Relational Database Service

FAQs

Issue   37
Date   2022-12-26

HUAWEI TECHNOLOGIES CO., LTD.

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

Huawei Technologies Co., Ltd.

Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:	https://www.huawei.com
Email:	support@huawei.com

Contents

1 Product Consulting

1.1 What Should I Pay Attention to When Using RDS?

1. DB instance operating systems (OSs) are invisible to you. Your applications can access a database only through an IP address and a port.

2. The backup files stored in Object Storage Service (OBS) and the Elastic Cloud Server (ECS) used by RDS are invisible to you. They are visible only to the RDS instance management system.

3. Before viewing the DB instance list, ensure that the region is the same as the region where the DB instance is purchased.

4. After creating RDS DB instances, you do not need to perform basic O&M operations, such as enabling HA and installing security patches. However, you must pay attention to:

   a. Whether the CPU, input/output operations per second (IOPS), and space of the RDS DB instance are sufficient. If any of these becomes insufficient, change the CPU/Memory or scale up the DB instance.

   b. Whether the performance of the RDS DB instances is adequate, a large number of slow query SQL statements exist, SQL statements need to be optimized, or any indexes are redundant or missing.

1.2 What Is the Availability of RDS DB Instances?

Calculation formula for RDS DB instance availability:

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

1.3 How Do I Distinguish Between General-Purpose and Dedicated RDS for MySQL Instances Using Cloud SSDs?

You can use either of the following methods:

Checking the Instance Class on the Console

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

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

Step 4 On the **Instances** page, click the instance name.

Step 5 In the **DB Information** area on the displayed page, check the specification code next to the **Instance Class** field.

- General-purpose: The specification code contains **n1**.
- Dedicated: The specification code contains **x1**.

----End

Querying the Instance Class through the API

Call the API used for **querying database specifications** and check the instance class based on the value of the returned response parameter **group_type**.

- **general**: general-purpose
- **dedicated**: dedicated
- **rapid**: dedicated (offline)

1.4 Will My RDS DB Instances Be Affected by Other User Instances?

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

1.5 Does RDS Support Cross-AZ High Availability?

Yes. When you **buy a DB instance**, you can select **Primary/Standby** for **DB Instance Type** and then select different AZs for **Primary AZ** and **Standby AZ**.

☐ NOTE

RDS does not support 3-AZ deployment.

An AZ is a physical region where resources have independent power supplies and networks. AZs are physically isolated but interconnected through an internal network. You can deploy your instance across AZs in some regions.

To achieve higher reliability, if you deploy the primary and standby instances in the same AZ, RDS will automatically deploy the primary and standby instances in different physical servers. If you attempt to deploy your primary and standby 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 different (default setting), the primary and standby instances are deployed in different AZs to ensure failover support and high availability.

- If they are the same, the primary and standby instances are deployed in the same AZ. If an AZ failure occurs, high availability cannot be ensured.

Figure 1-1 Cross-AZ high availability

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

No. But you can change single instances to primary/standby instances. For details, see **Changing a DB Instance Type from Single to Primary/Standby**. You can use Data Replication Service (DRS) or the export and import tool of the client to migrate data from primary/standby DB instances to single DB instances.

1.7 What Can I Do About Slow Responses of Websites When They Use RDS?

To solve this problem:

- Check the performance of RDS DB instances on the RDS console.

- Compare the database connection statuses of local databases and RDS DB instances. This problem depends on web applications.

1.8 Can I Change the Replication Mode Between Primary DB Instances and Read Replicas?

- For the MySQL engine:

  A read replica uses a single-node architecture (without a standby node). Changes to the primary DB instance are also automatically synchronized to all associated read replicas through the native MySQL replication function. The synchronization is not affected by network latency. Even if a DB instance does not have a primary key ID, its data is synchronized to the associated read replicas.

  The replication mode displayed on the RDS console indicates the data synchronization method between primary and standby DB instances. Semi-synchronous and asynchronous are both supported. The semi-synchronous mode is more secure but the asynchronous mode improves performance.

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

- For the Microsoft SQL Server engine:

  The synchronous-commit mode is supported between primary and standby instances and cannot be modified.

  The asynchronous-commit mode is supported between primary instances and read replicas and cannot be modified.

  For more information, see **official documentation**.

1.9 What Is the Time Delay for Primary/Standby Replication?

When standby instances cannot keep up with the updates on the primary, this generates replication delay. If the standby SQL and I/O thread are running, the replication delay is a positive value measured in seconds. If the standby SQL thread is not running, or if the SQL thread has consumed all of the relay log and the standby I/O thread is running, then it is **NULL** (undefined or unknown)

The delay for primary/standby replication cannot be calculated using a formula as the delay is affected by the following factors:

- Network communication status
- Transaction workload on the primary DB instance in transactions per second (TPS)
- The size of the transaction executed by the primary DB instance (this affects the duration of transaction executions)
- Load balancing of the standby DB instance and read replicas

If the primary DB instance has a heavy load for a certain period of time and executes a large number of transactions per second, replication to the standby DB instance will be delayed. This delay is generally a few seconds.

- RDS for MySQL: Click the DB instance name on the **Instances** page. The replication source is the primary DB instance. When the replication status is normal, view **Real-Time Replication Delay** to obtain the value of the primary/standby replication delay.
- RDS for PostgreSQL: To check data consistency between the primary and standby DB instances, view **Replication Lag** on the Cloud Eye console to obtain the value of the primary/standby replication delay.
- RDS for SQL Server: To check data consistency between the primary and standby DB instances, view **Replication Delay** on the Cloud Eye console to obtain the value of the primary/standby replication delay.

1.10 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.

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

You can enable disk encryption when purchasing an RDS DB instance. For details, see **Buy a DB Instance**.

After an instance is created, the disk encryption status and the key cannot be changed.

If you want to configure disk encryption for a created instance, perform the following operations:

- Restore data to a new instance from backups and enable disk encryption for the new instance.

- Use Data Replication Service (DRS) to migrate data from the instance to an encrypted instance.

1.12 Will Backups Be Encrypted After Disk Encryption Is Enabled for My RDS Instance?

- RDS for MySQL:

  If you enable disk encryption during instance creation, the disk encryption status and the key cannot be changed later. Disk encryption will not encrypt backup data stored in OBS. To enable backup data encryption, contact customer service.

- RDS for PostgreSQL:

  If you enable disk encryption during instance creation, the disk encryption status and the key cannot be changed later. Disk encryption will not encrypt backup data stored in OBS. To enable backup data encryption, contact customer service.

- RDS for SQL Server:

  If you enable disk encryption during instance creation, the disk encryption status and the key cannot be changed later. Disk encryption will not encrypt backup data stored in OBS.

NOTICE

If disk encryption or backup data encryption is enabled, keep the key properly. Once the key is disabled, deleted, or frozen, the database will be unavailable and data may not be restored.

- If disk encryption is enabled but backup data encryption is not enabled, you can **restore data to a new instance from backups**.

- If both disk encryption and backup data encryption are enabled, data cannot be restored.

1.13 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**.

1.14 What Are the Restrictions on RDS for MySQL DB Instances After GTID Is Enabled?

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.

1.15 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.

1.16 How Many Databases Can Run on an RDS DB Instance?

The maximum number of databases that can run on an RDS DB instance depends on the DB engine settings.

If there are enough CPU, memory, and storage resources, there are no limitations to the number of databases running on a DB instance. However, the number of tables in the databases affects the backup speed. If there are more than 500,000 tables, the backup will fail.

- RDS for MySQL allows you to create numerous databases and tables. For details, see the official MySQL documentation.
- RDS for PostgreSQL allows you to create numerous databases and database accounts.

1.17 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 GPL licensing. One of the reasons for developing MariaDB is that Oracle acquired MySQL, so there is a chance that MySQL could get shut down. The community developed MariaDB to protect against 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.

1.18 Does RDS for MySQL Support TokuDB?

Currently, the official MySQL does not support TokuDB.

RDS for MySQL does not support TokuDB, either.

1.19 What Is the Maximum Size Allowed for a Single Table in RDS for MySQL Instances?

The maximum size allowed for a single table depends on the maximum file size allowed by the OS.

Due to metadata overhead, the maximum size allowed for a single table is 2 TB.

2 Resource Freezing, Release, Stopping, Deletion, and Unsubscription

Why Are My RDS Resources Released?

If your subscriptions have expired and not renewed, or you are in arrears due to an insufficient balance, your resources enter a grace period. If the renewal is still not completed or the outstanding amount is not paid off when the grace period ends, the resources enter a retention period, during which the resources will be unavailable. If the renewal is still not completed or the outstanding amount is still not paid off when the retention period ends, the stored data will be deleted and the cloud service resources will be released. For details, see **Service Suspension and Resource Release**.

Why Are My RDS Resources Frozen?

Your resources may be frozen for a variety of reasons. The most common reason is that you are in arrears.

Can I Still Back Up Data If My DB Instance Is Frozen?

No. If your RDS instance is frozen due to arrears, you need to unfreeze the instance first.

How Do I Unfreeze My Resources?

If your resources are frozen due to arrears, to unfreeze your resources, you can renew your resources or top up your account. RDS instances frozen due to arrears can be renewed, released, or deleted. Yearly/Monthly RDS instances that have expired cannot be unsubscribed from, but those that have not expired can.

What Happens When My Resources Are Frozen, Unfrozen, or Released?

- After your resources are frozen:
  - They cannot be accessed, causing downtime. For example, if your RDS instance is frozen, it cannot be connected to.
  - If they are yearly/monthly resources, no changes can be made to them.

- – They can be unsubscribed from or deleted manually.
- After your resources are unfrozen, you can connect to them again.
- If your resources are released, your instances will be deleted. Before the deletion, RDS determines whether to **move the instances to the recycle bin** based on the recycling policy you specified.

How Do I Renew My Resources?

After a yearly/monthly RDS instance expires, you can renew it on the **Renewals** page. For details, see **Renewal Management**.

Can My Resources Be Recovered After They Are Released or Unsubscribed From?

If your instance is moved to the recycle bin after being deleted and is within the retention period, you can **rebuild** it from the recycle bin. Otherwise, data cannot be restored.

Before unsubscribing from a resource, confirm the resource information carefully. If you have unsubscribed from a resource by mistake, you are advised to purchase a new one.

Why Is My RDS DB Instance Still Billed After Being Stopped?

After a DB instance is stopped, the ECS where the DB instance is located is no longer billed. Other resources, including EIPs, storage resources, RDS for MySQL database proxies, and backups, are still billed.

How Do I Delete an RDS Instance?

An RDS instance cannot be deleted if any operation is being performed on it. For example, the instance is being created, rebooted, or restored, or its instance class is being changed. You can delete the instance only after the operation is complete.

- For pay-per-use instances, see **Deleting a Pay-per-Use DB Instance or Read Replica**.
- For yearly/monthly instances, see **Unsubscribing from a Yearly/Monthly DB Instance**.

3 Resource and Disk Management

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

- RDS for MySQL and RDS for PostgreSQL instances:

  Generally, creating a DB instance (single or primary/standby) takes 5 to 7 minutes. The time required for creating a read replica depends on the data amount of the primary instance. More data will take longer to replicate. If the primary instance is empty, creating a read replica takes 7 to 8 minutes.

- RDS for SQL Server instances:

  It takes about 12 to 15 minutes to create a single instance and 15 to 18 minutes to create a primary/standby instance.

If it takes an extended time, an error may occur during the creation. In this case, contact customer service.

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

The following logs and files occupy RDS storage space.

Table 3-1 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 3-2 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 3-3 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 if there are a large number of sorting queries executed by applications.

   b. A large number of binlog files are generated and occupy space if there are large amounts of insert, delete, and update operations in a short period.

   c. A large number of binlog files are generated if there are a large number of transactions and write operations.

4. Use Cloud Eye to monitor the size, usage, and utilization of storage space of your DB instance and set alarm policies.

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

No. You can create a DB instance with less storage space and use Data Replication Service (DRS) to migrate your data to the instance.

For details, see **Real-Time Migration**.

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

Both your regular data (backup data not included) and the data required for the operation of your DB instances (such as system database data, rollback logs, redo logs, and indexes) take up storage space on your RDS DB instances. The storage space includes the file system overhead required for inode, reserved blocks, and database operations. The following RDS log files also occupy storage space:

- Binlog files generated by RDS for MySQL databases
- Logs files generated by RDS for PostgreSQL database servers
- Log files, including RDS for SQL Server logs, default trace logs, and agent logs, generated by RDS for SQL Server databases.

These files ensure the stability of RDS DB instances.

3.5 How Much Storage Space Is Required for DDL Operations?

Data Definition Language (DDL) operations may increase storage usage sharply. To ensure that services are running properly, do not perform DDL operations during peak hours. If DDL operations are required, ensure that storage space is at least twice the tablespace size plus 10 GB. For example, if your tablespace is 500 GB, ensure that storage space is at least 1,010 GB (500 GB x 2 + 10 GB).

3.6 How Do I Prevent a Sharp Increase in Data Disk Usage If I Want to Push a Large Amount of Data to My RDS for SQL Server Instance in a Short Period of Time?

If you push a large amount of data to your primary/standby instance in a short period of time, the data may not be able to be synchronized between the primary and standby instances fast enough. As a result, logs cannot be truncated or shrunk, and the disk usage spikes.

- Method 1

  Push data in batches, and leave plenty of time for each batch of data to be replicated from the primary instance to the standby instance.

- Method 2

  Before pushing data, set **Recovery model** of your database to **Simple**. In this model, data is not synchronized between the primary and standby instances, and no incremental backups are generated. During this period, point-in-time recovery (PITR) cannot be performed. After the data is pushed, set **Recovery model** of your database to **Full** to resume the replication between the primary and standby instance. For details, see **How Do I Remove and Re-establish a Replication of My RDS for SQL Server Instance?**

- Solution 3

  To migrate an on-premises database to your RDS instance, **use DRS to restore backup files of the on-premises database to your RDS instance**.

4 Database Connection

4.1 What Should I Do If I Can't Connect to My RDS DB Instance?

Possible Causes

Try the following:

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

   For example, the system is faulty, the DB instance is abnormal, or the DB instance or a table is locked.

2. **(Common) Check whether the client connection is correct.**
   - If you connect to a DB instance over a private network, ensure that the DB instance and ECS are in the same region and VPC.
   - If you connect to a DB instance over a public network, bind an EIP to the DB instance and then connect to the DB instance through the EIP.

3. **Check the connection method.**

   Run either of the following example commands to enable or disable SSL:
   - SSL enabled: **mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem**
   - SSL disabled: **mysql -h 172.16.0.31 -P 3306 -u root -p**

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

   For example, check whether the following parameters are configured correctly: connection address, port number, username, password, and connection method.

5. **(Common) Check whether the network connectivity is normal**

   For a private network connection:

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

   b. Check security group rules.

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

c. On the ECS, check whether the DB instance port can be connected to.

For a public network connection:

a. Check security group rules.

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

b. Check network ACL rules.

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

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

If there is an excessive number of database connections, applications may be unable to connect.

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

If the DB instance is in the **Storage full** state, data read and write performance is affected.

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

Find corresponding solutions based on connection error messages.

Fault Locating

Figure 4-1 Locating instance connection failures

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

    Check whether the DB instance is in the **Available** state.

    Possible cause: The RDS system is faulty, the DB instance is abnormal, or the DB instance or a table is locked.

    Solution: If the DB instance is abnormal, reboot it.

    Figure 4-2 Checking DB instance status

	Name/ID		Description	DB Instanc...	DB Engine Version	Status	Billing Mode	Floating IP Ad...	Created	Storage Type	Operation
☐		⬚	--	Primary/Standby 1 vCPU | 1 GB	MySQL 5.7.31	⊕ Available	Pay-per-use Created on De...	192.1... ⬚		Hybrid SSD	Log In | View Metric | More ▾

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

    Install an **engine client** whose version is at least as new as the DB instance version.

    For details about how to connect to a DB instance over a private or public network, see **Can an External Server Access the RDS Database?**

    Table 4-1 Connection model

Connection method	Scenario	Example
Private network	A private IP address is provided by default. If your applications are deployed on an ECS that is in the same region and VPC as the DB instance, connect to the ECS and DB instance through a private IP address.	RDS for MySQL: **mysql -h <**_private IP address_**> -P 3306 -u root -p --ssl-ca=/tmp/ ca.pem**
Public network	If you cannot access the DB instance using a private IP address, bind an EIP to the DB instance and then connect to the DB instance through the EIP. For EIP pricing details, see **EIP billing details**.	RDS for MySQL: **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 **Connectivity & Security** page and upload the certificate to the ECS.

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

Figure 4-3 Enabling SSL
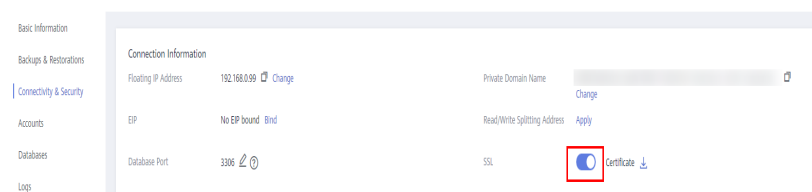
– Common connection: Disable SSL on the **Basic Information** page.

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

4. **Check the parameters in the command used to connect.**

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

If you use a private connection with SSL enabled, run **mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem**.

– IP address

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

Figure 4-4 Floating IP address
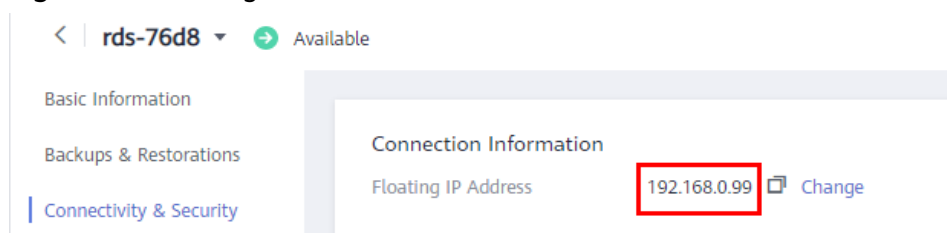
– Database Port

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

– Root login credentials

Make sure you have entered the root password correctly.

– Certificate

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

If you use a public connection with SSL enabled, run the following example command: **mysql -h** *EIP* **-P 3306 -u root -p --ssl-ca=/tmp/ca.pem**

– IP address

On the **Public Connection** tab of the **Connectivity & Security** page, obtain the EIP in the **Connection Information** area.

Figure 4-5 EIP
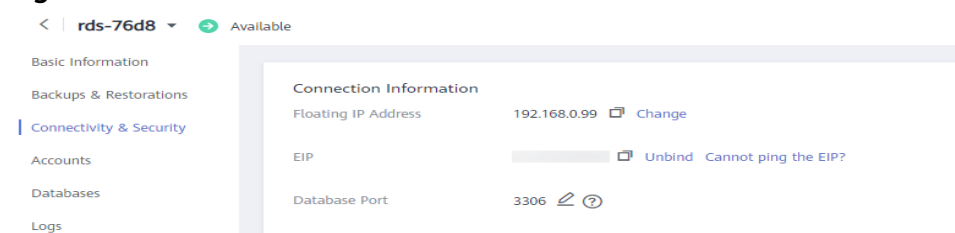
- Database Port

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

- Root login credentials

  Make sure you have entered the root password correctly.

- Certificate

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

5. **Check the network connection.**

   Private network connection

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

      - 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?**

   Figure 4-6 Checking the VPC of an ECS
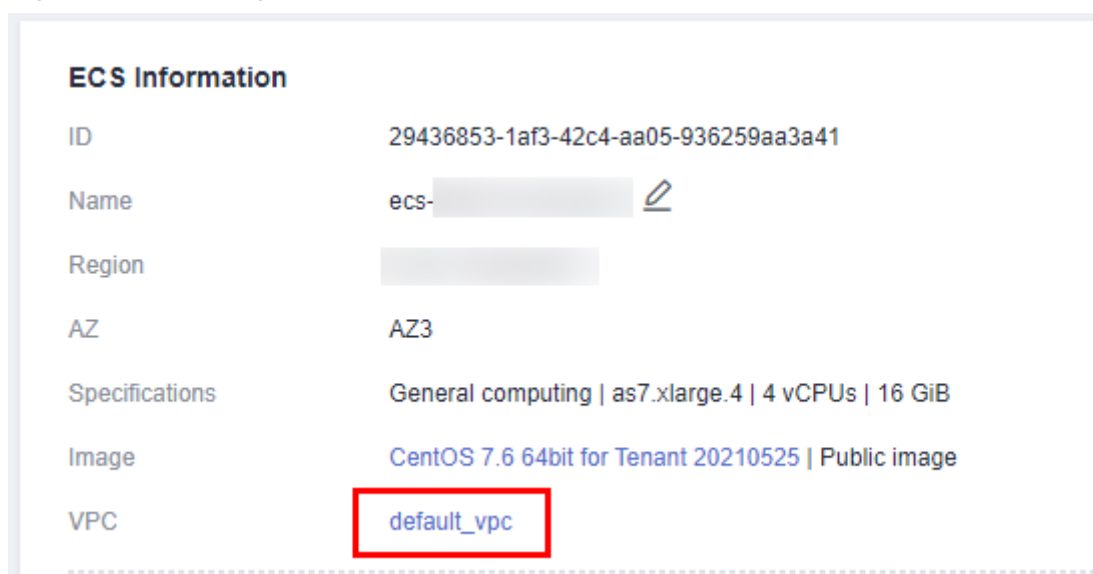
Figure 4-7 Checking the VPC of an RDS instance
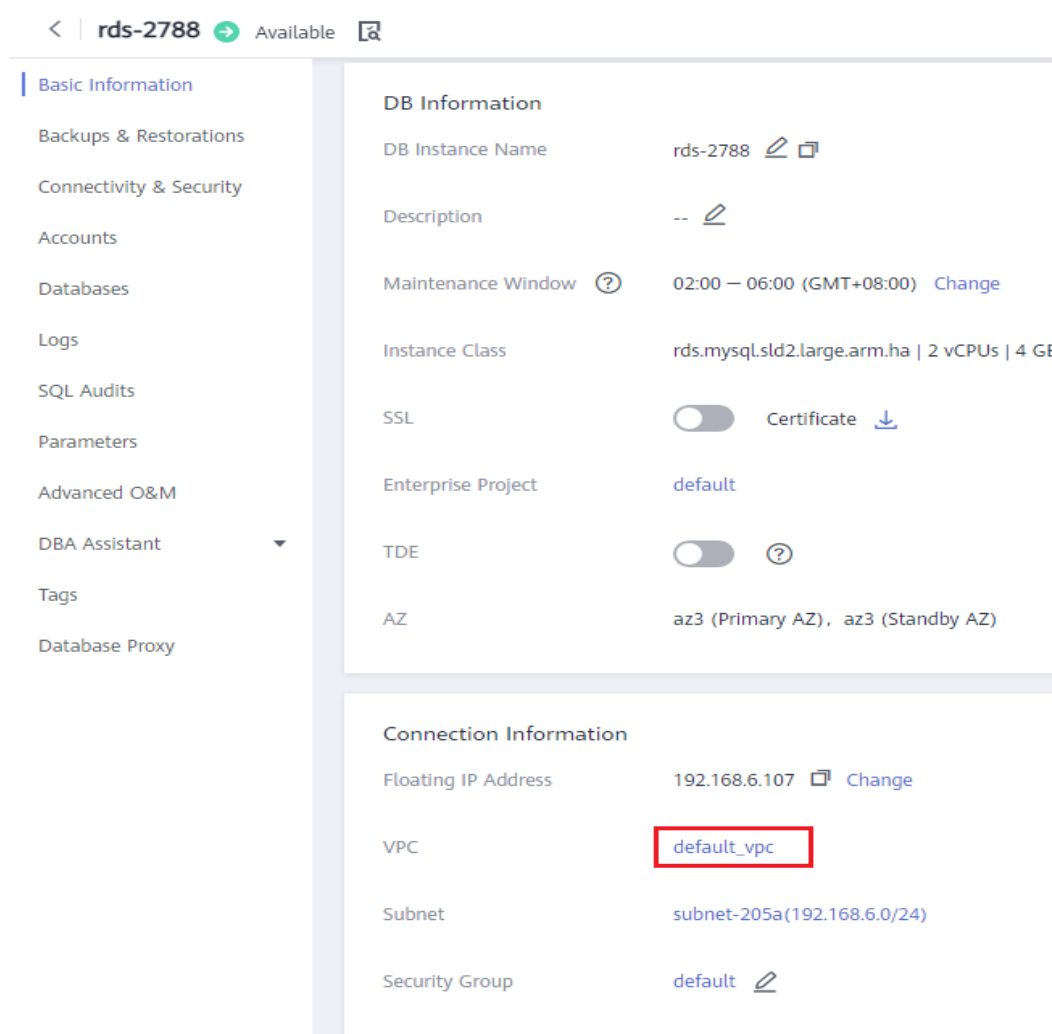
b.   Check security group rules.

  ▪   If **Destination** is not **0.0.0.0/0** and **Protocol & Port** is not **All** on the
      Outbound Rules page of the ECS, add the floating IP address and
      port of the RDS instance to the outbound rules.

      Figure 4-8 ECS security group
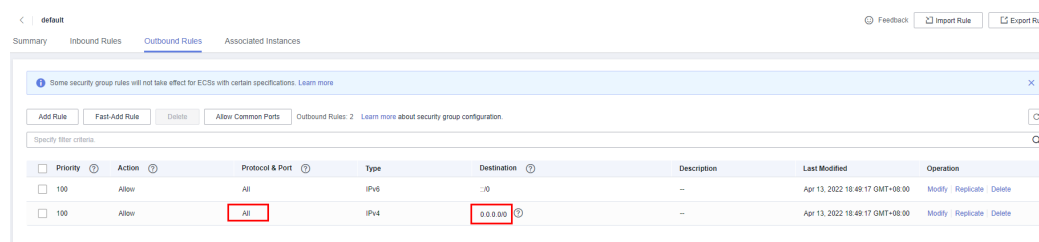
  ▪   If **Source** is not **0.0.0.0/0** and **Protocol & Port** is not **All** on the
      Inbound Rules page of the RDS instance, add the IP address and
      port of the ECS to the **inbound rules**.

Figure 4-9 RDS instance security group

c. On the ECS, check whether the DB instance port can be connected to.

telnet *<IP address> <port number>*

- If the connection is normal, the network is normal.

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

Public network connection

a. Check security group rules.

- If **Destination** is not **0.0.0.0/0** and **Protocol & Port** is not **All** on the **Outbound Rules** page of the ECS, add the EIP and port of the RDS instance to the outbound rules.

Figure 4-10 ECS security group

- If **Source** is not **0.0.0.0/0** and **Protocol & Port** is not **All** on the **Inbound Rules** page of the RDS instance, add the IP address and port of the ECS to the **inbound rules**.

Figure 4-11 RDS instance 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 yes, **add an ICMP rule to allow traffic**.

The default network ACL rule denies all inbound and outbound packets. This default rule is still applied even if the network ACL is disabled.
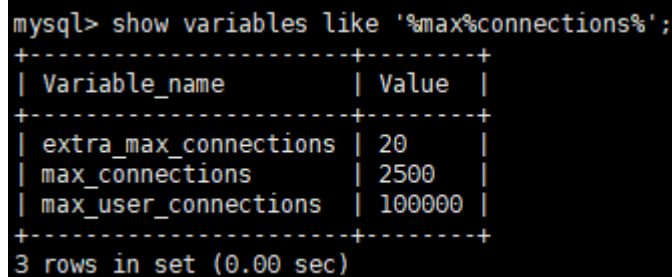
c. Ping the DB instance on an ECS in the same region.

If you cannot ping the RDS instance's EIP from an ECS, try pinging it from another ECS in the same region. If the EIP can be pinged, the network is normal. In this case, **create a service ticket** to contact customer service.

6. **Check whether there are too many connections to the DB instance.**

Check method:

a. Run **show variables like '%max%connections%';** to view the number of instance connections.

```
mysql> show variables like '%max%connections%';
+-----------------------+--------+
| Variable_name         | Value  |
+-----------------------+--------+
| extra_max_connections | 20     |
| max_connections       | 2500   |
| max_user_connections  | 100000 |
+-----------------------+--------+
3 rows in set (0.00 sec)
```

- **max_connections**: the maximum number of clients that can be connected at the same time. If this parameter is set to **default**, the maximum number of clients depends on the amount of memory configured. For details, see **What Is the Maximum Number of Connections to an RDS DB Instance?**.

- **max_user_connections**: the maximum number of concurrent connections allowed for a specific RDS for MySQL account.

b. Check whether the total connections and current active connections have reached the upper limits by referring to **Viewing Monitoring Metrics**. Determine whether to release the connections.

Possible cause: If there are too many database connections, applications may be unable to connect, and full and incremental backups may fail, affecting services.

Solution:

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

b. If this parameter is set to **default**, you can scale up the DB instance to set **max_connections** to a larger value. For details, see **Changing DB Instance Specifications**.

c. Check whether any metrics are abnormal and whether any alarms are generated on the Cloud Eye console. Cloud Eye monitors database metrics, such as the CPU usage, memory usage, storage space usage, and database connections, and allows you to set alarm policies to identify risks in advance if any alarms are generated. For details about the supported monitoring metrics, see **Configuring Displayed Metrics**.

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

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

– On the RDS console

Locate a DB instance and click its name to go to the **Basic Information** page. In the **Storage Space** area, view the storage space usage.

Figure 4-12 Storage space usage
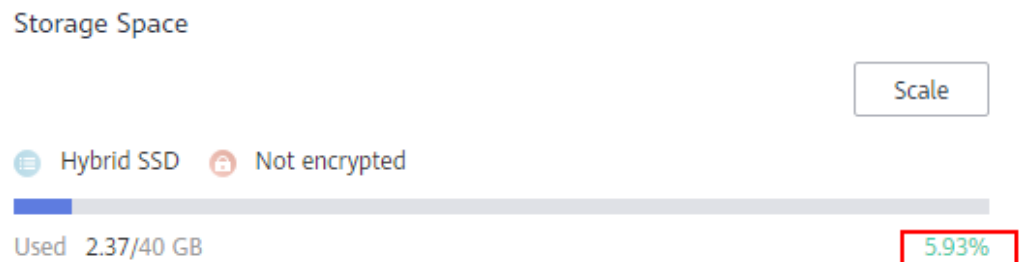
– On Cloud Eye

Locate a DB instance and click **View Metric** in the **Operation** column. On the displayed page, view the storage space usage.

Possible cause and solution: See **What Should I Do If an RDS DB Instance Is Abnormal Due to Full Storage Space?**

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

When you run commands to connect to a DB instance, understanding the error messages can help:

– ERROR 2013: Lost connection to MySQL server during query

If the values of **wait_timeout** and **interactive_timeout** are too small, RDS for 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 RDS for MySQL client can ping the DB instance's floating IP address. For details, see **RDS for 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 RDS for MySQL client connection attempts (not caused by incorrect passwords) exceeds the value of

max_connection_errors. For details, see **RDS for 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 an RDS for MySQL or RDS for 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 an RDS for MySQL or RDS for 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 an RDS for SQL Server DB instance, check whether the username or password is correct.

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

4.2 Can an External Server Access the RDS Database?

DB Instance Bound with an EIP

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

For details, see:

- **Connecting to an RDS for MySQL DB Instance Through a Public Network**
- **Connecting to an RDS for PostgreSQL DB Instance Through a Public Network**
- **Connecting to an RDS for SQL Server 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 details, see:

- **Connecting to an RDS for MySQL DB Instance Through a Private Network**
- **Connecting to an RDS for PostgreSQL DB Instance Through a Private Network**
- **Connecting to an RDS for SQL Server DB Instance Through a Private Network**

4.3 What Do I Do If the Number of RDS Database Connections Reaches the Upper Limit?

The number of database connections indicates the number of applications that can be simultaneously connected to a database, and is irrelevant to the maximum number of users allowed by your applications or websites.

If there is an excessive number of database connections, applications may fail to be connected, and the full and incremental backups may fail, affecting services.

Fault Locating

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

2. Check the specifications and scale them up if needed.

3. On the Cloud Eye console, view metrics of your DB instance to identify performance issues and set alarms for metric thresholds. Cloud Eye monitors metrics of different categories, including CPU, memory, storage, and connections. For details, see the *Cloud Eye User Guide*.

Solution

1. Connect to a DB instance through a private network. Using a private network prevents congestion caused by insufficient bandwidth.

   Follow the steps provided in:

   – **RDS for MySQL**

   – **RDS for PostgreSQL**

   – **RDS for SQL Server**

2. On the management console, set the parameter **innodb_adaptive_hash_index** to **off** to reduce lock wait time. For operation details, see **Modifying Parameters**.

3. Optimize slow queries.

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

RDS does not have constraints on how many connections are supported. It depends on the default values and value ranges of the following parameters: **max_connections** and **max_user_connections** for the MySQL DB engine and **max_connections** for the PostgreSQL DB engine. You can customize these parameters in a parameter template.

- For details about the number of connections supported for RDS for MySQL DB instances, see **RDS for MySQL Performance White Paper**.

- For details about the number of connections supported for RDS for PostgreSQL DB instances, see **RDS for PostgreSQL Performance White Paper**.

Changing the Maximum Number of Connections

- RDS for MySQL

  You can change the maximum number of connections on the console. For details, see **Modifying Parameters**.

  Or, you can query or change the maximum number of connections allowed using commands.

  a. Querying the maximum number of connections
     show global variables like 'max_connections';

  b. Changing the value of **max_connections** under **mysqld** in the **my.cnf** file
     [mysqld]
     max_connections = 1000

- RDS for PostgreSQL

  You can change the maximum number of connections allowed on the console. For details, see **Modifying Instance Parameters**.

  You can query the maximum number of connections allowed using commands.

  show max_connections;

  If you want to change the maximum number of connections allowed using commands, contact Huawei technical support.

Setting the Maximum Number of Connections to an Appropriate Value

- RDS for MySQL

  - In addition to the value of **max_connections**, the maximum number of concurrent client connections allowed by RDS for MySQL is also limited by the maximum number of files that can be opened by a single process in the operating system. For example, if the maximum number of files that can be opened by each process is set to **100** in the operating system, the **max_connections** parameter does not take effect even if it is set to **200**.

  - Check the maximum number of files that can be opened by a single process in the operating system. The default value is **1024**.
    ulimit -n

  - Check the value of **open_files_limit**. **open_files_limit** indicates the maximum number of files that can be opened by a single process, which is read from the operating system during RDS for MySQL startup.
    show variables like 'open_files_limit';

  - Suggestions

    The maximum number of RDS for MySQL connections can be modified to any amount allowed by your instance specifications. The maximum number of connections supported is closely related to the instance memory.

    max_connections: maximum number of concurrent connections to a DB instance. If this parameter is set to **default**, the maximum number of connections depends on the memory (unit: GB) of the DB instance. The formula is as follows:

    Estimated value of max_connections = Available node memory/ Estimated memory occupied by a single connection

📖 **NOTE**

- Available node memory = Total memory – Memory occupied by the buffer pool – 1 GB (mysqld process/OS/monitoring program)
- Estimated memory usage of a single connection (single_thread_memory) = thread_stack (256 KB) + binlog_cache_size (32 KB) + join_buffer_size (256 KB) + sort_buffer_size (256 KB) + read_buffer_size (128 KB) + read_rnd_buffer_size (256 KB) ≈ 1 MB

The following table lists the default values of **max_connections** for different memory specifications.

Table 4-2 Max_connections for different memory specifications

Memory (GB)	Connections
512	100,000
384	80,000
256	60,000
128	30,000
64	18,000
32	10,000
16	5,000
8	2,500
4	1,500
2	800

Set the maximum number of connections to an appropriate value because more connections consume more system resources.

- RDS for PostgreSQL

  Set **max_connections** based on the complexity of your workloads. For details, see **Instance Usage Specifications**.

4.5 How Can I Create and Connect to an ECS?

1. For details about how to create an ECS, see *Elastic Cloud Server User Guide*.

   – If you connect to an RDS DB instance through a private network, ensure that the ECS and DB instance are in the same VPC. If you connect to an RDS DB instance through a public network, the ECS and DB instance can be in different VPCs.

   – Configure a security group to allow the ECS to access the RDS DB instance through the IP address.

2. For details about how to connect to an ECS, see "Logging In to an ECS" in *Elastic Cloud Server User Guide*.

4.6 What Should I Do If an ECS Cannot Connect to an RDS DB Instance Through a Private Network?

Perform the following steps to identify the problem:

Step 1 Check whether the ECS and RDS DB instances are located in the same VPC.

- If they are in the same VPC, go to **Step 2**.
- If they are in different VPCs, create an ECS in the VPC in which the RDS DB instance is located.

Step 2 Check whether the security group rules of the ECS instance are appropriate.

For RDS for MySQL instances, see **Configuring Security Group Rules**. Then, go to **Step 3**.

Step 3 On the ECS, check whether the RDS DB instance port can be connected.

The default port of RDS for MySQL is **3306**.

The default port of RDS for PostgreSQL is **5432**.

The default port of RDS for SQL Server 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 and no further action is required.
- If the ECS still cannot connect to the port, contact technical support.

----End

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

Troubleshoot RDS connection failures caused by a client problem by checking the following items:

1. ECS Security Policy

   In Windows, check whether the RDS instance port is enabled in the Windows security policy. In Linux, run **iptables** to check whether the RDS instance port is enabled in firewall settings.

2. Application Configuration

   Check whether the connection address, port parameter configuration, and JDBC connection parameter configuration are correct.

3. Username or Password

   Check whether the username or password is correct if an error similar to the following occurs during RDS DB connection:

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

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

– **Login failed for user 'username'**

 NOTE

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

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

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

1. The RDS DB instance is not properly connected.

   Solution: Check the connection. If you connect to the RDS DB instance through a private network, the ECS and DB instance must be in the same VPC and the DB instance can be accessed only through an ECS in the same VPC. If you connect to the RDS DB instance through a public network, the ECS and DB instance can be in different VPCs.

2. The maximum number of connections has been reached.

   Solution: Use RDS resource monitoring to check if the CPU usage and the number of current connections are abnormal. If either of them has reached the maximum, reboot, disconnect, or scale up the class of the RDS DB instance.

3. The DB instance is abnormal. For example, the RDS DB instance fails to be rebooted, the system is faulty, or the instance or table is locked.

   Solution: Reboot the RDS DB instance to see if the problem is resolved. If the problem persists, contact post-sales technical support.

4.9 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.

4.10 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.

To reduce resource consumption and improve performance, configure your applications to connect to the database using a persistent connection.

4.11 Why Cannot I Ping My EIP After It Is Bound to a DB Instance?

Fault Location

1. Check security group rules.

2. Check network ACLs.

3. Ping the affected EIP from another ECS in the same region.

Solution

1. Check security group rules.

   a. **Log in to the management console**.

   b. Click ⌖ in the upper left corner and select a region and a project.

   c. Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

   d. On the **Instances** page, click the target DB instance.

   e. In the **Connection Information** area, click the security group.

   f. Check whether the ECS NIC security group allows the inbound ICMP traffic.

   Table 4-3 Security group rules

Direction	Type	Protocol/Port Range	Source IP Address
Inbound	IPv4	Any: Any	0.0.0.0/0 (all IP addresses)
Inbound	IPv4	ICMP: Any	0.0.0.0/0 (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. If the network ACL is disabled, the default rule still takes effect.

3. Ping the affected EIP from another ECS in the same region.

   If the affected EIP can be pinged from another ECS in the same region, the virtual network is functional. In this case, contact technical support.

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

Scenario

EIPs obtained through tools are inaccurate. Therefore, applications still cannot be connected to RDS DB instances even though you have added IP addresses to a whitelist. This section describes how to obtain a local IP address.

Procedure

Step 1 Add IP addresses or IP address ranges that are allowed to access DB instances to the RDS whitelist.

Step 2 Use the MySQL client to connect to an RDS for MySQL DB instance.

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

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

Enter password:

For example, if you run the following command as user **root** to connect to a DB instance:

mysql -h 172.16.0.31 -P 3306 -u root -p
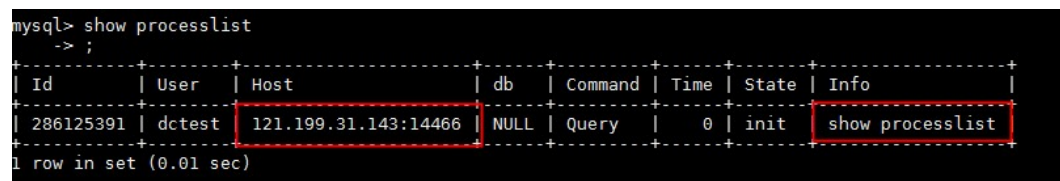
Enter password:

Step 3 Query process information.

show processlist

Figure 4-13 shows the query result. The outbound IP address is the host IP address in the "show processlist" row of the Info field.

Figure 4-13 IP query result

Step 4 View historical connection sources in audit logs if you have **enabled SQL audit**.

If this function is disabled, historical records cannot be viewed.

----End

4.13 What Should I Do If an RDS for 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.

  In private network connection mode, the ECS and RDS DB instance must be in the same VPC and the DB instance can be accessed only through an ECS in the same VPC. In public network connection mode, the ECS and DB instance can be in different VPCs.

- Check whether the IP address and port are correct.

  Use a colon to separate the IP address and port.

- 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 in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

Step 4 On the **Instances** 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

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

By default, RDS DB instances cannot be accessed over an intranet across regions. Cloud services in different regions cannot communicate with each other over an intranet. You can use EIP, Cloud Connect (CC), or Virtual Private Network (VPN) to connect to RDS instances across regions.

- You can access RDS instances across regions using EIP.
  - For RDS for MySQL instances, see **Using MySQL CLI to Connect to an Instance Through a Public Network**.
  - For RDS for PostgreSQL instances, see **Using psql CLI to Connect to an Instance Through a Public Network**.
  - For RDS for SQL Server instances, see **Connecting to an Instance Through a Public Network**.
- CC allows you to connect VPCs in different regions, even if they are not owned by the same account. For details, see **Communications Among VPCs of the Same Account**.
- VPN uses an encrypted tunnel to connect VPCs in different regions and sends traffic over the Internet. It is inexpensive, easy to configure, and easy to use. However, the quality of VPN connections depends on the quality of your Internet connection. For details, see **Connecting to a VPC Through a VPN**.

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

For DB instances connected using 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.

4.16 Will My Access Be Restricted by Bandwidth When I Connect to My Instance from an ECS over a Private Network?

No.

4.17 Why Did the New Password Not Take Effect After I Reset the Administrator Password?

Possible Causes

You may have restored from a backup before you reset the administrator password.

Locating Method

Check whether the DB instance was restored after you reset the administrator password.

Solution

Log in to the RDS console and reset the administrator password again. For details, see **Resetting the Administrator Password**.

4.18 Will I Be Logged Out If the Connection to RDS for SQL Server Instances Times Out?

No, you will not be logged out if the connection times out. You can modify the **remote query timeout** parameter to adjust how long a remote operation can take in seconds before RDS for SQL Server times out. The default value is **600**, which is a 10-minute wait. This value applies to an outgoing connection initiated by the DB engine as a remote query. This value has no effect on queries received by the DB engine. For details about how to modify parameters, see **Modifying Parameters**.

4.19 How Do I Set the Encoding Format of the MySQL 8.0 Character Set?

1. Set **character_set_server** to **utf8** and **collation_server** to **utf8_general_ci**.

   a. **Log in to the management console**.

   b. Click ⊙ in the upper left corner and select a region and a project.

   c. Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

   d. On the **Instances** page, click the instance name.

   e. In the navigation pane on the left, choose **Parameters**.

   f. Search for **character_set_server** and **collation_server**, respectively, in the search box.

   g. Set the parameters to **utf8** and **utf8_general_ci**, respectively, and click **Save**.

2. If you use a client of PHP 7.1.x, change the PHP version because it will fail to connect to MySQL 8.0 DB instances with the utf8mb4 character set.

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

1. Change the VPC hosting the ECS to the same as that hosting the RDS.

2. Create a VPC peering connection.

4.21 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;

4.22 Can I Access Standby RDS DB Instances?

No. You can directly access primary DB instances and read replicas. Standby DB instances are not visible to users and therefore you cannot access them directly.

RDS supports primary/standby failover and switchover. Data is synchronized between the primary and standby instances in real time.

4.23 How Do I Check the Connections to an RDS for MySQL Instance?

Use either of the following methods:

- Log in to the instance as user **root** and run the following command to view the threads running on it:

  show full processlist;

  – **Id**: Thread ID. You can use **kill** *id* to terminate a thread.

  – **User**: User used for connecting to the instance.

  – **Host**: IP address and port of the host that connects to the instance.

  – **db**: Database name.

  – **Command**: Connection status, which is usually **Sleep**, **Query**, or **Connect**.

  – **Time**: Connection duration, in seconds.

  – **State**: Status of the SQL statement being executed.

  – **Info**: SQL statement that is being executed.

  – **Memory_used**: Memory usage of the current connection.

  – **Memory_used_by_query**: Memory usage of the current query.

  – **CPU_time**: Amount of time for which the current connection has been established. (Such information is not collected, so this column is left blank.)

- **Trx_executed_time**: Execution time of the current transaction.

- On the **Instances** page, locate the instance and click **View Metric** in the **Operation** column.

View **Total Connections**. Generally, the primary and standby DB instances occupy two connections. If there are more than two connections, the instance is being connected and used by other users.
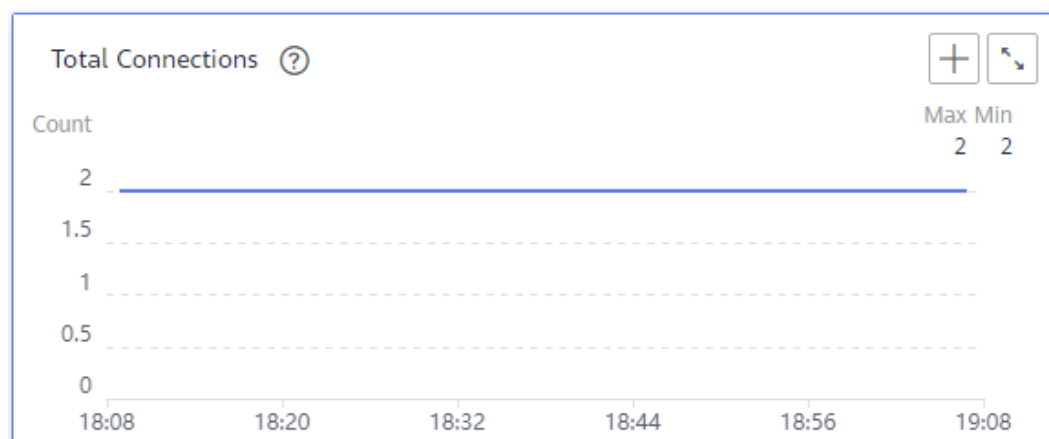
5 Database Migration

5.1 Why Do I Need to Use the mysqldump or pg_dump Tools for Migration?

The mysqldump or pg_dump tool is easy to use for data migration. However, when you use this tool, the server is stopped for a long period of time during data migration. Only use these tools when there is not much data to migrate or if stopping the server for a long period of time is not an issue.

RDS is compatible with source database services. The procedure for migrating data from your database to RDS is similar to the procedure for migrating data from one database server to another.

5.2 What Should I Do When a Large Number of Binlog Files Cause Storage Space Insufficiency During an RDS MySQL Instance Migration?

During an RDS for MySQL DB instance migration, a large number of binlog files are generated in a short period of time, causing insufficient data disk space (disk usage: 91%) and affecting services.

Solution

1. Clear expired data in a timely manner.

2. As your service data grows, the original storage space may be insufficient. If this happens, scale up storage space for your DB instance.

   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.

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

5.3 What Types of DB Engines Does RDS Support for Importing Data?

- Exporting or importing data between DB engines of the same type is called homogeneous database export or import.

- Exporting or importing data between DB engines of different types is called heterogeneous database export or import. For example, import data from Oracle to DB engines supported by RDS.

  Generally, data cannot be exported or imported between heterogeneous databases due to the different data formats involved. However, if the data formats are compatible, table data can, in theory, be migrated between them.

  Third-party software is usually required for data replication to export and import between heterogeneous databases. For example, you can use a third-party tool to export table records from Oracle into a .txt file. Then, you can use LOAD statements to import the exported table records to a DB engine supported by RDS.

6 Database Permission

6.1 Why Does the Root User Not Have the Super Permissions?

RDS does not provide super permissions for the **root** user. The super permissions allow you to execute management commands, such as **reset master**, **set global**, **kill**, and **reset slave**. These operations may cause primary/standby replication errors.

If you need to perform operations that require super permissions, RDS provides alternative methods.

- Scenario 1: If you cannot run the following command on an RDS instance to modify parameter values, you can modify parameter values through the RDS console.

  set global parameter name=_Parameter value_;

  If the script contains the **set global** command, delete the **set global** command and modify parameter values on the RDS console.

- Scenario 2: An error is reported after you run the following command because the **root** user does not have the super permissions. To solve this problem, delete **definer='root'** from the command.

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

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

- Scenario 3: If you cannot create RDS for PostgreSQL plugins due to lack of super permissions, see **Creating or Deleting a Plugin**.

6.2 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.

6.3 RDS for MySQL Built-in Accounts

When you create an RDS for MySQL DB instance, RDS automatically creates certain system accounts (unavailable to users) for O&M operations. The system accounts include:

- mysql.session: used by plugins to access the server.
- mysql.sys: used to define objects in the sys schema.
- rdsAdmin: a management account with superuser permissions. It is used to query and modify instance information, rectify faults, migrate data, and restore data.
- rdsRepl: a replication account, used to synchronize data from the primary instance to the standby instance or read replicas.
- rdsMetric: a metric monitoring account used by watchdog to collect database status data.
- rdsbackup: a backup account used for background backup.
- dsc_readonly: used to anonymize data.

6.4 Does RDS for MySQL Support Multiple Accounts?

Yes, RDS for MySQL supports multiple accounts. You can assign different rights to these accounts through authorization commands to control access to different tables. Each table can be controlled independently.

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 **Relational Database Service Performance White Paper**.

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

6.5 Can Multiple Users Log In to DAS at the Same Time? Will the Accounts Be Locked If I Enter Wrong Passwords Several Times in a Row?

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

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

6.6 Why Did I Fail to Create an Object on the postgres Database as a Common User?

Symptom

- **Creating a Schema as a Common User**

  Command: **CREATE SCHEMA my_schema;**

  Error: ERROR: permission denied for database postgres
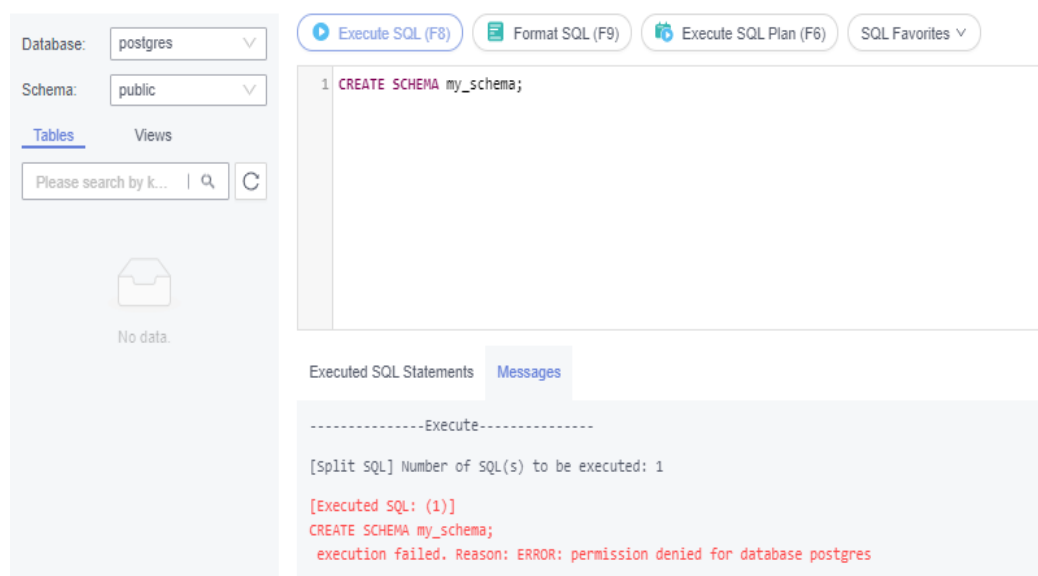
- **Creating a Table as a Common User**

  Command: **CREATE TABLE my_table(id int PRIMARY KEY,name VARCHAR(30));**

  ERROR: permission denied for schema public
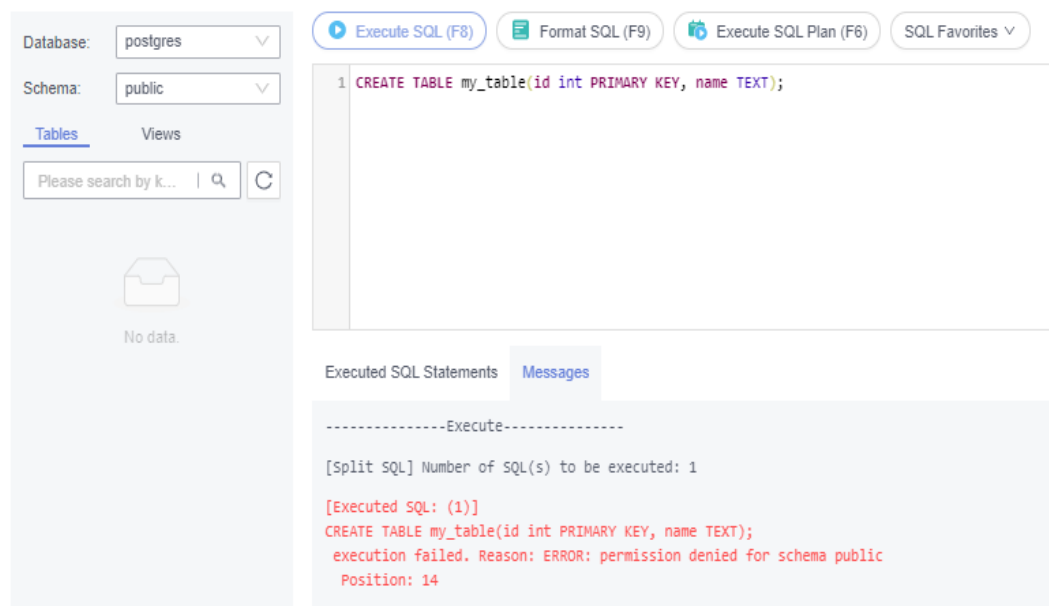
Solution

A common user cannot create objects on the **postgres** database, but a **root** user can.

☐ **NOTE**

Switch to user **root** and ensure that your database kernel allows for root privilege escalation. For details, see **Privileges of the root User**.

Privileges of the root User

RDS for PostgreSQL does not provide super user permissions but provides permissions for the **root** user.

To create objects on an RDS for PostgreSQL database without operation risks, escalate your account to root privileges when necessary.

The following table describes root privilege escalation in different versions.

Table 6-1 Privileges of the **root** user

Version	Whether to Escalate Privileges	Initial Version for Privilege Escalation
Pgcore9	No	N/A
Pgcore10	No	N/A
Pgcore11	Yes	11.11
Pgcore12	Yes	12.6
Pgcore13	Yes	13.2
Pgcore14	Yes	14.4

Escalate to root privileges when you need to:

- Create an event trigger.
- Create a wrapper.
- Create a logical replication publication.
- Create a logical replication subscription.
- Query and maintain replication sources.
- Create a replication user.
- Create a full-text index template and parser.
- Run the **vacuum** command on a system table.
- Run the **analyze** command on a system table.
- Create a plugin.
- Grant an object permission to a user.

6.7 What Should I Do If a Role Failed to Be Deleted from an RDS for PostgreSQL Instance?

Symptom

Role **test** failed to be deleted from an RDS for PostgreSQL instance by running the **DROP ROLE test;** command on the DAS console.
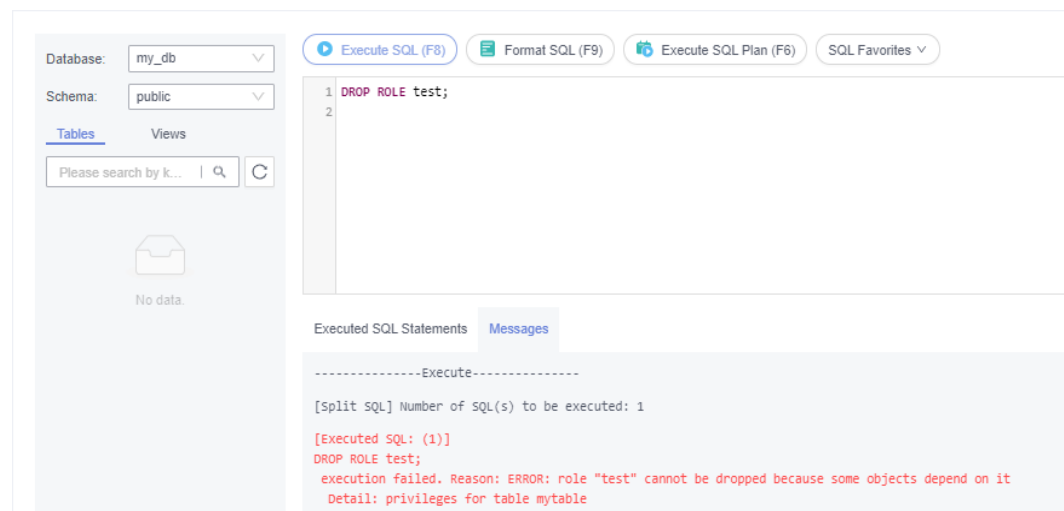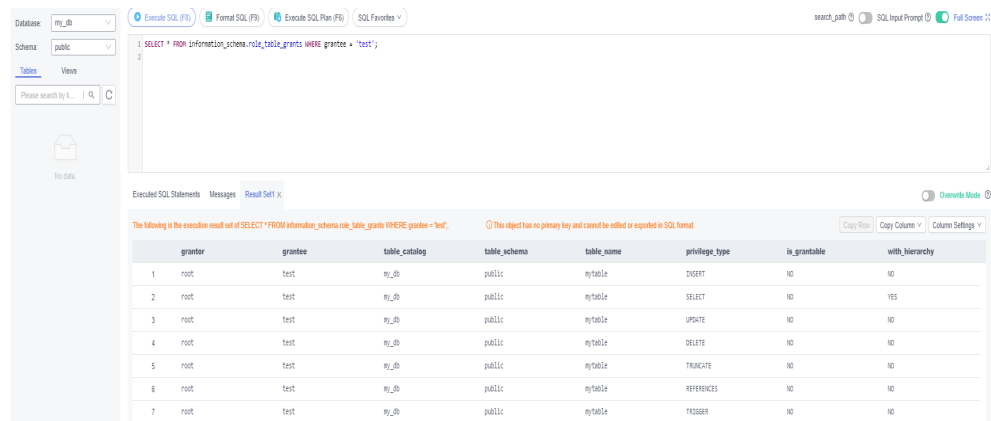
Possible Causes

Role **test** cannot be deleted probably because it is associated with objects. Before deleting this role, revoke the permissions of its associated objects.

Solution

1. Check the permissions of the role.

   select * from INFORMATION_SCHEMA.role_table_grants WHERE grantee='test';
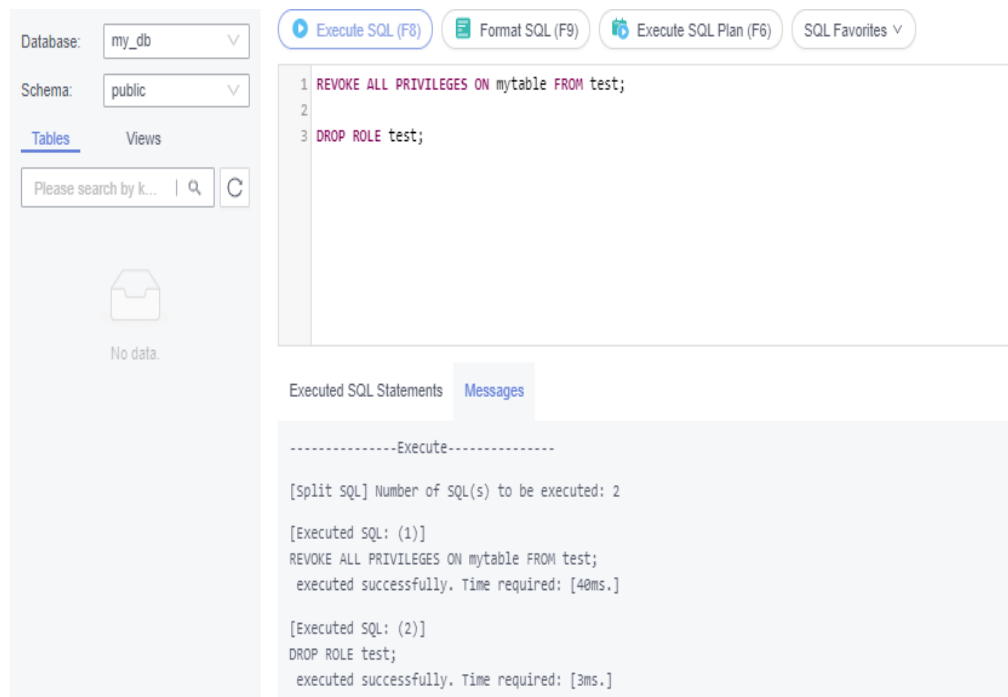
2. If role **test** is associated with objects, revoke the permissions of the objects and then delete the role.

   REVOKE ALL PRIVILEGES ON mytable FROM test;

   DROP ROLE test;

6.8 Why Did My RDS for PostgreSQL Migration Fail?

Symptom

An error is reported when user **root** uses DRS to migrate RDS for PostgreSQL database data. In this case, you need to switch to another account or grant permissions to the current account.

Possible Causes

The migration may have failed because user **root** may not have permissions to operate certain objects when migrating the database using DRS.

Solution

1. Log in to the database as user **root** and run the following statements.
   grant USAGE on schema public to root;
   grant SELECT,REFERENCES,TRIGGER on all tables in schema public to root;
   grant EXECUTE on ALL FUNCTIONS IN SCHEMA public to root;

2. After the migration is complete, revoke the permissions.
   revoke USAGE schema public from root;
   revoke SELECT,REFERENCES,TRIGGER on all tables in schema public from root;
   revoke EXECUTE on ALL FUNCTIONS IN SCHEMA public from root;

☐ **NOTE**
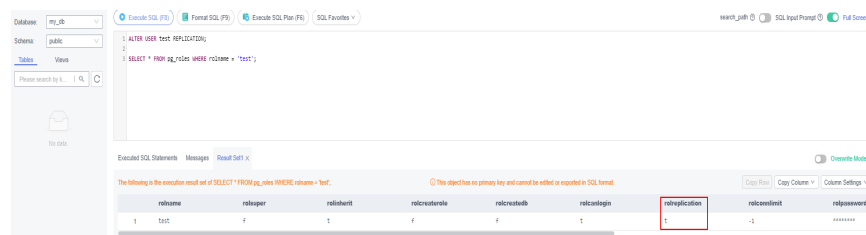
You can run the commands to grant permissions as user **root** only when your database kernel version supports root privilege escalation. For details, see **Privileges of the root User**.

6.9 How Do I Grant the REPLICATION Permission to an RDS for PostgreSQL Database User?

1. Log in to the database as user **root**.

2. Grant the REPLICATION permission to your account and query the pg_roles table to verify that the permission has been granted.

   ALTER USER <user> REPLICATION;

   SELECT * FROM pg_roles;

☐ **NOTE**

You can run the commands to grant permissions as user **root** only when your database kernel version supports root privilege escalation. For details, see **Privileges of the root User**.

6.10 Why Is An Error Reported When I Attempt to Change a Table Owner of the RDS for PostgreSQL Database?

Symptom

An error is reported when the owner of the PostgreSQL database table **mytable** is being changed to user **test**. The PostgreSQL database is named **my_db** and created by user **root**.

ALTER TABLE mytable OWNER TO test;

Possible Causes

The error is displayed because user **root** has not escalated the privilege.

◻ **NOTE**

After the privilege is escalated, user **root** has the permission to assign the table owner to another user.

Solution

1. Log in to the database as user **test**.
2. Run the following command as user **test**:

   GRANT test TO root;
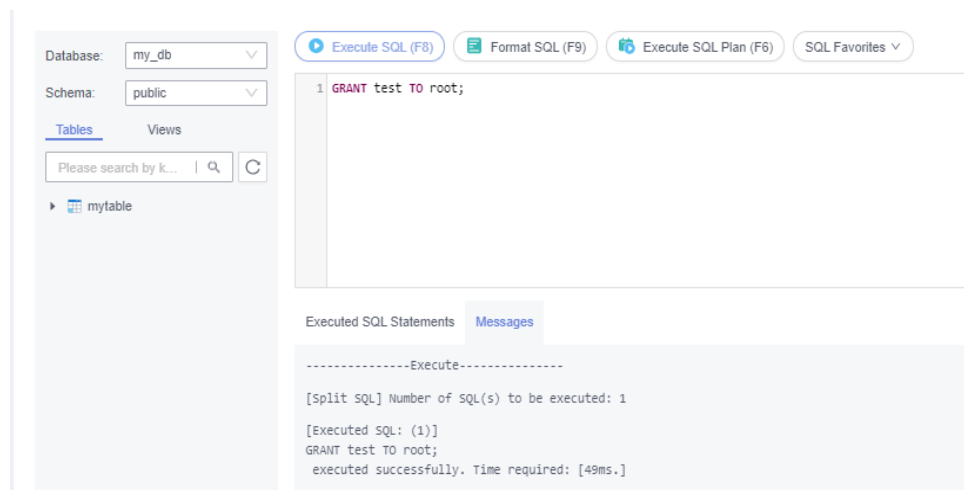
3. Log in to the database as user **root**.
4. Run the following command as user **root** to change the owner of the **mytable** table:

   ALTER TABLE mytable OWNER TO test;
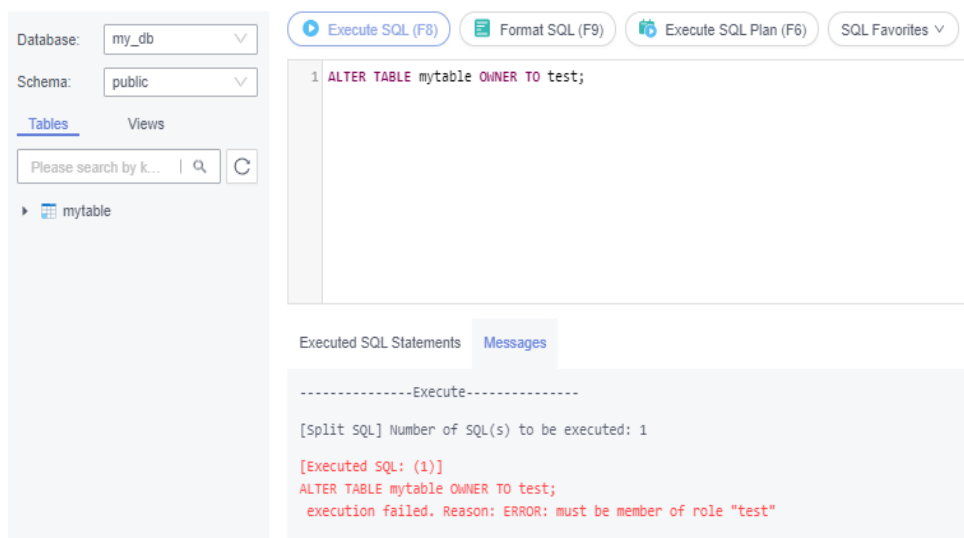
6.11 How Are the Login Name Permissions of RDS for SQL Server 2017 Enterprise Edition Primary/Standby DB Instances Synchronized to Its Read Replicas?

- The Login Name permissions created by the primary DB instance are automatically synchronized to read replicas once per minute. Wait for about a minute until the synchronization is complete, and 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 once a 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 read replicas, the account password is synchronized to read replicas from the primary instance. Changing the Login Name permissions on read replicas will not have any effect.

6.12 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 DB instance will be automatically synchronized to the standby DB instance and read replicas.

6.13 How Do I View Authorized Databases After a Local Client Is Connected to a DB Instance?

After connecting to the database on a local client, run the following command to grant permissions to view the database. In the command, *ip* indicates the local IP address.

show grants for root@'*ip*';

show grants for root@'%';

7 Database Storage

7.1 What Storage Engines Does RDS for MySQL Support?

The database storage engine is a core service for **storing, processing, and protecting data**. It can be used to control access permissions and rapidly process transactions to meet enterprise requirements.

InnoDB Storage Engine

For RDS for MySQL databases, only InnoDB supports backups and restorations and is therefore recommended.

Other Storage Engines

Table 7-1 lists the storage engines not supported by MySQL 5.6 or later versions.

Table 7-1 Unsupported storage engines

Storage Engine	Reason
MyISAM	• MyISAM engine tables do not support transactions. They only support table-level locks. As a result, read and write operations conflict with each other. • MyISAM is not good at protecting data integrity. Data can be damaged or lost. • If data is damaged, MyISAM does not support data restoration provided by RDS for MySQL. Data can only be restored manually. • Data can be transparently migrated from MyISAM to InnoDB without changing code.

Storage Engine	Reason
FEDERATED	• If primary/standby DB instances support FEDERATED, the same DML operations will be repeatedly executed on remote databases, and the data will become disordered. • For PITR restoration, after a full backup is restored, data on remote databases is not restored to the state it was in when the full backup was created. Accessing data during an incremental restoration will disorder FEDERATED table data.
MEMORY	• If a memory table becomes empty after a restart, the database adds a DELETE event to the binlog when the table is opened. If a primary/standby DB instance uses memory tables and the standby instance (or a read replica) is restarted, a GTID is generated, which makes the standby inconsistent with that of the primary instance. As a result, the standby instance (read replica) has to be rebuilt. • Using memory tables may cause out-of-memory (OOM) errors and even service terminations.

7.2 What Types of Storage Does RDS Use?

RDS uses Elastic Volume Service (EVS) disks for storage. For details, see **Elastic Volume Service Service Overview**.

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

7.3 Does RDS for MySQL Support Stored Procedures and Functions?

Yes.

- Stored procedures and functions are a set of SQL statements that have been compiled and stored in databases. Invoking stored procedures and functions reduces the amount of data that needs to be transmitted between databases and application servers, which improve data processing efficiency.

- Differences between stored procedures or functions:
  - A function must have a return value, but a stored procedure does not.
  - The parameters of a stored procedure can be of the IN, OUT, and INOUT type, but the parameters of a function can only be of the IN type.

For details about how to create a stored procedure and a function, see the **official document**.

7.4 What Should I Do If My Data Exceeds the Available Storage of an RDS for MySQL Instance?

Symptom

There is not enough storage available for an RDS instance and the instance becomes read-only, so applications cannot write any data to the instance.

You can check which data or files occupy too much storage in the **Disk Space Distribution** area on the **Storage Analysis** page. For details, see **Storage Analysis**.

Figure 7-1 Disk space distribution
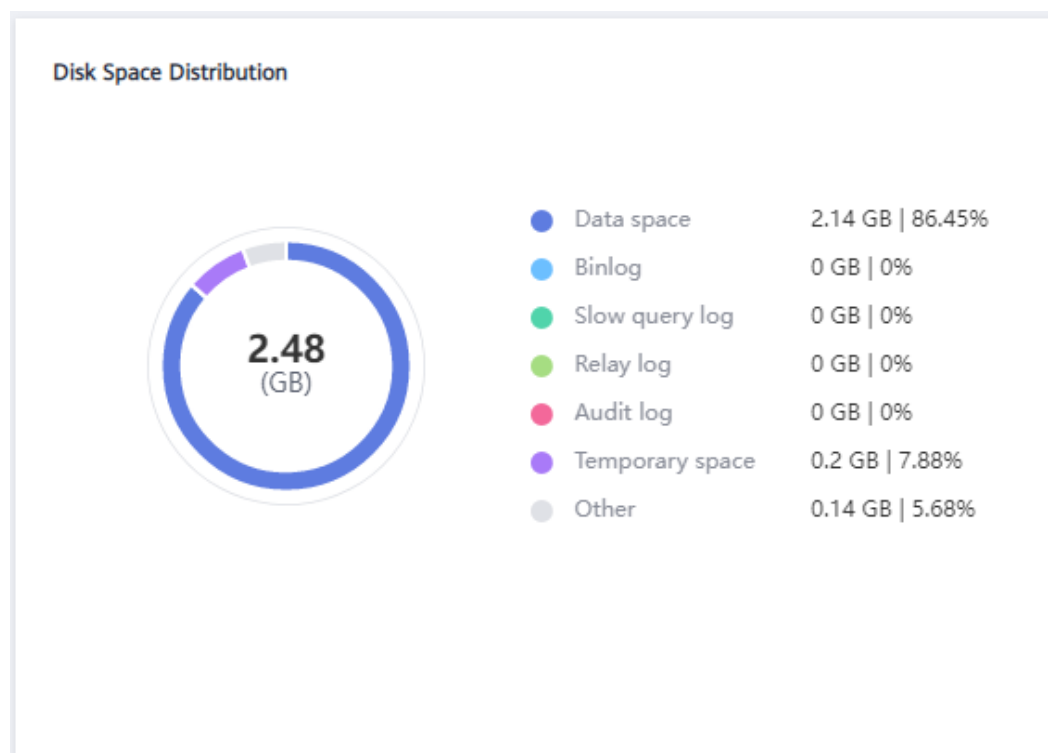
Causes

1. Increased workload data
2. Too much data being stored
3. Too many RDS for MySQL binlogs generated due to a large number of transactions and write operations
4. Too many temporary files generated due to a large number of sorting queries executed by applications

Solution

1. For insufficient storage caused by increased workload data, **scale up storage space**.

If the original storage has reached the maximum, **upgrade the specifications** first.

For instances using cloud disks, you can configure **autoscaling** so that RDS can autoscale your storage when the storage usage reaches the specified threshold.

2. If too much data is stored, delete unnecessary historical data.

   a. If the instance becomes read-only, you need to contact customer service to cancel the read-only status first.

   b. Check the top 50 databases and tables with large physical files and identify the historical table data that can be deleted. For details, see **Storage Analysis**.

   c. To clear up space, you can optimize tables with a high fragmentation rate during off-peak hours.

      To delete data of an entire table, run **DROP** or **TRUNCATE**. To delete part of table data, run **DELETE** and **OPTIMIZE TABLE**.

3. If binlog files occupy too much space, **clear local binlogs**.

4. If temporary files generated by sorting queries occupy too much storage space, optimize your SQL statements.

   You can query **slow query logs** and **top SQL statements**, and analyze and optimize the problematic SQL statements.

5. Subscribe to daily health reports to obtain SQL and performance analysis results, including slow SQL analysis, all SQL analysis, performance & storage analysis, and performance metric trend charts. You can receive a diagnosis report if there are any risks detected.

   For details, see **Daily Reports**.

7.5 How Do I View the Storage Usage of My RDS Instance?

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

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

Step 4 On the **Instances** page, click the DB instance name.

Step 5 On the **Basic Information** page, view the storage space usage in the **Storage Space** area.

Figure 7-2 Storage space
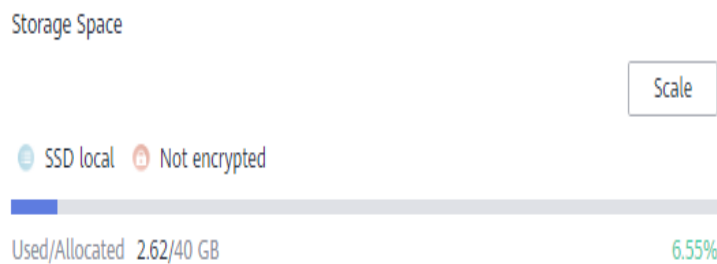
----**End**

7.6 Where Are the Database Files Created on My RDS for SQL Server Instance Stored?

The database files created on your RDS for SQL Server instance are stored in the **D:\RDSDBDATA\DATA** directory, which cannot be changed.

If you enabled FileStream for your instance, the filegroups must also be created in the **D:\RDSDBDATA\DATA** directory.

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 5.7 is used as an example. You can download the **latest version** or **any other version** for your project. The following procedure illustrates how to obtain the required installation package and install the MySQL client into a Red Hat Linux system.

Procedure

Step 1 Obtain the installation package.

Find the **link** to the required version on the download page. MySQL-client-5.7.31-1.el6.x86_64.rpm is used as an example in the following figure.

Figure 8-1 Download

Step 2 Upload the installation package to the ECS.

1. When you create an ECS, select an OS, such as Red Hat 6.6, and bind an EIP to it.

2. Use a remote connection tool to connect to the ECS through the bound EIP and upload the installation package to the ECS.

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

sudo rpm -ivh *MySQL-client-5.7.31-1.el6.x86_64.rpm*

📖 **NOTE**

- If there are any conflicts during the installation, add the **replacefiles** parameter to the command and try to install the client again. Example:
  rpm -ivh --replacefiles MySQL-client-5.7.31-1.el6.x86_64.rpm
- If a message is displayed prompting you to install a dependency package, you can add the **nodeps** parameter to the command and install the client again. Example:
  rpm -ivh --nodeps MySQL-client-5.7.31-1.el6.x86_64.rpm

----End

8.2 How Can I Install a PostgreSQL Client?

PostgreSQL provides **client installation methods** for different OSs on its official website.

The following describes how to install a PostgreSQL 12 client in CentOS.

Procedure

Step 1 Log in to an ECS.

1. When you create an ECS, select an OS like CentOS 7 and bind an EIP to it.
2. Use a remote connection tool to connect to the ECS through the EIP.

Step 2 Open the **client installation page**.

Step 3 Select a DB engine version, OS, and OS architecture, and run the following commands on the ECS to install a PostgreSQL client.

sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
sudo yum install -y postgresql12-server

Figure 8-2 Installing a client

- Select a DB engine version that is consistent with that of your RDS for PostgreSQL instance.
- Select an OS that is consistent with that of the ECS.

● Select an OS architecture that is consistent with that of the ECS.

Figure 8-3 Installing the RPM package

Figure 8-4 Client installed

Step 4 Connect to the RDS for PostgreSQL instance.

Figure 8-5 Connection successful

----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, 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 Database Usage

9.1 Does MySQL 8.0 Support Full-Text Search?

Yes. MySQL 8.0 supports full-text search. The keyword is FULLTEXT. Run the following SQL statements to perform a test.

- Creating a table

```
CREATE TABLE ARTICLE (
id int unsigned NOT NULL AUTO_INCREMENT,
title varchar(200) DEFAULT NULL,
Content text,
PRIMARY KEY (id),
FULLTEXT KEY title (title,content),
FULLTEXT KEY fulltext_article (title,content)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

- Creating an index
  ```
  ALTER TABLE ARTICLE ADD FULLTEXT INDEX fulltext_article (title,content);
  ```

- Querying an index
  ```
  SHOW INDEX FROM ARTICLE;
  ```

9.2 How Do I Use DAS to Query SQL Statements?

DAS is a professional database management tool with a visual interface. You can enable SQL Explorer to query related SQL statements.

Constraints

SQL Explorer cannot record all data. As for RDS for MySQL, it has the following constraints:

- Some data cannot be recorded if a buffer overrun occurs.
- Any SQL statement that exceeds 4,096 bytes is discarded by default.

> 📖 **NOTE**
>
> This constraint can be removed by setting parameter
> **rds_sql_tracer_reserve_big_records** for RDS for MySQL 5.7.33.3 or later. You can set
> this parameter to **ON** on the **Parameters** page, indicating that SQL statements
> containing more than 4,096 bytes are still recorded.

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 ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

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

Step 6 In the navigation pane, choose **Cloud DBA (Intelligent O&M)** to go to the **Instance Overview** page.

Step 7 Locate the instance you want to view and click **Details**.

Step 8 Choose **SQL** > **SQL Explorer** to view full SQL details of the instance.

Step 9 On the **SQL Statements** tab page, click **Enable DAS SQL Explorer**. Query the SQL statements executed by the current instance by time range, user, keyword, operation type, or database.

Figure 9-1 Enabling SQL Explorer
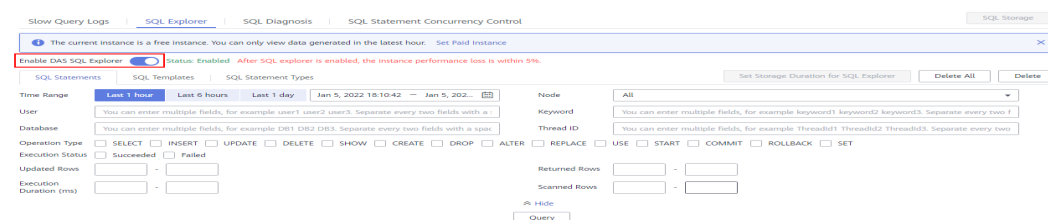
Step 10 Filter operation types by referring to **Table 9-1** and click **Export** to export the corresponding SQL statements.

Table 9-1 Common SQL statement types

Type	Keyword
DDL	CREATE, DROP, ALTER
DML	INSERT, UPDATE, DELETE, SELECT
DCL	GRANT, REVOKE

📖 **NOTE**

A maximum of 10,000 SQL statements can be displayed. If you need to view more, click **Export**.

Up to 100,000 records can be exported.

----End

9.3 How Do I Use the mysqlbinlog Tool?

This section describes how to use the mysqlbinlog tool to locally parse binlogs.

The basic unit of binlog is the binlog event. Servers write binlog files in binary format. Therefore, if you want to display the binlog content in text format, you need to use the mysqlbinlog tool to parse the binlog. Generally, this tool is stored in the same directory as mysqld.

Invoking method: **mysqlbinlog [options] log_file …**

Example: **mysqlbinlog masterbin.000001**

Example of binlog content:

at 141#210309 9:28:36 server id 123 end_log_pos 245Query thread_id=3350 exec_time=11 error_code=0

- **at 141**: starting position of the event in the binlog file.
- **#210309 9:28:36**: timestamp information, indicating that the binlog file is written at 09:28:36 on March 9, 2021 (UTC).
- **Query thread_id**: thread ID.

Common mysqlbinlog parameters:

- **--start-position**: position where the decoding starts.
- **--start-datetime**: time where the decoding starts.
- **--stop-position**: position where the decoding stops.
- **--stop-datetime**: time where the decoding stops.
- **--skip-gtids**: gtid_log_event is not printed.
- **--short-form**: Only statements are displayed.
- **--result-file**: SQL file to which binlog decoding results are written.

9.4 How Do I View Session IDs and Login and Logout Time of a Database?

- View database login and logout time in SQL audit logs. For details about how to enable SQL audit, see **Enabling SQL Audit**.
- To view sessions, run the **show processlist** command in the database.

9.5 How Do I Create a Scheduled Task?

You can create scheduled tasks on the Data Admin Service (DAS) console.

Constraints

Scheduled tasks cannot be created for RDS for SQL Server instances on 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 in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

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

Step 5 Enter the username and password and click **Log In**.

Step 6 On the top menu bar, choose **Background Tasks** > **Task Scheduling**.

Step 7 Click **Create Task**, enter the task name and execution time tolerance, and set **Type** to **Scheduled**.

- **Scheduled**: indicates that a task is executed at a scheduled point in time after being submitted. The task is executed only once.
- **Execution Time Tolerance**: indicates the length of time (in seconds) to wait for a task to be executed before it is no longer scheduled. However, this will not affect the task if it is scheduled again later.

Step 8 Under **Add SQL Statements**, click **Add**. On the displayed page, set parameters as needed and click **Save**. Then, submit the task.

----End

9.6 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 in the exported Excel file.

9.7 Does the OPTIMIZE TABLE Operation Lock Tables on an RDS DB Instance?

When the OPTIMIZE TABLE operation is performed on an RDS DB instance, the tables are locked only for a short period of time. During the table locking period, DML operations can be performed but DDL operations cannot. DML will recreate

tables, which consumes CPU and disk resources. If there are a large number of concurrent DML operations, the table will be locked for longer. To avoid impacting services, perform the OPTIMIZE TABLE operation during off-peak hours.

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

Symptom

The error shown in **Figure 9-2** is reported on SQL Server Management Studio when a database is being deleted from RDS for SQL Server primary/standby DB instances.

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

Figure 9-2 Error
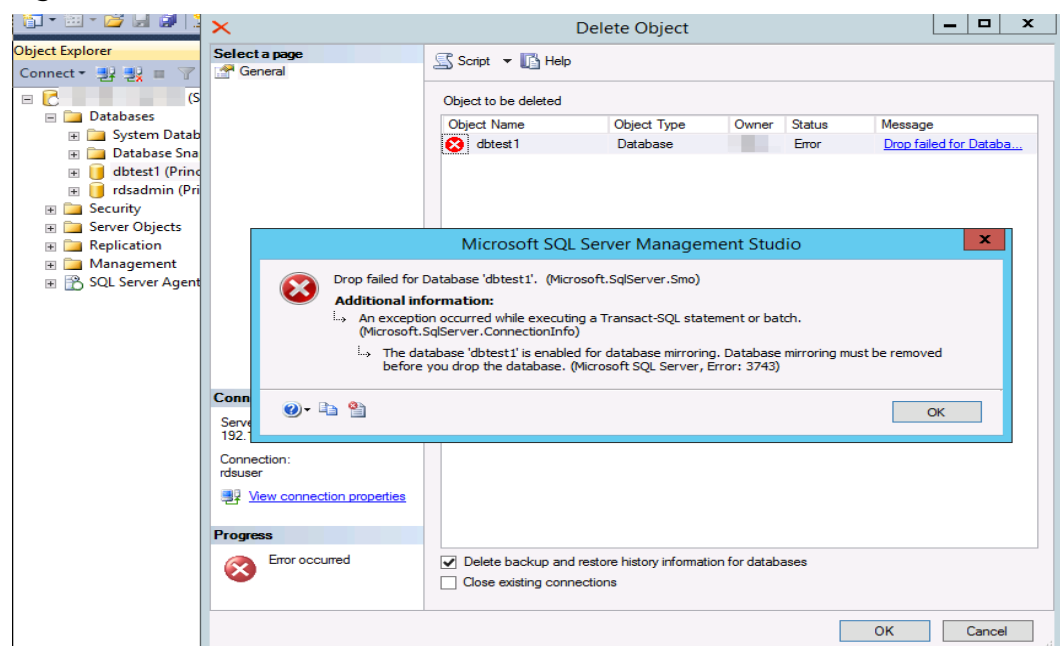
Possible Causes

The error details indicate that the RDS for 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

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

9.9 What Should I Do If My root Account Was Deleted by Mistake?

You can restore the deleted **root** account by resetting its password. For details, see **Resetting a Password for a Database Account**.

10 Backup and Restoration

10.1 How Long Does RDS Store Backup Data For?

Automated backup data is kept based on the backup retention period you specified. For details, see **Configuring an Automated Backup Policy**.

There is no limit for the manual backup retention period. You can delete manual backups as needed. For details, see **Deleting a Manual Backup**.

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

10.2 How Do I Clear RDS Backup Space?

The RDS backup space stores automated backups, manual backups, and SQL audit logs.

- **Automated full and incremental backups**

    Automated backups cannot be manually deleted. You need to change the backup retention period by referring to **Configuring an Automated Backup Policy**. Backups that have expired will be automatically deleted.

- **Manual full backups**

    You can manually delete manual backups. For details, see **Deleting a Manual Backup**.

- **SQL audit logs**

    You need to change the retention period by referring to **Enabling SQL Audit**. Audit logs that have expired will be automatically deleted.

    You can also disable SQL audit and select check box "I acknowledge that after audit log is disabled, all audit logs are deleted.".

10.3 Can My Instance Still Be Used in the Backup Window?

A backup window is a user-specified time during which RDS DB instances are backed up. With these periodic data backups, RDS allows you to restore DB instances to a point in time within the backup retention period.

- During the backup window, you can still use your instance except rebooting it on the console.
- When starting a full backup task, RDS first tests connectivity to your instance. If either of the following conditions is met, the test fails and a retry is performed. If the retry fails, the backup task fails.
  - DDL operations are being performed on the DB instance.
  - The backup lock fails to be obtained from the DB instance.

10.4 How Is RDS Backup Data Charged?

All the RDS full and binlog backups are stored on OBS without occupying the storage of your DB instances. RDS provides free backup space of the same size as your purchased storage.

The lifecycle of automated backups is the same as that of the DB instance. If you delete a DB instance, its automated backups are also deleted, but manual backups are not. For details, see **Deleting a Manual Backup**.

For example, if you purchase a DB instance with 200 GB of storage, you can get an additional 200 GB of backup space and will only be billed for backups in excess of 200 GB. The first 200 GB of backup data is free. When the 200 GB storage is used up, the backups will be billed on a pay-per-use basis. For pricing details, see **Product Pricing Details**.

> **NOTICE**
>
> If your storage is frozen, it is no longer billed and the free backup space is also unavailable.
>
> If your DB instance is frozen, no free backup space is available. As a result, the original automated backups of the DB instance will be billed.
>
> - If you unfreeze the DB instance, the free backup space will be restored.
> - If you directly delete the frozen DB instance, its automated backups will also be deleted and the backup space will not be billed any longer.

10.5 How Do I View My Backup Storage Usage?

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

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

Step 4 On the **Instances** page, click the DB instance name.

Step 5 On the **Basic Information** page, view the backup space usage in the **Backup Space** area.

Figure 10-1 Backup space
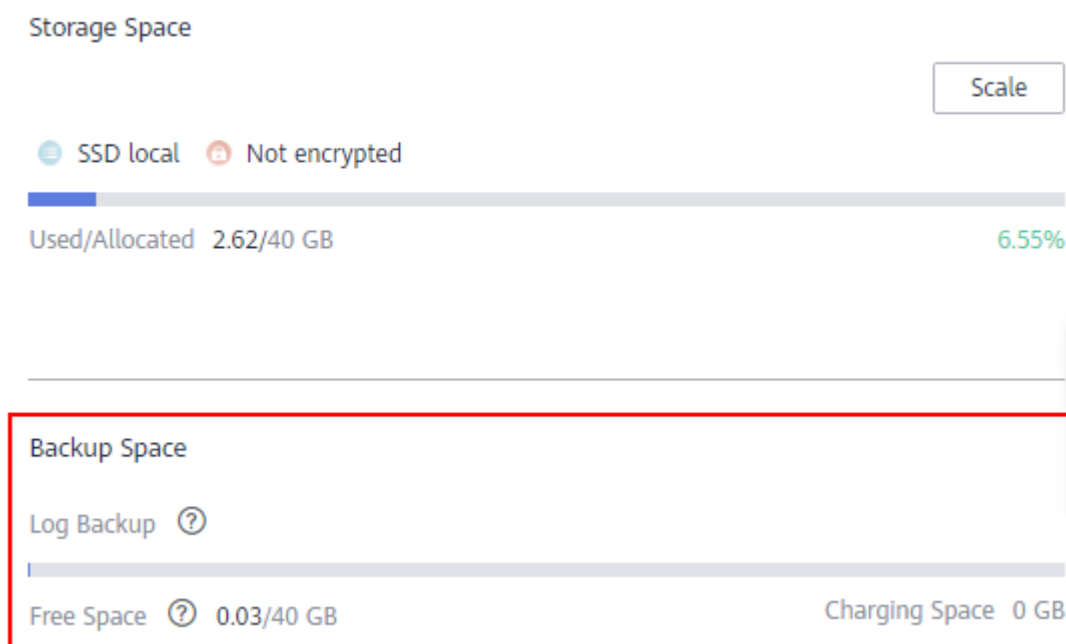
> ☐ **NOTE**
>
> The storage spaces of primary and standby instances are the same because they both need to hold the same amount of data. Free backup storage equal to your purchased storage space is also provided. If free backup space is used up, the additional space will be billed. You need to configure an automated backup policy before using the backup space.

----End

10.6 How Can I Back Up an RDS Database to an ECS?

You can back up data to an ECS the same way you export SQL statements. The ECS service does not have restrictions on the types of data to be backed up as long as the data complies with local laws and regulations. You can store RDS backup data on an ECS, but using an ECS is not recommended.

You are advised to use RDS **automated backup** and **manual backup** to back up data to OBS for higher data reliability and service assurance.

10.7 Will Backups Be Retained After My RDS Instance Is Deleted?

If your RDS instance is deleted, its manual backups are retained by default and will be billed based on the OBS pricing details. If you do not need the backups anymore, **delete them manually**. If your instance is frozen, its backups are not billed.

Automated backups, binlog backups, and their related files are automatically deleted.

10.8 How Can I Retrieve Databases and Tables Deleted by Mistake?

You can use backups to restore the data that was deleted by mistake. For details, see **Restoration Solutions**.

10.9 How Are Unsynchronized Backups Generated for RDS for 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 be the new primary instance. During the failover, 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 most recent backup, contact customer service.

10.10 Why Has My Automated Backup Failed?

The following figure shows the possible reasons for automated backup failures.

Figure 10-2 Reasons why automated backup fails
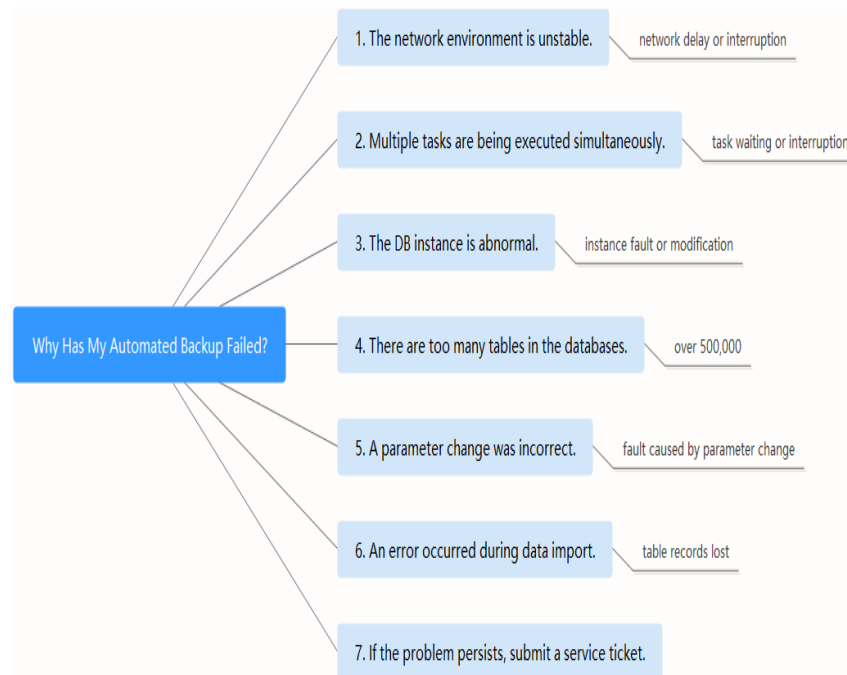
- The network environment may be unstable due to problems such as network delay or interruptions.

  If RDS detects any of these problems, it triggers another automated backup half an hour later. Alternatively, you can perform a manual backup immediately.

- If multiple tasks are being executed simultaneously, there can be problems such as excessive task wait times or interruptions.

  If RDS detects any of these problems, it triggers another automated backup half an hour later. Alternatively, you can perform a manual backup immediately.

- The DB instance is abnormal probably because it is faulty or being modified.

  If RDS detects any of these problems, it triggers another automated backup half an hour later. Alternatively, you can perform a manual backup immediately.

- The backup speed depends on how many tables there are in the databases.

  If the number of tables exceeds 500,000, the backup will fail.

- A parameter change was incorrect.

  If your DB instance becomes faulty after you modify parameters of a parameter template and apply the template to the instance, check whether the modified parameters are set to correct values and whether there are any associated parameters that need to be changed, or reset the parameters to their defaults and reboot the DB instance.

- An error occurred during data import.

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

  - For RDS for MySQL, you can import data again by referring to **Migration Solution Overview**.

- For RDS for PostgreSQL, you can import data again by referring to **Migration Solution Overview**.

- For RDS for SQL Server, you can import data again by referring to **Migration Solution Overview**.

- If the problem persists, contact customer service.

10.11 Why Is a Table or Data Missing from My Database?

RDS does not delete or perform any operations on any user data. If this problem occurs, check if there have been any misoperations and restore the data from backup files, if necessary.

Check for misoperations: If **the SQL audit function has been enabled**, you can view data execution records in audit logs.

Restore data using backup files:

- Use the RDS restoration function.

- Import the backup data to RDS through an ECS.

10.12 How Do I Restore a Local Database Backup to RDS?

You can use the DRS migration function to restore a local database backup to RDS.

For more information, see **Restoration Solutions**.

10.13 Does RDS for PostgreSQL Support Table PITR?

No.

You can use a manual or an automated backup to restore data to the status when the backup was created. This operation restores the data of the entire DB instance. For details, see **Restoration Solutions**.

10.14 Can I Dump Backup Files to My OBS Bucket?

No. Backup files cannot be directly dumped to your OBS bucket.

- RDS for MySQL: You can download full backups or merged binlogs to your local PC and dump them to your OBS bucket using OBS Browser+.

- RDS for PostgreSQL: You can download full backups or incremental backups to your local PC and dump them to your OBS bucket using OBS Browser+.

- RDS for SQL Server: You can download full backups to your local PC and dump them to your OBS bucket using OBS Browser+.

10.15 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.

10.16 Can I Delete the RDS for MySQL Backup Policy?

Sorry, you cannot delete the RDS for MySQL backup policy.

Once the backup policy is enabled, it cannot be disabled. You can change the backup retention days and backup cycle on the RDS console. The backup cycle can be changed to one day. For details, see **Configuring an Automated Backup Policy**.

11 Read Replicas and Read/Write Splitting

11.1 Does RDS Support Read/Write Splitting?

Table 11-1 lists the DB engines and versions which support read/write splitting.

Table 11-1 RDS read/write splitting

Database	Read/Write Splitting	Database Proxy	Remarks
RDS for MySQL	Supported	Supported	**Prerequisites:** You have obtained the permissions required for read/write splitting. To apply for the permissions, choose **Service Tickets > Create Service Ticket** in the upper right corner of the management console. **Procedure:** See **Enabling Read/Write Splitting**. **Function:** ● If read/write splitting is enabled and there is no read replica, read and write requests are automatically routed through the read/write splitting address to the primary instance. ● If read/write splitting is enabled and there are read replicas, RDS automatically routes write requests through the read/write splitting address to the primary instance and read requests to each read replica by user-defined weights. **Constraints:** See **Suggestions on Using Database Proxy**.
RDS for PostgreSQL	Supported with client drivers	Not supported	After read replicas are created, 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 RDS for PostgreSQL read replicas, see **Introducing Read Replicas**. For details about how to implement read/write splitting, see **Using Client Drivers to Implement Failover and Read/Write Splitting**.

Database	Read/Write Splitting	Database Proxy	Remarks
RDS for SQL Server	Supported only for 2017 Enterprise Edition	Not supported	After read replicas are created, 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.

11.2 Does RDS for MySQL Support Sharding and Read/Write Splitting?

Yes. RDS for MySQL supports sharding and read/write splitting.

- RDS works with Distributed Database Middleware (DDM) to provide sharding, allowing you to easily scale up your database.
- Up to five read replicas can be created for a primary DB instance. Read replicas and DB instances are connected through separate IP addresses.

  If you want to access your instance and read replicas using a unified read/write splitting address, **enable read/write splitting** first.

11.3 Can I Request Multiple Read/Write Splitting Addresses for My RDS for MySQL Instance?

Yes.

When single-proxy is enabled, a read/write splitting address is automatically assigned. Write requests are automatically routed through the read/write splitting address to the primary instance and read requests to each read replica by user-defined weights.

When multi-proxy is enabled, you can create multiple database proxies. Different applications are connected to different proxies, and proxies are associated with specific read replicas. In this way, read requests from the applications are forwarded to different read replicas, keeping application workloads isolated from each other.

12 Database Monitoring

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

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

You can configure the system to report alarms based on service requirements and take measures to handle any reported alarms.

Configuration examples:

● Configure RDS to report alarms to Cloud Eye if its CPU utilization reaches or exceeds a specific value (for example, 90%) multiple times (for example, 3 times) within a set period (for example, 5 minutes).

● Configure RDS to report alarms to Cloud Eye if its memory utilization reaches or exceeds a specific value (for example, 90%) multiple times (for example, 4 times) within a set period (for example, 5 minutes).

● Configure RDS to report alarms to Cloud Eye if its storage utilization reaches or exceeds a specific value (for example, 85%) multiple times (for example, 5 times) within a set period (for example, 5 minutes).

> **NOTE**
>
> For details on Cloud Eye alarm configuration, see "Creating an Alarm Rule" in the *Cloud Eye User Guide*.

Measures:

● If a CPU or memory alarm is reported, you can scale up the vCPUs or memory by changing the DB instance class.

For details, see **Changing a DB Instance Class**.

● If a storage space usage alarm is reported, you can:

– Check the storage space consumption to see if any space can be freed up by deleting data from DB instances or by dumping the data to another system.

For details, see **What Should I Do If an RDS DB Instance Is Abnormal Due to Full Storage Space?**

– Scale up the storage space.

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

12.2 How Can I Calculate the Memory Usage of an RDS DB Instance?

Click the target RDS DB instance. On the **Advanced O&M** page, you can view its memory usage.

Figure 12-1 Instance monitoring
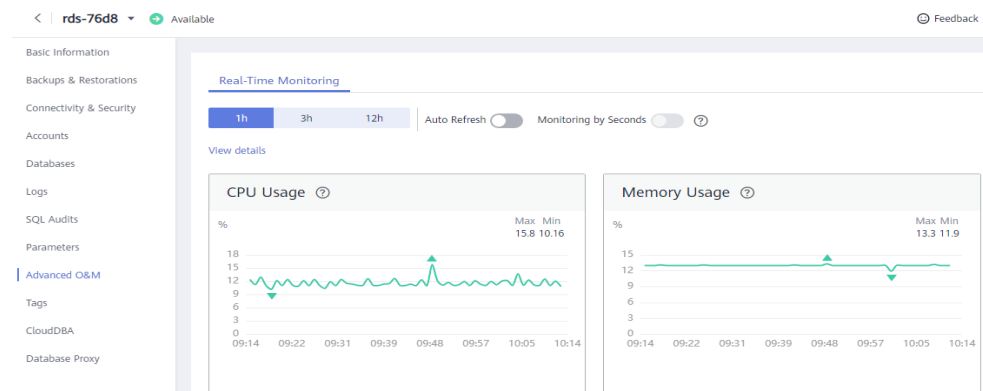
The formula for calculating the memory usage is as follows:

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

12.3 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 RDS for MySQL DB Instances**

● **Setting Alarm Rules for RDS for PostgreSQL DB Instances**

● **Setting Alarm Rules for RDS for SQL Server DB Instances**

13 Capacity Expansion and Specification Change

13.1 Are My RDS DB Instances Still Available During Storage Scale-up and Instance Class Change?

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

- When storage space is being scaled up, RDS DB instances are still available and services are not affected. However, you cannot delete or reboot DB instances that are being scaled.

- During the change of the vCPU or memory, the network is intermittently disconnected for one or two times in seconds. A failover may occur during this period and services may be briefly interrupted. Changing the vCPU or memory takes 5 to 15 minutes.

  After you change the vCPU or memory, the DB instances will reboot and services will be interrupted. Therefore, you are advised to change instance classes during off-peak hours.

13.2 Why Does the DB Instance Become Faulty After the Original Database Port Is Changed?

Symptom

- The DB instance is in **Faulty** state after the original database port is changed.
- The DB instance cannot be connected using the new database port.

Possible Causes

The submitted database port is occupied.

Procedure

Change the database port to the new port again. For details, see **Changing a Database Port**.

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

13.3 Can I Change the VPC that My RDS DB Instance Belongs To?

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

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

14 Database Parameter Modification

14.1 What Inappropriate Parameter Settings Cause Unavailability of the RDS for PostgreSQL Database?

In the following cases, inappropriate parameter settings cause the database to be unavailable:

- Parameter value ranges are related to DB instance specifications.

  The maximum values of **shared_buffers** and **max_connections** are related to the DB instance physical memory. If you set these parameters inappropriately, the database will be unavailable.

- Parameter association is incorrect.

  max_connections, **autovacuum_max_workers**, and **max_worker_processes** must meet the following requirements. Otherwise, the database is unavailable.

  max_connections value + **autovacuum_max_workers** value + **max_worker_processes** value + 1 < 8388607

> 📖 **NOTE**
>
> For additional details, visit the **PostgreSQL official website**.

Solution:

1. Log in to the RDS console and query the logs to locate the incorrectly configured parameters.
2. On the **Configuration** page, change parameters to default values and reboot the database.
3. Configure the incorrect parameter values and restore other parameters to their original default values.

14.2 How Can I Change the Time Zone?

You can set the time zone only on the RDS console. Different DB engines have different time zone policies.

● RDS for MySQL and RDS for PostgreSQL allow you to select a time zone when you create a DB instance and change the time zone after the instance is created.

● RDS for 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.

NOTICE

● If the time zone of your RDS for MySQL instance is different from that of the region where your workloads are deployed, or if the DST and standard time are switching in your country, you need to adjust the time zone of the instance.

● After the time zone parameter is modified, you need to reconnect to the instance for the modification to take effect.

To change the time zone for an RDS for MySQL or RDS for PostgreSQL DB instance, perform the following steps:

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

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

Step 3 Click in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Step 5 In the navigation pane on the left, choose **Parameters**.

Step 6 Search for a time zone parameter in the search box, for example, **time_zone**.

● The time zone parameter for RDS for MySQL is **time_zone**.

● The time zone parameter for RDS for PostgreSQL is **timezone**.

Step 7 Select a time zone, and click **Save**.

Step 8 In the displayed dialog box, click **OK**.

For example, to change the time zone to UTC+08:00, select **Asia/Shanghai** from the drop-down list.

----End

Time Zone Parameters

● **system_time_zone**: operating system (OS) time zone. This parameter cannot be changed and it has no impact on the database time zone.

● **time_zone**: database time zone. You can modify this parameter to change the time zone for your DB instance.

14.3 How Do I Configure a Password Expiration Policy for RDS for MySQL DB Instances?

In MySQL 5.6, you can run **ALTER USER *username* PASSWORD EXPIRE** to set the password expiration policy.

In MySQL 5.7 and 8.0, you can set the global variable **default_password_lifetime** to control the default validity period of a user password.

The value of **default_password_lifetime** indicates how many days until a password expires. The default value is **0**, indicating that the created user password will never expire.

```
mysql> show variables like 'default_password_lifetime';
+---------------------------+-------+
| Variable_name             | Value |
+---------------------------+-------+
| default_password_lifetime | 0     |
+---------------------------+-------+
1 row in set (0.00 sec)
```

Changing the Global Automatic Password Expiration Policy

Change the value of the **default_password_lifetime** parameter on the RDS console. For operation details, see **Modifying Parameters**.

Checking the Password Expiration Date of All Users

Run the following command:

mysql> select user,host,password_expired,password_last_changed,password_lifetime from user;

```
mysql> select user,host,password_expired,password_last_changed,password_lifetime from user;
+---------------+-----------+------------------+-----------------------+-------------------+
| user          | host      | password_expired | password_last_changed | password_lifetime |
+---------------+-----------+------------------+-----------------------+-------------------+
| mysql.session | localhost | N                | 2020-01-17 15:02:23   |              NULL |
| mysql.sys     | localhost | N                | 2020-01-17 15:02:23   |              NULL |
| rdsAdmin      | localhost | N                | 2020-01-17 15:02:30   |                 0 |
| root          | %         | N                | 2020-03-05 14:23:54   |              NULL |
| rdsRepl       | 192.168.% | N                | 2020-01-17 15:02:45   |                 0 |
| rdsMetric     | 192.168.% | N                | 2020-01-17 15:02:30   |                 0 |
| rdsBackup     | localhost | N                | 2020-01-17 15:02:30   |                 0 |
| u_test01      | %         | N                | 2020-03-05 14:28:10   |                30 |
| u_test02      | %         | N                | 2020-03-05 14:28:38   |              NULL |
| jeffrey       | localhost | N                | 2020-03-05 15:23:17   |              NULL |
+---------------+-----------+------------------+-----------------------+-------------------+
10 rows in set (0.00 sec)
```

Checking the Password Expiration Policy of a Specified User

Run the following command:

mysql> show create user *jeffrey*@'localhost';

```
mysql> show create user jeffrey@'localhost';
+--------------------------------------------------------------------------------------------------------------------------------------------------------+
| CREATE USER for jeffrey@localhost                                                                                                                       |
+--------------------------------------------------------------------------------------------------------------------------------------------------------+
| CREATE USER 'jeffrey'@'localhost' IDENTIFIED WITH 'mysql_native_password' AS '*1369F151650FC982555B53119A9CB8D554DB0D7F' REQUIRE NONE PASSWORD EXPIRE DEFAULT ACCOUNT UNLOCK |
+--------------------------------------------------------------------------------------------------------------------------------------------------------+
1 row in set (0.00 sec)
```

EXPIRE DEFAULT indicates that the password follows the global expiration policy.

Configuring the Password Expiration Policy for a Specified User

- Configuring the password expiration policy during user creation

  create user '*script*'@'localhost' identified by '*******' password expire interval 90 day;**

- Configuring the password expiration policy after user creation

  ALTER USER '*script*'@'localhost' PASSWORD EXPIRE INTERVAL 90 DAY;

- Setting the password to be permanently valid

  CREATE USER '*mike*'@'%' PASSWORD EXPIRE NEVER;

  ALTER USER '*mike*'@'%' PASSWORD EXPIRE NEVER;

- Setting the password to follow the global expiration policy

  CREATE USER '*mike*'@'%' PASSWORD EXPIRE DEFAULT;

  ALTER USER '*mike*'@'%' PASSWORD EXPIRE DEFAULT;

14.4 How Do I Change the RDS Transaction Isolation Level?

You can change the transaction isolation level by setting the **tx_isolation** parameter on the RDS console.

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

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Step 5 In the navigation pane on the left, choose **Parameters**. On the **Parameters** tab page, locate **tx_isolation** and select the desired isolation level from the drop-down list in the **Value** column. The following values are available for you to choose from:

- **READ-UNCOMMITTED**
- **READ-COMMITTED**
- **REPEATABLE-READ**
- **SERIALIZABLE**

Step 6 Click **Save**. In the displayed dialog box, click **Yes**.

----End

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

UTF-8 supports 4 byte characters, but RDS for MySQL utf8 supports only 3 byte characters. Emojis, uncommon Chinese characters, and newly added Unicode

characters cannot be stored using the MySQL utf8 character set. MySQL released the utf8mb4 character set in 2010 and added the utf8mb4 code after 5.5.3 to be compatible with the 4-byte unicode. You only need to change utf8 to utf8mb4. No other conversion is required.

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 [icon] in the upper left corner and select a region and a project.

Step 3 Click [icon] in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Alternatively, click the target DB instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.
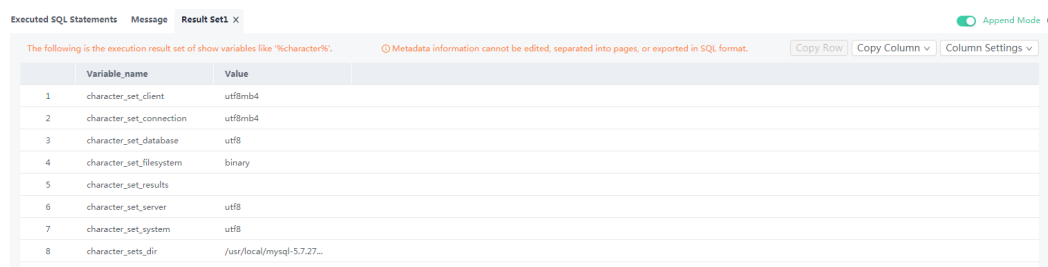
Step 5 On the displayed login page, enter the correct username and password and click **Log In**.

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 14-1 SQL execution result

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

show variables like 'collation%';

Figure 14-2 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.
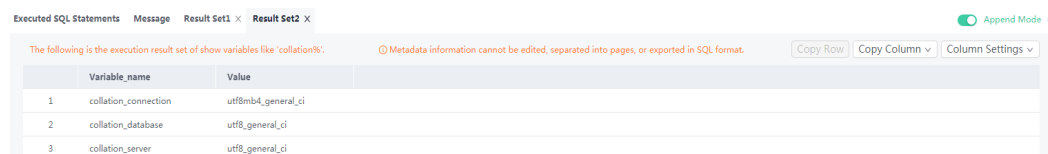   - **character_set_system**, **character_set_server**, and **character_set_database** are the settings of the server.
   - The priorities of the parameters on the server are as follows: **character_set_database** > **character_set_server** > **character_set_system**.

   ----End

14.6 Does RDS for PostgreSQL Support the test_decoding Plugin?

PostgreSQL 10, PostgreSQL 11, and PostgreSQL 13 support test_decoding. For more information about test_decoding, see **test_decoding introduction**.

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

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

Step 2 Click ⑨ in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Step 5 In the navigation pane on the left, choose **Parameters**. On the **Parameters** tab page, locate **wal_level** and change its value to **logical**.

Step 6 Click **Save**. In the displayed dialog box, click **Yes**.

----End

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

To store emojis in an RDS for MySQL DB instance, ensure that:

● The client outputs the utf8mb4 character set.

● The connection supports the utf8mb4 character set. If you want to use a JDBC connection, download MySQL Connector/J 5.1.13 or a later version and leave **characterEncoding** undefined for the JDBC connection string.

● Configure the RDS DB instance as follows:

– Setting **character_set_server** to **utf8mb4**

Parameter Name ↓≡	Effective upon Reboot ↓≡	Value	Allowed Values	Description
character_set_server	Yes	utf8mb4 ▼	utf8, latin1, gbk, utf8mb4	The server's default character set.

i. **Log in to the management console**.

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

iii. Click in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

iv. On the **Instances** page, click the instance name.

v. In the navigation pane on the left, choose **Parameters**. On the **Parameters** tab page, locate **character_set_server** and change its value to **utf8mb4**.

vi. Click **Save**. In the displayed dialog box, click **Yes**.

– Selecting **utf8mb4** for database character set

i. **Log in to the management console**.

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

iii. Click in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

iv. On the **Instances** page, click the instance name.

v. On the **Databases** page, click **Create Database**. In the displayed dialog box, enter a database name and remarks, select the character set **utf8mb4**, and authorize permissions for users. Then, click **OK**.

Figure 14-3 Creating a database

– Setting the character set of the table to **utf8mb4**

FAQs

If you have set **characterEncoding** to **utf8** for the JDBC connection string, or the emoji data cannot be inserted properly after you have performed the above operations, you are advised to set the connection character set to **utf8mb4** as follows:

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

14.8 Where Should I Store NDF Files for RDS for SQL Server?

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

14.9 Can I Use SQL Commands to Modify Global Parameters?

Sorry, you cannot use SQL commands to modify global parameters, but you can modify specific parameters on the RDS console.

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

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Step 5 In the navigation pane on the left, choose **Parameters**.

Step 6 Change the value of the target parameter and click **Save**.

Step 7 In the displayed dialog box, click **OK**.

----End

14.10 How Do I Modify the Collation of RDS for SQL Server?

- A database-level collation can be specified during database creation. If it is not specified, an instance-level collation is automatically used. You can change the database-level collation as user **rdsuser** at any time. You are advised to change the collation on the DAS console.

    a. **Log in to the management console**.

    b. Click ⊙ in the upper left corner and select a region and a project.

    c. Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

       Alternatively, click the DB instance name on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner.

    e. Enter the username and password and click **Log In**.

    f. Select the target database and choose **SQL Operations** > **SQL Query**. In the displayed SQL window, run required commands.

       (In this example, the collation of the **test** database is set to simplified Chinese.)

       ```
       use test
       go
       ALTER DATABASE test COLLATE Chinese_PRC_CS_AS
       ```

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

You can use either of the following methods to set the case sensitivity:

- **Modify parameter lower_case_table_names for created DB instances**: RDS for MySQL 5.6 and 5.7

- **Specify the case sensitivity during instance creation**: For RDS for MySQL 8.0, 5.7, and 5.6, you can specify whether table names are case sensitive when creating DB instances on the console or through an API.

Modifying the Parameter for Created DB Instances

NOTICE

- Before changing the case sensitivity, ensure that each table name is unique in your instance.

- You can change the case sensitivity of table names only when there is no replication delay. To check the replication delay, view the **Real-Time Replication Delay** metric on the Cloud Eye console.

- Scenario 1: The DB instance does not have read replicas.

  a. **Log in to the management console**.

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

  c. Click 　 in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

  d. On the **Instances** page, click the instance name.

  e. In the navigation pane, choose **Parameters**. On the displayed page, change the value of **lower_case_table_names**.

  For example, change the value from **1** to **0**, indicating that table names are case sensitive.

  f. Click **Save**. In the displayed dialog box, click **Yes**.

  g. Return to the DB instance list, locate the DB instance, and choose **More** > **Reboot** in the **Operation** column.

  h. In the displayed dialog box, click **OK** to reboot the DB instance for the modification to take effect.

- Scenario 2: The DB instance has read replicas.

  a. **Log in to the management console**.

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

  c. Click 　 in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

d. On the **Instances** page, click ⊞ and then click the target read replica name.

e. In the navigation pane, choose **Parameters**. On the displayed page, change the value of **lower_case_table_names**.

For example, change the value from **1** to **0**, indicating that table names are case sensitive.

f. Click **Save**. In the displayed dialog box, click **Yes**.

g. Return to the DB instance list, locate the primary DB instance, and choose **More** > **Reboot** in the **Operation** column.

h. In the displayed dialog box, click **OK** to reboot the DB instance for the modification to take effect.

i. On the **Instances** page, click the primary instance name.

j. In the navigation pane, choose **Parameters**. On the displayed page, change the value of **lower_case_table_names**.

For example, change the value from **1** to **0**, indicating that table names are case sensitive.

k. Click **Save**. In the displayed dialog box, click **Yes**.

l. Return to the DB instance list, locate the primary instance, and choose **More** > **Reboot** in the **Operation** column.

m. In the displayed dialog box, click **OK** to reboot the DB instance for the modification to take effect.

Specifying Case Sensitivity During Instance Creation

- Set **Table Name** to **Case sensitive** or **Case insensitive** on the RDS console during instance creation. For details, see **Buy a DB Instance**.

- Set parameter **lower_case_table_names** to **0** or **1** when calling an API to create a DB instance. For details, see **Creating a DB Instance**.

  Value range:

  - **0**: Table names are case sensitive.

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

14.12 Can I Enable Query Caching for My RDS for MySQL Instance?

Parameters related to query caching cannot be set on the console. To enable query caching, **submit a service ticket**.

You are not advised to enable query caching because:

- Query caching helps improve query speed only when you frequently access the same SQL statement, but consumes additional resources and reduces the SQL execution speed in other scenarios.

- Function test results show that the query speed of an instance without enabling query caching is faster than that when this function is enabled.

- Query caching is no longer maintained in the MySQL community.

15 Log Management

15.1 How Long Is the Delay for 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 in advance. Slow query log statistics cannot be exported for RDS.

15.2 How Do I View All SQL Logs Executed by RDS for MySQL?

You can use the SQL audit function of RDS to query all SQL operation records. You can also use the visualized database management service Data Admin Service (DAS) to quickly search for target SQL execution 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 ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

Step 4 On the **Instances** 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.

Figure 15-1 SQL History

- To access the **Database Management** page, 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

15.3 How Can I Obtain RDS for 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 15-2 shows the query results.

Figure 15-2 Example query results

----End

15.4 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.
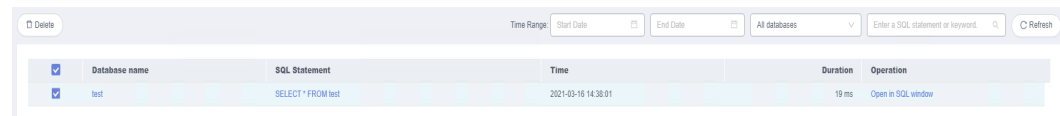
Procedure

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 ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Figure 15-3 Logging in to a database

Name/ID		Description	DB Instanc...	DB Engine Version	Status	Billing Mode	Floating IP Address	Storage Type	Operation
		--	Primary/Standby 1 vCPU	2 GB	MySQL 5.7.31	Available	Pay-per-use Created on Jan 13,...	192.168.2...	Ultra-high I/O	Log In View Metric More
		--	Primary/Standby 1 vCPU	2 GB	MySQL 5.7.31	Available	Pay-per-use Created on Jan 13,...	192.168.2...	Ultra-high I/O	Log In View Metric More

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 Query**. In the displayed SQL window, run **show engine innodb status** to view the latest deadlock logs of the selected database. Use the keyword **LATEST DETECTED DEADLOCK** to locate the latest deadlock logs. The latest deadlock logs will overwrite the historical deadlock logs.

----End

16 Network Security

16.1 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.

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

When you access RDS through an EIP, workload data will be transmitted on the Internet. To prevent any potential data breaches, you are advised to use SSL to encrypt data transmitted on the Internet. For details, see **Configuring an SSL Connection**. You can also use Direct Connect or VPN to encrypt data transmission.

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

- If you enable public accessibility, your EIP DNS and database port may be vulnerable to hacking. To protect information such as your EIP, DNS, database port, database account, and password, you are advised to set the range of source IP addresses in the RDS security group to ensure that only trusted source IP addresses can access your DB instances.

- To prevent your database password from being cracked, set a strong password and periodically change it.
- RDS for SQL Server includes defense against brute force cracking. If malicious individuals have obtained your EIP DNS, database port, or database login information and attempt a brute force attack, 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 RDS for PostgreSQL do not include defense against brute force attacks.

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

16.4 How Do I Configure a Security Group to Enable Access to RDS DB Instances?

- When you attempt to connect to a DB instance through a private network, check whether the ECS and RDS DB instance are in the same security group.
  - If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No security group rules need to be configured.
  - If the ECS and RDS DB instance are in different security groups, you need to configure security group rules for them, separately.

    - RDS DB instance: Configure an **inbound rule** for the security group with which the DB instance is associated.

    - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.
- When you attempt to connect to a DB instance through an EIP, you need to configure an **inbound rule** for the security group associated with the DB instance.

16.5 How Can I Import the Root Certificate to a Windows or Linux OS?

Importing the Root Certificate to the Windows OS

1. Click **Start** and choose **Run**. In the displayed **Run** dialog box, enter **MMC** and press **Enter**.
2. On the displayed console, choose **File** > **Add/Remove Snap-in**.
3. In the left **Available snap-ins** pane of the displayed **Add or Remove Snap-ins** dialog box, select **Certificates** and click **Add**.
4. In the displayed **Certificates snap-in** dialog box, select **Computer account** and click **Next**.

5.   In the displayed **Select Computer** dialog box, click **Finish**.

6.   In the **Add or Remove Snap-ins** dialog box, click **OK**.

7.   On the console, double-click **Certificates**.

8.   Right-click **Trusted Root Certification Authorities** and choose **All Tasks** > **Import**.

9.   In the displayed **Certificate Import Wizard** dialog box, click **Next**.

10. Click **Browse** to change the file type to **All Files (*.*)**.

11. Locate the downloaded root certificate ca.pem file and click **Open**. Then, click **Next**.

> **NOTICE**
>
> You must change the file type to **All Files (*.*)** because **.pem** is not a standard certificate extension name.

12. Click **Next**.

13. Click **Finish**.

14. Click **OK** to complete the import of the root certificate.

Importing the Root Certificate to the Linux OS

You can use a connection tool (such as WinSCP or PuTTY) to upload the certificate to any directory on a Linux OS.

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

When you connect to an RDS for MySQL DB instance using an SSL connection, run the following command to check whether the certificate has expired:

```
show status like '%ssl_server%';
```

Update the root certificate to the latest version before it expires:

1.   In the **DB Information** area on the **Basic Information** page, click ⤓ in the **SSL** field to download the root certificate or certificate bundle.

2.   Reboot the DB instance for the new certificate to take effect.

3.   Connect to the DB instance using the new certificate or certificate bundle.

     –   **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.

16.7 What Are the Possible Causes for Data Corruption?

- Data tampering

  Lots of security measures are provided to ensure that only authenticated users have permissions to perform operations on database table records. Database tables can be accessed only through specific database ports.

  Verifying package during primary/standby synchronization can prevent data tampering. RDS for MySQL uses the InnoDB storage engine to prevent data from being damaged.

- DB instance servers may be powered off suddenly, causing database page corruption and database rebooting failures.

  If a primary DB instance becomes faulty, RDS switches to the standby DB instance within 1 to 5 minutes to provide services for you. Databases cannot be accessed during a failover. You must configure automatic reconnection between your applications and RDS to make sure that your applications are available after the failover.

17 Version Upgrade

17.1 How Can I View the Version of an RDS DB Instance?

- On the **Instances** page of the RDS console, view the version of the DB instance.

  Figure 17-1 Instances

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

  a. Log in to the target DB instance.

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

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

17.2 Does RDS for MySQL Support Version Upgrades?

- Major version upgrades

  Major versions cannot be upgraded on the RDS console. You can use Data Replication Service (DRS) to migrate databases from RDS for MySQL 5.6 to RDS for MySQL 5.7 smoothly. **Before using DRS to upgrade a major version, you need to prepare a DB instance of the target version.**

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

  For more information, see **Creating a Migration Task** in the *Data Replication Service User Guide*.

Table 17-1 MySQL database version information

Source Database Version	Destination Database Version	Migration Type
RDS for MySQL/Self-built MySQL/MySQL in other clouds 5.5.x 5.6.x 5.7.x 8.0.x	RDS for MySQL 5.6.x 5.7.x 8.0.x	Version upgrade

☐ **NOTE**

- DRS only supports migration from an earlier version to a later version.
- During the specification change, two primary/standby switchovers and two intermittent disconnections will occur. After that, check the DRS task.

- 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 upgrade operations, see **Upgrading a Minor Version**.

17.3 Does RDS for MySQL Support Version Downgrades?

RDS for MySQL does not support version downgrades on the management console.

You can **use mysqldump to migrate data**, or delete the DB instance and create a new one.

17.4 Does RDS for PostgreSQL Support Major Version Upgrades?

RDS for PostgreSQL supports major version upgrades.

To upgrade a major version, you can use Data Replication Service (DRS) to migrate on-premises databases to RDS for PostgreSQL running the target major version smoothly. Therefore, you need to prepare a DB instance running the target version before the migration.

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

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

18 Developer-Related APIs and SDKs

Table 18-1 RDS APIs and SDKs

Category	Reference Document
RDS API	**RDS API Reference**
RDS Java SDK	**SDK Developer Guide**
RDS Python SDK	
RDS Go SDK	

A Change History

Released On	Description
2022-12-26	This issue is the thirty-seventh official release, which incorporates the following change: Added **Can I Enable Query Caching for My RDS for MySQL Instance?**.
2022-07-30	This issue is the thirty-sixth official release, which incorporates the following change: Added **Resource Freezing, Release, Stopping, Deletion, and Unsubscription**.
2022-04-30	This issue is the thirty-fifth official release, which incorporates the following change: Optimized **Can I Request Multiple Read/Write Splitting Addresses for My RDS for MySQL Instance?**.
2021-11-29	This issue is the thirty-fourth official release, which incorporates the following change: Optimized **Does RDS Support Read/Write Splitting?**.
2021-10-27	This issue is the thirty-third official release, which incorporates the following changes: Added **How Do I Distinguish Between General-Purpose and Dedicated RDS for MySQL Instances Using Cloud SSDs?**.
2021-10-22	This issue is the thirty-second official release, which incorporates the following changes: Optimized the content in **How Can I Calculate the Memory Usage of an RDS DB Instance?**.
2021-08-12	This issue is the thirty-first official release, which incorporates the following changes: Added **How Do I Create a Scheduled Task?**.

Released On	Description
2021-07-21	This issue is the thirtieth official release, which incorporates the following changes: Added **How Do I Configure a Password Expiration Policy for RDS for MySQL DB Instances?**.
2021-06-21	This issue is the twenty-ninth official release, which incorporates the following changes: Optimized the content in **What Is the Maximum Number of Connections to an RDS DB Instance?**. Optimized the content in **Does RDS Support Read/Write Splitting?**.
2021-05-21	This issue is the twenty-eighth official release, which incorporates the following change: ● Added **Why Did I Fail to Create an Object on the postgres Database as a Common User?** ● Added **What Should I Do If a Role Failed to Be Deleted from an RDS for PostgreSQL Instance?** ● Added **Why Did My RDS for PostgreSQL Migration Fail?** ● Added **How Do I Grant the REPLICATION Permission to an RDS for PostgreSQL Database User?** ● Added **Why Is An Error Reported When I Attempt to Change a Table Owner of the RDS for PostgreSQL Database?** ● Added **How Do I Use the mysqlbinlog Tool?** ● Added **How Do I View Session IDs and Login and Logout Time of a Database?** ● Added **How Do I Clear RDS Backup Space?** ● Added the description in **How Do I View My Backup Storage Usage?** ● Added the solution in **What Do I Do If the Number of RDS Database Connections Reaches the Upper Limit?** ● Optimized the solution in **What Should I Do If My Data Exceeds the Available Storage of an RDS for MySQL Instance?**
2021-04-23	This issue is the twenty-seventh official release, which incorporates the following change: ● Changed the section title from "Why Can't I Ping My EIP After It Is Bound to a DB Instance?" to "Why Cannot I Ping My EIP After It Is Bound to a DB Instance?".

Released On	Description
2021-04-19	This issue is the twenty-sixth official release, which incorporates the following changes: • Added **Does MySQL 8.0 Support Full-Text Search?** • Added **How Do I Use DAS to Query SQL Statements?** • Added **How Do I View Authorized Databases After a Local Client Is Connected to a DB Instance?** • Added **How Do I Clear RDS Backup Space?** • Added the keyword **LATEST DETECTED DEADLOCK** in the procedure in **How Do I View Deadlock Logs of RDS for MySQL?**
2021-01-18	This issue is the twenty-fifth official release, which incorporates the following changes: • Added **How Do I Set Case Sensitivity for RDS for MySQL Table Names?** • Added **How Do I View Deadlock Logs of RDS for MySQL?** • Added **Can I Delete the RDS for MySQL Backup Policy?**
2020-09-15	This issue is the twenty-fourth official release, which incorporates the following change: Added **How Can I Calculate the Memory Usage of an RDS DB Instance?**
2020-07-17	This issue is the twenty-third 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 PITR?** Added section **Can I Dump Backup Files to My OBS Bucket?**
2020-04-10	This issue is the twenty-first official release, which incorporates the following changes: Added **Does RDS for MySQL Support Version Downgrades?** Added **Developer-Related APIs and SDKs**.
2020-03-06	This issue is the twentieth official release, which incorporates the following changes: Added **What Should I Do When a Large Number of Binlog Files Cause Storage Space Insufficiency During an RDS MySQL Instance Migration?**

Released On	Description
2020-01-31	This issue is the nineteenth official release, which incorporates the following changes: Added section **What Are the Differences Between RDS ManageAccess and DAS Permissions?** Optimized the content in **What Is the Maximum Number of Connections to an RDS DB Instance?**.
2019-10-31	This issue is the seventeenth official release, which incorporates the following changes: Added section **Can Multiple Users Log In to DAS at the Same Time? Will the Accounts Be Locked If I Enter Wrong Passwords Several Times in a Row?** Added section **How Are Unsynchronized Backups Generated for RDS for SQL Server DB Instances?** Added section **How Do I Ensure that the Character Set of an RDS MySQL Database Is Correct?**
2019-10-12	This issue is the sixteenth official release, which incorporates the following changes: Added section **How Do I View All SQL Logs Executed by RDS for MySQL?**
2019-09-12	This issue is the fifteenth 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?
2019-08-12	This issue is the fourteenth 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 RDS for SQL Server? Added an FAQ: How Long Is the Delay of RDS for MySQL Slow Query Logs?

Released On	Description
2019-07-12	This issue is the thirteenth 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 twelfth official release, which incorporates the following changes: Added **Can I Access an RDS DB Instance Over an Intranet Connection Across Regions?** Added **Does RDS for MySQL Support Stored Procedures and Functions?**
2019-03-30	This issue is the eleventh official release, which incorporates the following change: Optimized content in section **What Storage Engines Does RDS for MySQL Support?**
2019-03-15	This issue is the tenth official release, which incorporates the following change: Added section **Does RDS for MySQL Support Multiple Accounts?**
2019-02-15	This issue is the ninth official release, which incorporates the following change: Added section **Where Should I Store NDF Files for RDS for SQL Server?**
2019-01-08	This issue is the eighth official release, which incorporates the following change: Optimized the content in **Why Does the Root User Not Have the Super Permissions?**.
2018-10-15	This issue is the seventh official release, which incorporates the following changes: Added section **How Is RDS Backup Data Charged?** Added section **Why Does the Root User Not Have the Super Permissions?** Added section **Can I Change the Replication Mode Between Primary DB Instances and Read Replicas?** Added section **Why Cannot I Ping My EIP After It Is Bound to a DB Instance?** Added section **Does RDS Support Scaling Down Storage Space of DB Instances?**
2018-09-04	This issue is the sixth official release, which incorporates the following change: Optimized MySQL parameter groups.

Released On	Description
2018-07-13	This issue is the fifth official release, which incorporates the following change: Changed the default port number to **5432** when an RDS for 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 RDS for 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 RDS for SQL Server Error Logs Using Commands?** ● Added an FAQ: How do I obtain IP addresses of applications?
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?**
2018-05-04	This issue is the first official release.