

# Relational Database Service

## FAQs

**Issue**            01  
**Date**             2025-11-11



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.**

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

## **Trademarks and Permissions**



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

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

## **Notice**

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

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

# Contents

<b>1 Product Consulting</b>	<b>1</b>
1.1 What Should I Pay Attention to When Using RDS?	1
1.2 Will My RDS DB Instances Be Affected by Other User Instances?	1
1.3 What Can I Do About Slow Responses of Websites When They Use RDS?	1
1.4 Can Multiple ECSs Connect to the Same RDS DB Instance?	2
<b>2 Resource and Disk Management</b>	<b>3</b>
2.1 Which Types of Logs and Files Occupy RDS Storage Space?	3
2.2 Which Items Occupy the Storage Space of My RDS DB Instances?	4
2.3 How Much Storage Space Is Required for DDL Operations?	4
<b>3 Database Connection</b>	<b>5</b>
3.1 What Should I Do If I Can't Connect to My RDS DB Instance?	5
3.2 Can an External Server Access the RDS Database?	9
3.3 What Do I Do If the Number of RDS Database Connections Reaches the Upper Limit?	9
3.4 What Is the Maximum Number of Connections to an RDS DB Instance?	9
3.5 What Should I Do If an ECS Cannot Connect to an RDS DB Instance Through a Private Network?	12
3.6 What Should I Do If a Database Client Problem Causes a Connection Failure?	12
3.7 What Should I Do If an RDS Database Problem Causes a Connection Failure?	13
3.8 How Do My Applications Access an RDS DB Instance in a VPC?	13
3.9 Do Applications Need to Support Reconnecting to the RDS DB Instance Automatically?	13
3.10 Why Cannot I Ping My EIP After It Is Bound to a DB Instance?	14
3.11 How Can I Obtain the IP Address of an Application?	15
3.12 What Should I Do If an RDS for SQL Server DB Instance Failed to Be Connected?	16
3.13 Is an SSL Connection to a DB Instance Interrupted After a Primary/Standby Switchover or Failover?	16
3.14 Will My Access Be Restricted by Bandwidth When I Connect to My Instance from an ECS over a Private Network?	17
<b>4 Database Migration</b>	<b>18</b>
4.1 Why Do I Need to Use the mysqldump or pg_dump Tools for Migration?	18
4.2 What Types of DB Engines Does RDS Support for Importing Data?	18
<b>5 Database Permission</b>	<b>19</b>
5.1 Why Does the Root User Not Have the Super Permissions?	19
<b>6 Database Storage</b>	<b>20</b>

6.1 What Storage Engines Does RDS for MySQL Support?.....	20
6.2 What Types of Storage Does RDS Use?.....	21
6.3 What Should I Do If My Data Exceeds the Available Storage of an RDS for MySQL Instance?.....	21
<b>7 Client Installation.....</b>	<b>23</b>
7.1 How Can I Install the MySQL Client?.....	23
7.2 How Can I Install a PostgreSQL Client?.....	24
7.3 How Can I Install SQL Server Management Studio?.....	26
<b>8 Backup and Restoration.....</b>	<b>27</b>
8.1 How Long Does RDS Store Backup Data For?.....	27
8.2 Can My Instance Still Be Used in the Backup Window?.....	27
8.3 How Can I Back Up an RDS Database to an ECS?.....	27
8.4 Why Has My Automated Backup Failed?.....	28
8.5 Why Is a Table or Data Missing from My Database?.....	29
<b>9 Database Monitoring.....</b>	<b>30</b>
9.1 Which DB Instance Monitoring Metrics Do I Need to Pay Attention To?.....	30
<b>10 Capacity Expansion and Specification Change.....</b>	<b>31</b>
10.1 Are My RDS DB Instances Still Available During Storage Scale-up and Instance Class Change?.....	31
10.2 Why Does the DB Instance Become Faulty After the Original Database Port Is Changed?.....	31
<b>11 Database Parameter Modification.....</b>	<b>33</b>
11.1 What Inappropriate Parameter Settings Cause Unavailability of the RDS for PostgreSQL Database?.....	33
11.2 Where Should I Store NDF Files for RDS for SQL Server?.....	34
<b>12 Log Management.....</b>	<b>35</b>
12.1 How Can I Obtain RDS for SQL Server Error Logs Using Commands?.....	35
<b>13 Network Security.....</b>	<b>37</b>
13.1 How Can Data Security Be Ensured During Transmission When I Access RDS Through an EIP?.....	37
13.2 How Can I Prevent Untrusted Source IP Addresses from Accessing RDS?.....	37
13.3 How Do I Configure a Security Group to Enable Access to RDS DB Instances?.....	38
13.4 What Are the Possible Causes for Data Corruption?.....	38

# 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 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.

## 1.3 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.

## **1.4 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.

# 2 Resource and Disk Management

## 2.1 Which Types of Logs and Files Occupy RDS Storage Space?

The following logs and files occupy RDS storage space.

**Table 2-1** MySQL database file types

DB Engine	File Type
MySQL	Log files: database undo-log, redo-log, and binlog files
	Data files: database content files and index files
	Other files: ibdata, ib_logfile0, and temporary files

**Table 2-2** PostgreSQL database file types

DB Engine	File Type
PostgreSQL	Log files: database error log and transaction log files
	Data files: database content, index, replication slot data, transaction status data, and database configuration files
	Other files: temporary files

**Table 2-3** Microsoft SQL Server database file types

DB Engine	File Type
Microsoft SQL Server	Log files: database error log, transaction log, and trace files
	Data files: database content files

## Solution

1. If the original storage space is insufficient as your services grow, scale up storage space of your DB instance.
2. If data occupies too much storage space, run **DROP**, **TRUNCATE**, or **DELETE +OPTIMIZE TABLE** to delete useless historical table data to release storage space. If no historical data can be deleted, scale up your storage space.
3. If temporary files generated by sorting queries occupy too much storage space, optimize your SQL query statements.
  - a. A large number of temporary files are generated 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.

## 2.2 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 logs, default trace logs, and agent logs, generated by databases.

These files ensure the stability of RDS DB instances.

## 2.3 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 Database Connection

---

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

### Possible Causes

Try the following:

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

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

2. **(Common) Check whether the client connection is correct.**

- If you connect to a DB instance over a private network, ensure that the DB instance and ECS are in the same region and VPC.
- If you connect to a DB instance over a public network, bind an EIP to the DB instance and then connect to the DB instance through the EIP.

3. **Check the connection method.**

Run either of the following example commands to enable or disable SSL:

- SSL enabled: `mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem`
- SSL disabled: `mysql -h 172.16.0.31 -P 3306 -u root -p`

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

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

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

For a private network connection:

- a. Check whether the ECS and DB instance are in the same region and VPC.
- b. Check security group rules.
- c. On the ECS, check whether the DB instance port can be connected to.

For a public network connection:

- a. Check security group rules.
  - b. Check network ACL rules.
  - c. Ping the ECSs in the same region to the DB instance.
6. **(Common) Check whether the number of connections to the DB instance reaches the upper limit.**  
If there is an excessive number of database connections, applications may be unable to connect.
7. **(Common) Check whether the DB instance is in the Storage full state.**  
If the DB instance is in the **Storage full** state, data read and write performance is affected.

## Fault Locating

1. **Check whether the DB instance is available.**  
Check whether the DB instance is in the **Available** state.  
**Possible cause:** The RDS system is faulty, the DB instance is abnormal, or the DB instance or a table is locked.  
**Solution:** If the DB instance is abnormal, reboot it.
2. **Check whether the client connection is correct.**  
Install an **engine client** whose version is at least as new as the DB instance version.  
For details about how to connect to a DB instance over a private or public network, see [Can an External Server Access the RDS Database?](#)

**Table 3-1** Connection model

Connecti on method	Scenario	Example
Private network	A private IP address is provided by default. If your applications are deployed on an ECS that is in the same region and VPC as the DB instance, connect to the ECS and DB instance through a private IP address.	RDS for MySQL: <b>mysql -h &lt;private IP address&gt; -P 3306 -u root -p --ssl-ca=/tmp/ca.pem</b>
Public network	If you cannot access the DB instance using a private IP address, bind an EIP to the DB instance and then connect to the DB instance through the EIP.	RDS for MySQL: <b>mysql -h &lt;EIP&gt; -P 3306 -u root -p --ssl-ca=/tmp/ca.pem</b>

3. **Check the connection method.**
  - SSL connection is recommended. Enable SSL on the **Connectivity & Security** page and upload the certificate to the ECS.  
**mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem**

- Common connection: Disable SSL on the **Basic Information** page.  
**mysql -h 172.16.0.31 -P 3306 -u root -p**

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

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

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

- IP address  
On the **Private Connection** tab of the **Connectivity & Security** page, obtain the floating IP address in the **Connection Information** area.
- Database Port  
On the **Private Connection** tab of the **Connectivity & Security** page, obtain the database port in the **Connection Information** area.
- Root login credentials  
Make sure you have entered the root password correctly.
- Certificate  
Obtain the SSL certificate name from the directory where the command is executed.

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

- IP address  
On the **Public Connection** tab of the **Connectivity & Security** page, obtain the EIP in the **Connection Information** area.
- Database Port  
On the **Public Connection** tab of the **Connectivity & Security** page, obtain the database port in the **Connection Information** area.
- Root login credentials  
Make sure you have entered the root password correctly.
- Certificate  
Obtain the SSL certificate name from the directory where the command is executed.

5. **Check the network connection.**

**Private network connection**

- a. Check whether the ECS and DB instance are in the same region and VPC.
- b. Check security group rules.
  - 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.
- c. On the ECS, check whether the DB instance port can be connected to.  
**telnet <IP address> <port number>**

**Public network connection**

- a. Check security group rules.

- 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.
  - b. Ping the DB instance on an ECS in the same region.  
If you cannot ping the RDS instance's EIP from an ECS, try pinging it from another ECS in the same region.
- 6. **Check whether there are too many connections to the DB instance.**

**Check method:**

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

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

- **max\_connections**: the maximum number of clients that can be connected at the same time. If this parameter is set to **default**, the maximum number of clients depends on the amount of memory configured. For details, see [What Is the Maximum Number of Connections to an RDS DB Instance?](#)
    - **max\_user\_connections**: the maximum number of concurrent connections allowed for a specific RDS for MySQL account.
  - b. Check whether the total connections and current active connections have reached the upper limits by referring to [Viewing Monitoring Metrics](#). Determine whether to release the connections.

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

**Solution:**

- a. Check whether applications are connected, optimize the connections, and release unnecessary connections.
  - b. If this parameter is set to **default**, you can scale up the DB instance to set **max\_connections** to a larger value.
  - 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.
- 7. **Check whether the DB instance is in the Storage full state.**

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

- On the RDS console  
Locate a DB instance and click its name to go to the **Basic Information** page. In the **Storage Space** area, view the storage space usage.
- On Cloud Eye  
Locate a DB instance and click **View Metric** in the **Operation** column. On the displayed page, view the storage space usage.

## 3.2 Can an External Server Access the RDS Database?

### DB Instance Bound with an EIP

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

### DB Instance Not Bound with an EIP

- Enable a VPN in a VPC and use the VPN to connect to the RDS DB instance.
- Create an RDS and an ECS in the same VPC and access RDS through the ECS.

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

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

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

### Fault Locating

1. Check whether applications are connected, optimize the connections, and release unnecessary connections.
2. Check the specifications and scale them up if needed.

## 3.4 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.

### Definition

The maximum number of connections refers to the concurrent connections allowed for a DB instance.

## How to Change It

- RDS for MySQL  
You can run the following command to query the maximum number of connections allowed:

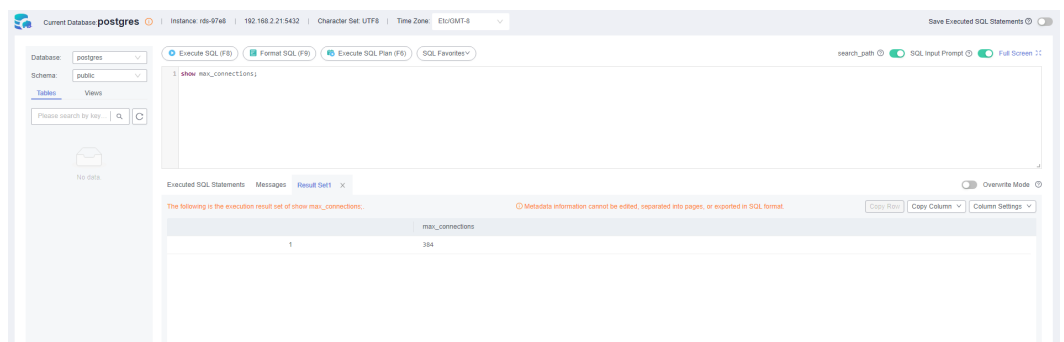
**show global variables like 'max\_connections';**

```
MySQL [(none)]> show global variables like 'max_connections';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| max_connections | 2500 |
+-----+-----+
1 row in set (0.00 sec)

MySQL [(none)]> █
```

- RDS for PostgreSQL  
You can run the following command to query the maximum number of connections allowed:

**show max\_connections;**



## Setting the Maximum Number of Connections to an Appropriate Value

- RDS for MySQL
  - In addition to the value of **max\_connections**, the maximum number of concurrent client connections allowed by RDS for MySQL is also limited by the maximum number of files that can be opened by a single process in the operating system. For example, if the maximum number of files that can be opened by each process is set to **100** in the operating system, the **max\_connections** parameter does not take effect even if it is set to **200**.
  - Check the maximum number of files that can be opened by a single process in the operating system. The default value is **1024**.

**ulimit -n**

```
[root@ecs-for-vpc-6192 ~]# ulimit -n
1024
```

- 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';**

```
MySQL [(none)]> show variables like 'open_files_limit';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| open_files_limit | 500000 |
+-----+-----+
1 row in set (0.00 sec)
```

- 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:

$$\text{Estimated value of max\_connections} = \frac{\text{Available node memory}}{\text{Estimated memory occupied by a single connection}}$$

 NOTE

- Available node memory = Total memory – Memory occupied by the buffer pool – 1 GB (mysqld process/OS/monitoring program)
- Estimated memory usage of a single connection (single\_thread\_memory) = thread\_stack (256 KB) + binlog\_cache\_size (32 KB) + join\_buffer\_size (256 KB) + sort\_buffer\_size (256 KB) + read\_buffer\_size (128 KB) + read\_rnd\_buffer\_size (256 KB) ≈ 1 MB

The following table lists the default values of **max\_connections** for different memory specifications.

**Table 3-2** Max\_connections for different memory specifications

Memory (GB)	Connections
512	100,000
256	60,000
128	30,000
64	18,000
32	10,000

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.

## 3.5 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.
- 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 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

## 3.6 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 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.

## 3.7 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.

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

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

## 3.9 Do Applications Need to Support Reconnecting to the RDS DB Instance Automatically?

It is recommended that your applications support automatic reconnections to the database. After a database reboot, your applications will automatically reconnect to the database to increase service availability and continuity.


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

## 3.10 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 of the page and choose **Databases > Relational Database Service**.
  - c. On the **Instances** page, click the target DB instance.
  - d. In the **Connection Information** area, click the security group.
  - e. Check whether the ECS NIC security group allows the inbound ICMP traffic.

**Table 3-3** 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.  
Use another ECS in the same region to ping the EIP. If the EIP can be pinged, the virtual network is normal. Contact customer service.

## 3.11 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 192.168.0.1 -P 3306 -u root -p
```

Enter password:

**Step 3** Query process information.

```
show processlist
```

**Figure 3-1** shows the query result. The outbound IP address is the host IP address in the "show processlist" row of the Info field.

**Figure 3-1** IP query result

```
mysql> show processlist
->
+-----+-----+-----+-----+-----+-----+-----+-----+
| Id      | User  | Host          | db   | Command | Time | State | Info          |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 286125391 | dctest | 192.168.0.1:14466 | NULL | Query   | 0    | init  | show processlist |
+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.01 sec)
```

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

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

----End


## 3.12 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 of the page and choose **Databases > Relational Database Service**.

**Step 3** On the **Instances** page, click the target DB instance. On the **Basic Information** and **Backups & Restorations** pages, check connection and backup information.

**Step 4** On the **Basic Information** page, check the administrator.

**Step 5** Download an SQL Server Management Studio installation package and install it on an ECS.

**Step 6** Connect to the RDS DB instance through an ECS.

----End

## 3.13 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.

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

No.

# 4 Database Migration

---

## 4.1 Why Do I Need to Use the mysqldump or pg\_dump Tools for Migration?

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

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

## 4.2 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.

# 5 Database Permission

---

## 5.1 Why Does the Root User Not Have the Super Permissions?

RDS does not provide super permissions for the **root** user. The super permissions allow you to execute management commands, such as **reset master**, **set global**, **kill *thread\_ID***, 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 Database Storage

## 6.1 What Storage Engines Does RDS for MySQL Support?

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

### InnoDB Storage Engine

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

### Other Storage Engines

[Table 6-1](#) lists the storage engines not supported by RDS for MySQL 5.6 or later versions.

**Table 6-1** Unsupported storage engines

Storage Engine	Reason
MyISAM	<ul style="list-style-type: none"><li>• MyISAM engine tables do not support transactions. They only support table-level locks. As a result, read and write operations conflict with each other.</li><li>• MyISAM is not good at protecting data integrity. Data can be damaged or lost.</li><li>• If data is damaged, MyISAM does not support data restoration provided by RDS for MySQL. Data can only be restored manually.</li><li>• Data can be transparently migrated from MyISAM to InnoDB without changing code.</li></ul>

Storage Engine	Reason
FEDERATED	<ul style="list-style-type: none"> <li>• If primary/standby DB instances support FEDERATED, the same DML operations will be repeatedly executed on remote databases, and the data will become disordered.</li> <li>• For PITR restoration, after a full backup is restored, data on remote databases is not restored to the state it was in when the full backup was created. Accessing data during an incremental restoration will disorder FEDERATED table data.</li> </ul>
MEMORY	<ul style="list-style-type: none"> <li>• If a memory table becomes empty after a restart, the database adds a DELETE event to the binlog when the table is opened. If a primary/standby DB instance uses memory tables and the standby instance (or a read replica) is restarted, a GTID is generated, which makes the standby inconsistent with that of the primary instance. As a result, the standby instance (read replica) has to be rebuilt.</li> <li>• Using memory tables may cause out-of-memory (OOM) errors and even service terminations.</li> </ul>

## 6.2 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*.

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

### Symptom

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

### Causes

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

## Solution

1. For insufficient storage caused by increased workload data, scale up storage space.  
If the original storage has reached the maximum, upgrade the specifications first.
2. If too much data is stored, delete unnecessary historical data.
  - a. If the instance becomes read-only, you need to contact technical support to cancel the read-only status first.
  - b. To clear up space, you can optimize tables with a high fragmentation rate during off-peak hours.  
To delete data of an entire table, run **DROP** or **TRUNCATE**. To delete part of table data, run **DELETE** and **OPTIMIZE TABLE**.
3. If binlog files occupy too much space, clear local binlogs.
4. If temporary files generated by sorting queries occupy too much storage space, optimize your SQL statements.

# 7 Client Installation

## 7.1 How Can I Install the MySQL Client?

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

### Procedure

**Step 1** Obtain the installation package.

Find the **link** to the required version on the download page. MySQL-client-5.7.31-1.el6.x86\_64.rpm is used as an example in the following figure.

**Figure 7-1** Download

MySQL Product Archives  
MySQL Community Server (Archived Versions)

**⚠ Please note that these are old versions. New releases will have recent bug fixes and features!**  
To download the latest release of MySQL Community Server, please visit [MySQL Downloads](#).

Product Version:   
 Operating System:   
 OS Version:

Package Name	Release Date	Size	Download
<b>RPM Bundle</b> (mysql-5.7.31-1.el6.x86_64.rpm-bundle.tar)	Jun 3, 2020	467.1M	<a href="#">Download</a>
<b>RPM Package, MySQL Server</b> (mysql-community-server-5.7.31-1.el6.x86_64.rpm)	Jun 3, 2020	161.7M	<a href="#">Download</a>
<b>RPM Package, Client Utilities</b> (mysql-community-client-5.7.31-1.el6.x86_64.rpm)	Jun 3, 2020	24.6M	<a href="#">Download</a>
<b>RPM Package, Development Libraries</b> (mysql-community-devel-5.7.31-1.el6.x86_64.rpm)	Jun 3, 2020	3.7M	<a href="#">Download</a>
<b>RPM Package, Development Libraries</b> (mysql-community-embedded-devel-5.7.31-1.el6.x86_64.rpm)	Jun 3, 2020	131.0M	<a href="#">Download</a>

**Step 2** Upload the installation package to the ECS.

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

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

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

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

**NOTE**

- If there are any conflicts during the installation, add the **replacefiles** parameter to the command and try to install the client again. Example:  
rpm -ivh --replacefiles MySQL-client-5.7.31-1.el6.x86\_64.rpm
- If a message is displayed prompting you to install a dependency package, you can add the **nodeps** parameter to the command and install the client again. Example:  
rpm -ivh --nodeps MySQL-client-5.7.31-1.el6.x86\_64.rpm

----End

## 7.2 How Can I Install a PostgreSQL Client?

PostgreSQL provides [client installation methods](#) for different OSs on its official website.

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

### Procedure

**Step 1** Log in to an ECS.

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

**Step 2** Open the [client installation page](#).

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

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

**Figure 7-2** Installing a client

To use the PostgreSQL Yum Repository, follow these steps:

```
# Install the repository RPM:
sudo yum install -y https://download.postgresql.org/pub/repos/yum/repoprms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm

# Install PostgreSQL:
sudo yum install -y postgresql12-server

# Optionally initialize the database and enable automatic start:
sudo /usr/pgsql-12/bin/postgresql-12-setup initdb
sudo systemctl enable postgresql-12
sudo systemctl start postgresql-12
```

- 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 7-3** Installing the RPM package

```

root@ecs-d605 ~]# sudo yum install -y https://download.postgresql.org/pub/repos/yum/reposrums/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
Loaded plugins: fastestmirror
pgdg-redhat-repo-latest.noarch.rpm                               | 8.6 kB  00:00:00
Examining /var/tmp/yum-root-2onITG/pgdg-redhat-repo-latest.noarch.rpm: pgdg-redhat-repo-42.0-28.noarch
Marking /var/tmp/yum-root-2onITG/pgdg-redhat-repo-latest.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
--> Package pgdg-redhat-repo.noarch 0:42.0-28 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch          Version           Repository          Size
=====
Installing:
pgdg-redhat-repo       noarch        42.0-28           /pgdg-redhat-repo-latest.noarch 13 k
Transaction Summary
-----
Install 1 Package

Total size: 13 k
Installed size: 13 k
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Warning: RPMDB altered outside of yum.
Installing : pgdg-redhat-repo-42.0-28.noarch                               1/1
Verifying  : pgdg-redhat-repo-42.0-28.noarch                               1/1

Installed:
  pgdg-redhat-repo.noarch 0:42.0-28

Complete!

```

**Figure 7-4** Client installed

```

Total                                                                 467 kB/s | 14 MB  00:00:30
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Importing GPG key 0x442DF0F8:
  Userid   : "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
  Fingerprint: 60c9 e2b9 1a37 d136 fe74 d176 1f16 d2e1 442d f0f8
  Package   : pgdg-redhat-repo-42.0-28.noarch (@/pgdg-redhat-repo-latest.noarch)
  From      : /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libicu-58.2-4.e17_7.x86_64                                1/4
  Installing : postgresql12-libs-12.13-1PGDG.rhel7.x86_64              2/4
  Installing : postgresql12-12.13-1PGDG.rhel7.x86_64                  3/4
  Installing : postgresql12-server-12.13-1PGDG.rhel7.x86_64           4/4
  Verifying  : postgresql12-libs-12.13-1PGDG.rhel7.x86_64             1/4
  Verifying  : postgresql12-12.13-1PGDG.rhel7.x86_64                  2/4
  Verifying  : postgresql12-server-12.13-1PGDG.rhel7.x86_64          3/4
  Verifying  : libicu-58.2-4.e17_7.x86_64                              4/4

Installed:
  postgresql12-server.x86_64 0:12.13-1PGDG.rhel7

Dependency Installed:
  libicu.x86_64 0:58.2-4.e17_7      postgresql12.x86_64 0:12.13-1PGDG.rhel7      postgresql12-libs.x86_64 0:12.13-1PGDG.rhel7

Complete!

```

**Step 4** Connect to the RDS for PostgreSQL instance.

**Figure 7-5** Connection successful

```

root@ecs-d605 ~]# psql -h ██████████ -d postgres -U root
Password for user root:
psql (12.13, server 12.11)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=>

```

----End

## 7.3 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

# 8 Backup and Restoration

---

## 8.1 How Long Does RDS Store Backup Data For?

Automated backup data is kept based on the backup retention period you specified.

There is no limit for the manual backup retention period. You can delete manual backups as needed.

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

## 8.2 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.

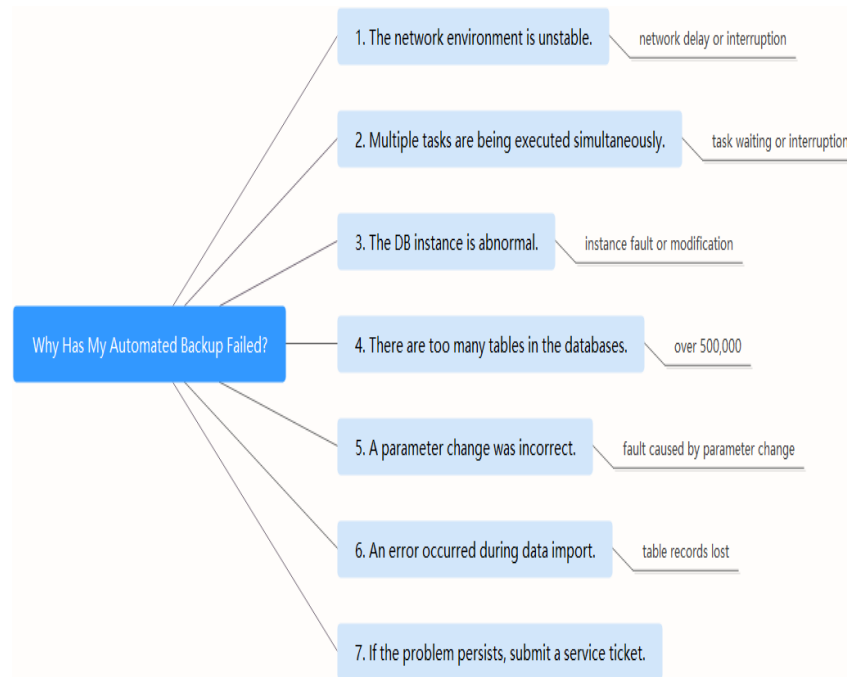
## 8.3 How Can I Back Up an RDS Database to an ECS?

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.

## 8.4 Why Has My Automated Backup Failed?

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

**Figure 8-1** 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.

## 8.5 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.

# 9 Database Monitoring

---

## 9.1 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).

### Measures:

- If a CPU or memory alarm is reported, you can scale up the vCPUs or memory by changing the DB instance class.
- If a storage space usage alarm is reported, you can:
  - Check the storage space consumption to see if any space can be freed up by deleting data from DB instances or by dumping the data to another system.
  - Scale up the storage space.

# 10 Capacity Expansion and Specification Change

---

## 10.1 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. To prevent service interruption, perform the operation during off-peak hours. Changing an instance class takes 5 to 15 minutes.

After you change the instance class of a DB instance, the DB instance will be rebooted and the cache in the memory will be automatically cleared. A failover is triggered during the change. The change process involves changing the instance class of the standby instance, rebooting the standby instance, performing a failover, changing the instance class of the new standby instance, and then rebooting the new standby instance. Workloads can be interrupted during the failover. The length of the interruption depends on how long the failover will take.

## 10.2 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

- 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.

# 11 Database Parameter Modification

---

## 11.1 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.  
$$\text{max\_connections value} + \text{autovacuum\_max\_workers value} + \text{max\_worker\_processes value} + 1 < 8388607$$

### 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.

## 11.2 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**.

# 12 Log Management

---

## 12.1 How Can I Obtain RDS for SQL Server Error Logs Using Commands?

**Step 1** .

**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 12-1** shows the query results.

**Figure 12-1** Example query results

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

**----End**

# 13 Network Security

---

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

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

## 13.2 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.

## 13.3 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.

## 13.4 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.