window**. In the displayed SQL window, run **show engine innodb status** to view the latest deadlock logs of the selected database. The latest deadlock logs will overwrite the historical deadlock logs.

----End

15 Network Security

15.1 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.

15.2 How Can I Ensure the Security of RDS DB Instances in a VPC?

The VPC security group helps ensure the security of RDS in a VPC. In addition, ACL can be used to allow or reject I/O network traffic for each subnet.

15.3 How Can Data Security Be Ensured During Transmission When I Access RDS Through an EIP?

When you access RDS through an EIP, service data will be transmitted on the public network. To prevent data breach, you are advised to use SSL to encrypt data transmitted on the public network. You can also use the Direct Connect or VPN services to encrypt data transmission channels.

15.4 How Can I Prevent Untrusted Source IP Addresses from Accessing RDS?

- After you enable public accessibility, your EIP DNS and database port may be obtained by malicious personnel. To protect your information including 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 maliciously cracked, set a strong password according to the password strength policies and periodically change it.
- RDS for SQL Server supports defense against brute force cracking. If malicious individuals have obtained your EIP DNS, database port, or database login information and try to crack your database with brute force, your service connections may be delayed. In this case, you can restrict the source connections and change the database username and password to prevent further damage.

  NOTE

  RDS for MySQL and PostgreSQL do not support defense against brute force cracking.

  For RDS for Microsoft SQL Server, defense against brute force cracking is enabled by default and cannot be disabled.

15.5 How Do I Configure a Security Group to Access 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 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 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.

15.6 Can I Edit or Delete the Security Group Associated with an RDS DB Instance?

You can add or modify rules for the security group associated with the RDS DB instance, but you cannot disassociate or delete the security group.

For details about how to add or modify security group rules, see **Configuring Security Group Rules**.

15.7 How Can I Import the Root Certificate to the 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 of the Linux OS.

15.8 How Can I Identify the Validity Period of an SSL Root Certificate?

When you connect to an RDS 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 new 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.
   - **Connecting to a DB Instance Through a Private Network**
   - **Connecting to a DB Instance Through a Public Network**

   NOTE

   If a certificate is about to expire, replace it with an officially issued certificate to improve system security.

15.9 How Can I Identify Data Corruption?

- Data tempering

  Lots of security measures are provided to ensure that only authenticated users have permissions to perform operations on database table records. The SSH protocol is inaccessible to users. Database tables can be accessed only through the specified database service port.

  Verifying package during primary/standby synchronization can prevent data tampering. MySQL uses the InnoDB storage engine to prevent data damage.
- DB instance servers may be powered off suddenly, causing database page corruption and database rebooting failures.

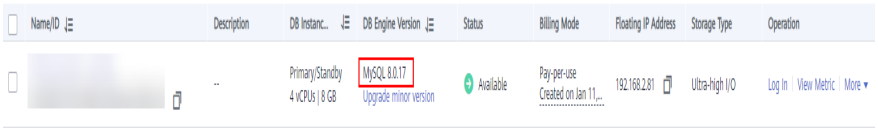
  If the primary DB instance is faulty, RDS switches to the standby DB instance within 1 to 5 minutes to provide services for you. Databases cannot be accessed during failover. You must set automatic reconnection between your applications and RDS to prevent your applications from becoming unavailable after the failover.

16 Version Upgrade

16.1 How Can I View the Minor Versions of RDS MySQL DB Instances?

- On the **Instance Management** page of the RDS console, view the DB engine version of the target DB instance.

  Figure 16-1 Instance management

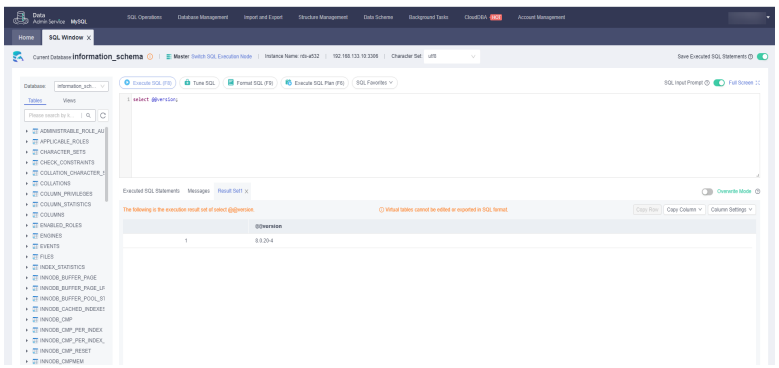
- On the DAS console, perform the following steps to view the minor version of the target DB instance:

  a. Log in to the target DB instance.

  b. On the top menu bar, choose **SQL Operations** > **SQL Window**.

  c. Run **select @@version;** to view the version of the DB instance.

  Figure 16-2 Viewing the version

16.2 Does RDS for MySQL Support Version Upgrades?

- Major version upgrades

  You can use DRS to smoothly migrate databases from MySQL 5.6 to MySQL 5.7 with minimal downtime. **Before using DRS to upgrade a major version, you need to prepare a DB instance of the target version.**

  On the **Instance Management** page, click the target DB instance. On the displayed **Basic Information** page, click **Migrate Database** in the upper right corner of the page.

  For more information, see **Before You Start** in the *Data Replication Service User Guide*.

  Table 16-1 MySQL database version information

Data Flow	Migration Direction	Source Database Version	Destination Database Version
MySQL database -> RDS MySQL instance	To the cloud	• MySQL 5.5.x • MySQL 5.6.x • MySQL 5.7.x • MySQL 8.0.x	• MySQL 5.6.x • MySQL 5.7.x • MySQL 8.0.x

  NOTE

  Data cannot be migrated from a later version database to an earlier version database.

- Minor version upgrades

  RDS for MySQL supports automatic and manual minor version upgrades, which can improve performance, add new functions, and fix bugs.

  For primary/standby DB instances, the standby DB instance is upgraded first and then the primary DB instance is upgraded.

  For more information about minor versions, see **RDS for MySQL Kernel Version Description**.

  For more information upgrade operations, see **Upgrading the Minor Version**.

16.3 Does RDS for MySQL Support Version Downgrades?

No. RDS for MySQL does not support version downgrades. To downgrade a DB instance version, you can delete the DB instance first and then create one running the target version.

16.4 Does RDS for PostgreSQL Support Major Version Upgrades?

No, RDS for PostgreSQL does not support major version upgrades.

To upgrade the major version, you can use DRS to migrate on-premises databases to RDS for PostgreSQL running the target major version with no downtime. Therefore, you need to prepare a DB instance running the target version before the migration.

On the **Instance Management** page, click the target DB instance. On the displayed **Basic Information** page, click **Migrate Database** in the upper right corner of the page.

For more information, see **Before You Start** in the *Data Replication Service User Guide*.

17 Developer-Related APIs and SDKs

Table 17-1 RDS APIs and SDKs

Category	Reference Document
RDS API	**RDS API Reference**
RDS Java SDK	**RDS Java SDK Demo**
RDS Python SDK	**RDS Python SDK Demo**
RDS Go SDK	**RDS Go SDK User Guide**

A Change History

Released On	Description
2021-01-18	This issue is the twenty-eighth official release, which incorporates the following changes: • Added **How Do I Set Case Sensitivity for RDS MySQL Table Names?** • Added **How Do I View Deadlock Logs of RDS for MySQL?** • Added **Does RDS Support 3-AZ Deployment?** • Added **Can I Delete the RDS for MySQL Backup Policy?**
2020-12-11	This issue is the twenty-seventh official release, which incorporates the following changes: • Added the troubleshooting method for connection failures caused by storage full disks in **What Should I Do If I Fail to Connect to an RDS DB Instance?**. • Added **What Should I Do If No EIPs Are Available When I'm Attempting to Bind an EIP?**
2020-09-15	This issue is the twenty-sixth official release, which incorporates the following change: Added **How Can I Calculate the Memory Usage of an RDS DB Instance?**
2020-08-15	This issue is the twenty-fifth official release, which incorporates the following change: Added **What Should I Do If the ECS and RDS Are Deployed in Different VPCs and They Cannot Communicate with Each Other?**

Released On	Description
2020-07-17	This issue is the twenty-fourth official release, which incorporates the following changes: Added section **After a Primary Instance Account Is Deleted and Recreated on RDS for SQL Server, Will the Permissions Be Automatically Synchronized?** Added section **Does RDS for PostgreSQL Support Table-Level Restoration?** Added section **Do Incremental and Full Backups Support Dump?** Added section **What Should I Do If Modifications to RDS PostgreSQL Parameters Do Not Take Effect After a DB Instance Reboot?**
2020-05-30	This issue is the twenty-third official release, which incorporates the following changes: Added section **Does RDS Support Remote Backups?** Added section **How Do I Use Differential Backup Provided by RDS for MySQL?**
2020-04-10	This issue is the twenty-second official release, which incorporates the following changes: Added **Does the SQL Audit Function Affect Database Performance?** Added **Does RDS for MySQL Support Version Downgrades?** Added **Developer-Related APIs and SDKs**. Added **Can I Change the VPC to Which My RDS DB Instance Belongs?**
2020-03-06	This issue is the twenty-first official release, which incorporates the following changes: Added **Does the Optimize Table Operation Lock Tables on an RDS DB Instance?** Added **How Do I Release DB Instances in Expired or Frozen State?** Added **What Should I Do When a Large Number of Binlog Files Cause Storage Space Insufficiency During an RDS MySQL Instance Migration?**
2020-01-31	This issue is the twentieth official release, which incorporates the following changes: Added section **What Are the Differences Between RDS ManageAccess and DAS Permissions?** Added section **What Should I Do If an RDS DB Instance Is Abnormal Due to Full Storage Space?** Optimized the content in section **What Is the Maximum Number of Connections to an RDS DB Instance?**

Released On	Description
2019-12-30	This issue is the nineteenth official release, which incorporates the following changes: Added section **Can I Export Statistics on RDS Slow Query Logs?** Added section **How Do I View the Storage Space Occupied by My Database?**
2019-10-31	This issue is the eighteenth official release, which incorporates the following changes: Added section **Does RDS for MySQL Support Version Upgrades?** Added section **Can Multiple Users Log in to DAS at the Same Time? Will the Passwords Be Locked If I Entered Wrong Passwords for Several Consecutive Times?** Added section **Will Services Be Interrupted When RDS Instance Classes Are Changed?** Added section **How Can I Retrieve the Databases and Tables Deleted by Mistake?** Added section **How Are Unsynchronized Backups Generated for RDS SQL Server DB Instances?** Added section **How Do I Ensure that the Character Set of an RDS MySQL Database Is Correct?** Added section **Can RDS DB Instances in Different VPCs Communicate with Each Other Over an Intranet?**
2019-10-12	This issue is the seventeenth official release, which incorporates the following changes: Added section **How Do I View All SQL Logs Executed by MySQL?** Added section **Does RDS Support Cross-Region Migration?** Added section **What Should I Do If Garbled Characters Are Displayed After SQL Query Results Are Exported to an Excel File?**
2019-09-12	This issue is the sixteenth official release, which incorporates the following changes: Added an FAQ: How Can I Connect to a MySQL Database Through JDBC? Added an FAQ: What Can I Do If the Connection Test Failed? Added an FAQ: Can RDS Primary/Standby DB Instances Be Changed to Single DB Instances? Added an FAQ: Can I Purchase Read Replicas Together with DB Instances? Added an FAQ: How Do the Login Name Permissions of RDS for SQL Server 2017 Enterprise Edition Primary/Standby DB Instances Synchronized to Read Replicas?

Released On	Description
2019-08-12	This issue is the fifteenth official release, which incorporates the following changes: Added an FAQ: Can I Change the Storage Type of an RDS DB Instance from Common I/O to Ultra-high I/O? Added an FAQ: What's the Slow Query Threshold for Microsoft SQL Server? Added an FAQ: How Long Is the Delay of RDS MySQL Slow Query Logs?
2019-07-12	This issue is the fourteenth official release, which incorporates the following change: Added a section of using the utf8mb4 character set to store emoji emoticons in an RDS for MySQL DB instance.
2019-06-12	This issue is the thirteenth official release, which incorporates the following changes: Added **Can I Access an RDS DB Instance Over an Intranet Across Regions?** Added **Does RDS for MySQL Support Stored Procedures and Functions?**
2019-03-30	This issue is the twelfth official release, which incorporates the following change: Optimized content in section **What Storage Engines Does the RDS for MySQL Support?**
2019-03-15	This issue is the eleventh official release, which incorporates the following change: Added section **Does RDS for MySQL Support Multiple Accounts?**
2019-02-15	This issue is the tenth official release, which incorporates the following change: Added section **Where Should I Store the NDF Files for Microsoft SQL Server?**
2019-01-08	This issue is the ninth official release, which incorporates the following change: Optimized the content in **Why Does the Root User Not Have the Super Permission?**

Released On	Description
2018-10-15	This issue is the eighth official release, which incorporates the following changes: Added section **How Long Does It Take to Create a DB Instance?** Added section **Is RDS for MySQL Compatible with MariaDB?** Added section **Does RDS Support Cross-AZ High Availability?** Added section **How Is RDS for MySQL Backup Data Charged?** Added section **Why Does the Root User Not Have the Super Permission?** Added section **Can I Set the Synchronize Model Between Primary DB Instances and Read Replicas?** Added section **How Does a Cloud Database Perform a Primary/Standby Switchover?** Added section **Why Can't I Ping My EIP After It Is Bound to a DB Instance?** Added section **Does RDS Support Scaling Down Storage Space of DB Instances?** Optimized the content in **How Many Databases Can Run on an RDS DB Instance?**
2018-09-04	This issue is the seventh official release, which incorporates the following change: Optimized MySQL parameter groups.
2018-08-15	This issue is the sixth official release, which incorporates the following change: Added an FAQ: How do I configure a custom policy?
2018-07-13	This issue is the fifth official release, which incorporates the following change: Changed the default port number to **5432** when a PostgreSQL DB instance is created.
2018-06-30	This issue is the fourth official release, which incorporates the following changes: • Added an FAQ: How can I decompress qp files of MySQL DB instances and restore data? • Added section **How Can I Change the Time Zone?**
2018-06-15	This issue is the third official release, which incorporates the following changes: • Added section **How Can I Obtain Microsoft SQL Server Error Logs Using Commands?** • Added an FAQ: How do I obtain IP addresses of applications?

Released On	Description
2018-06-01	This issue is the second official release, which incorporates the following change: Modified the content in section **How Can I Install the MySQL Client?**
2018-05-15	This issue is the first official release.