RDS for PostgreSQL

FAQs

Issue 01

Date 2025-09-11

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

1 Product Consulting....1
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 Will Different RDS DB Instances Share CPU and Memory Resources?....1
1.4 How Long Does It Take to Create an RDS for PostgreSQL Instance?....2
1.5 What Can I Do About Slow Responses of Websites When They Use RDS?....2
1.6 What Is the Time Delay for Primary/Standby Replication?....2
1.7 Can Multiple ECSs Connect to the Same RDS DB Instance?....3
1.8 Will Backups Be Encrypted After Disk Encryption Is Enabled for My RDS for PostgreSQL Instance?....3
1.9 What Is the Availability of RDS DB Instances?....3
1.10 Does RDS for PostgreSQL Support Cross-AZ High Availability?....3
1.11 Does RDS for PostgreSQL Support CloudPond?....4
1.12 Can I Use an Encrypted Password to Log In to an RDS DB Instance?....4
1.13 What Are the Differences Between Floating and Private IP Addresses of RDS DB Instances?....4
1.14 What Can I Do If I Can't Find My RDS Resources?....6
2 Resource Freezing, Release, Stopping, Deletion, and Unsubscription....8
3 Resource and Disk Management....10
3.1 Which Types of Logs and Files Occupy RDS for PostgreSQL Storage Space?....10
3.2 Which Items Occupy the Storage Space of My RDS for PostgreSQL Instances?....11
3.3 How Much Storage Space Is Required for DDL Operations?....11
3.4 What Are the Differences Between the Storage Space and Backup Space of an RDS for PostgreSQL Primary/Standby Instance?....11
4 Database Connection....13
4.1 What Do I Do If There Are Too Many Database Connections?....13
4.2 What Is the Maximum Number of Connections to an RDS for PostgreSQL Instance?....14
4.3 What Should I Do If an ECS Cannot Connect to an RDS for PostgreSQL Instance Through a Private Network?....15
4.4 What Should I Do If My RDS for PostgreSQL Instance Fails to Be Connected Due to Database Client Problems?....16
4.5 What Should I Do If an RDS for PostgreSQL Database Problem Causes a Connection Failure?....16
4.6 Do Applications Need to Support Reconnecting to an RDS DB Instance Automatically?....17
4.7 Why Can't I Ping My EIP After It Is Bound to an RDS DB Instance?....17
4.8 Can I Access an RDS for PostgreSQL Instance over an Intranet Across Regions?....18

4.9 Why Did the New Password Not Take Effect After I Reset the Administrator Password of My RDS for PostgreSQL Instance? 18
4.10 Can I Access Standby RDS DB Instances? 19
4.11 Will My Access Be Restricted by Bandwidth When I Connect to My RDS for PostgreSQL Instance from an ECS over a Private Network? 19

5 Database Migration 20
5.1 What Types of DB Engines Does RDS Support for Importing Data? 20
5.2 Why Do I Need to Use the pg_dump Tool for Migration? 20

6 Database Permission 21
6.1 Why Does the Root User of My RDS for PostgreSQL Instance Not Have the Super Permissions? 21
6.2 What Are the Differences Between RDS ManageAccess and DAS Permissions? 21
6.3 How Do I View Authorized Databases After a Local Client Is Connected to an RDS DB Instance? 22
6.4 Can Multiple Users Log In to an RDS Instance Through DAS at the Same Time? Will the Accounts Be Locked If I Enter Wrong Passwords Several Times in a Row? 22
6.5 Why Did I Fail to Create an Object on the **postgres** Database as a Common User? 22
6.6 What Should I Do If a Role Failed to Be Deleted from an RDS for PostgreSQL Instance? 24
6.7 Why Did My RDS for PostgreSQL Migration Fail? 26
6.8 How Do I Grant the REPLICATION Permission to an RDS for PostgreSQL Database User? 27
6.9 Why Is An Error Reported When I Attempt to Change a Table Owner of My RDS for PostgreSQL Instance? 27

7 Database Storage 29
7.1 What Types of Storage Does RDS Use? 29
7.2 How Do I View the Storage Usage of My RDS Instance? 29

8 Database Usage 31
8.1 How Do I Use DAS to Query SQL Statements? 31
8.2 How Do I View Session IDs and Login and Logout Time of an RDS Database? 32
8.3 What Should I Do If Garbled Characters Are Displayed After SQL Query Results Are Exported to an Excel File for My RDS Instance? 33
8.4 Does the OPTIMIZE TABLE Operation Lock Tables on an RDS DB Instance? 33

9 Backup and Restoration 34
9.1 How Do I View My Backup Storage Usage? 34
9.2 How Is RDS for PostgreSQL Backup Data Billed? 35
9.3 Why Has Automated Backup of My RDS Instance Failed? 35
9.4 Why Is a Table or Data Missing from My RDS for PostgreSQL Database? 37
9.5 How Long Does RDS for PostgreSQL Store Backup Data For? 37
9.6 How Do I Clear RDS for PostgreSQL Backup Space? 37
9.7 Can My RDS for PostgreSQL Instance Still Be Used in the Backup Window? 38
9.8 How Can I Back Up an RDS for PostgreSQL Database to an ECS? 38
9.9 Can I Dump RDS for PostgreSQL Backups to My OBS Bucket? 38
9.10 Does RDS for PostgreSQL Support Restoration of Only a Single Table? 38

10 Read Replicas and Read/Write Splitting 39

10.1 Can I Change the Replication Mode Between RDS for PostgreSQL Primary Instances and Read Replicas? 39
10.2 Does RDS for PostgreSQL Support Read/Write Splitting? 39
11 Database Monitoring 41
11.1 Which RDS for PostgreSQL Instance Metrics Do I Need to Pay Attention To? 41
11.2 How Can I Calculate the Memory Usage of an RDS DB Instance? 42
12 Capacity Expansion and Specification Change 43
12.1 Are My RDS for PostgreSQL Instances Still Available During Storage Scale-up or Instance Class Change? 43
12.2 Why Does My RDS for PostgreSQL Instance Become Faulty After Its Database Port Is Changed? 44
12.3 Can I Change the VPC or Subnet that My RDS for PostgreSQL Instance Belongs To? 44
13 Database Parameter Modification 45
13.1 Can I Use SQL Commands to Modify Global Parameters of My RDS Instance? 45
13.2 How Do I Change the Time Zone of My RDS for PostgreSQL Instance? 45
13.3 What Inappropriate Parameter Settings Will Cause Unavailability of My RDS for PostgreSQL Instance? 46
13.4 How Do I Set the Upper Limit for the Storage Space Occupied by Temporary Files of My RDS for PostgreSQL Instance? 47
13.5 How Do I Configure the test_decoding Extension for My RDS for PostgreSQL Instance? 47
14 Network Security 49
14.1 How Can Secure Data Transmission Be Ensured When I Access an RDS for PostgreSQL Instance Through an EIP? 49
14.2 How Can I Prevent Untrusted Source IP Addresses from Accessing RDS for PostgreSQL? 49
14.3 How Do I Import the SSL Certificate of an RDS Instance to a Windows or Linux Server? 49
14.4 What Are the Possible Causes for Data Corruption of an RDS Instance? 51
14.5 After My RDS for PostgreSQL Instance Is Deleted, Why Can't the Associated Security Group Be Deleted Immediately? 52
15 Version Upgrade 53
15.1 How Can I View the Version of an RDS DB Instance? 53
15.2 Does RDS for PostgreSQL Support Major Version Upgrades? 53
16 Developer-Related APIs and SDKs for RDS 55

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 only visible in the RDS backend 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 Will Different RDS DB Instances Share CPU and Memory Resources?

Yes, that depends on the instance class.

- General-purpose:

CPU resources are shared with other general-purpose DB instances on the same physical machine. CPU usage is maximized through resource overcommitment. This instance class is a cost-effective option and suitable for scenarios where performance stability is not critical.

- Dedicated:

  The instance has dedicated CPU and memory resources to ensure stable performance. The performance of a dedicated instance is never affected by other instances on the same physical machine. This instance class is good when performance stability is important.

1.4 How Long Does It Take to Create an RDS for PostgreSQL Instance?

- It takes 5 to 7 minutes to create a single-node or primary/standby instance.
- 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.

If creating an instance takes much more time than described above, there may be problems during the creation. In this case, contact customer service by **submitting a service ticket**.

1.5 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.

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

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

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

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

- Load balancing of the standby DB instance and read replicas

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

RDS for 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.

1.7 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.

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

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.

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.

1.9 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%

1.10 Does RDS for PostgreSQL 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 for PostgreSQL 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

1.11 Does RDS for PostgreSQL Support CloudPond?

Yes. For details, see **CloudPond and Other Services**.

1.12 Can I Use an Encrypted Password to Log In to an RDS DB Instance?

No. When you log in to an RDS instance, use the password set on the console for authentication. Encrypted password authentication is not supported.

1.13 What Are the Differences Between Floating and Private IP Addresses of RDS DB Instances?

Definitions of the Floating IP Address and Private IP Address

After an RDS DB instance is created, the system assigns the instance a floating IP address, which is used by external systems to connect to the instance over a private network.

The system also assigns a private IP address to each database node for internal network communication (two private IP addresses for a primary/standby instance,

one for a single-node instance, and one for a read replica). Private IP addresses cannot be accessed by external systems.

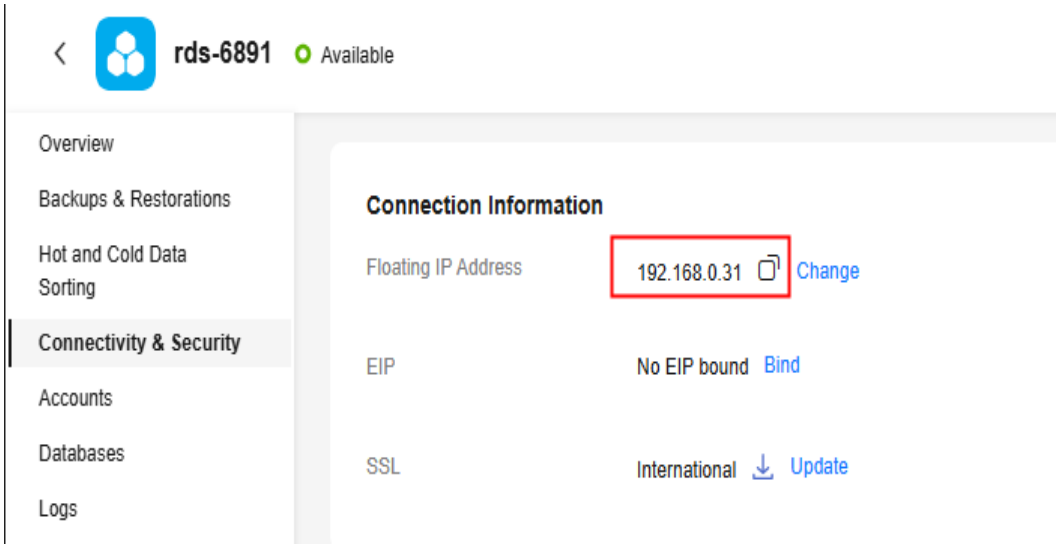
For more information, see **What Are the Differences Between EIPs, Private IP Addresses, and Virtual IP Addresses?**

Querying the Floating and Private IP Address of an RDS DB Instance

- Floating IP address

  On the RDS console, click the name of a DB instance to go to the **Overview** page. In the navigation pane on the left, choose **Connectivity & Security** to check the floating IP address of the instance.

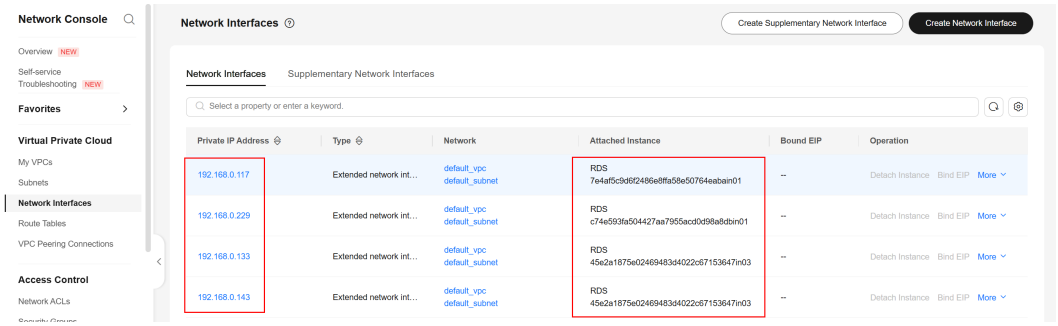
  Figure 1-2 Floating IP address



- Private IP address

  Log in to the management console and choose **Networking** > **Virtual Private Cloud**. In the navigation pane on the left, choose **Network Interfaces** to check the private IP addresses of the RDS instance.

  Figure 1-3 Checking the private IP addresses



1.14 What Can I Do If I Can't Find My RDS Resources?

Symptom

After I logged in to the management console, I could not find my purchased RDS resources.

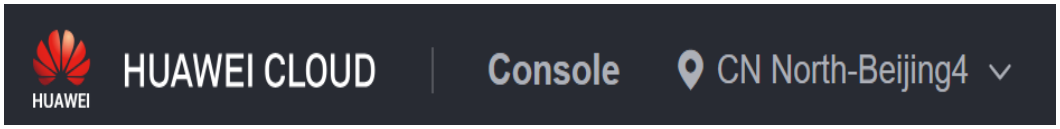
Possible Causes

- Your purchased resources are not in the selected region.
- Your purchased resources are not under the selected service.

Solution 1

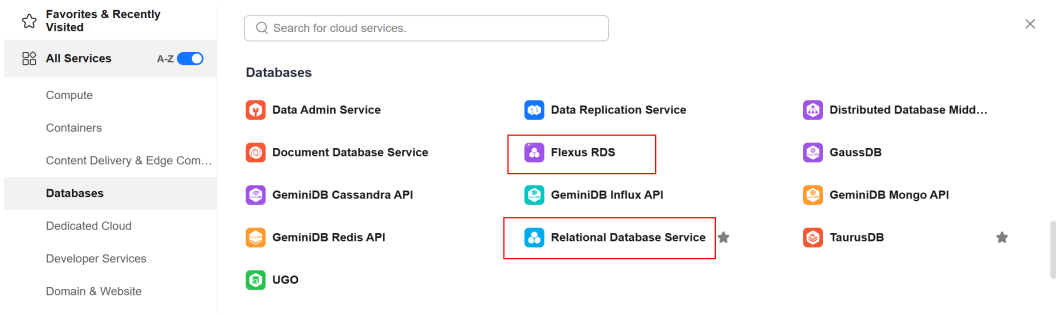
1. **Log in to the management console**.
2. In the upper part of the page, switch to the region that your RDS resources belong to.

   Figure 1-4 Changing a region

3. Click ☰ in the upper left corner and select the correct service name.
   - To search for RDS DB instances, choose **Databases** > **Relational Database Service**.
   - To search for FlexusRDS DB instances, choose **Databases** > **Flexus RDS**.

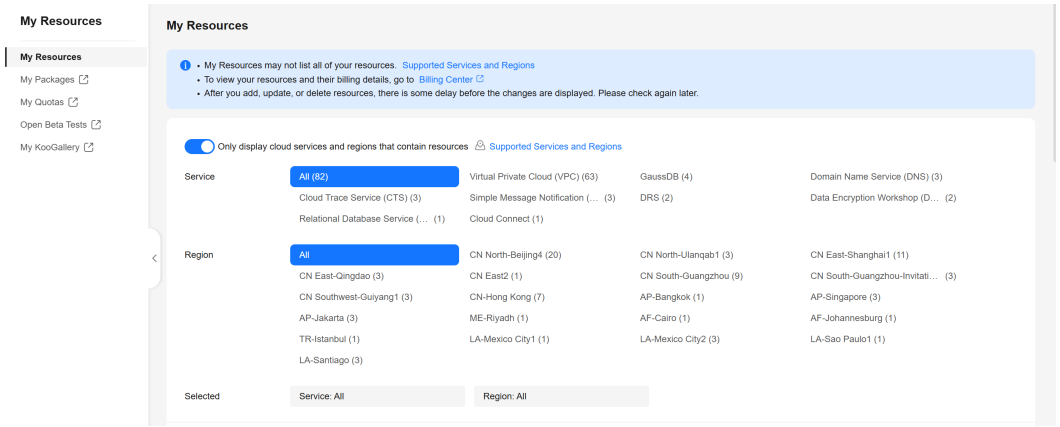
   Figure 1-5 Selecting a service

Solution 2

1. **Go to the My Resources page**.
2. Select the correct service and region to view the purchased resources.

Figure 1-6 My Resources



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, the system 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 VM where the DB instance is located is no longer billed. Other resources, including EIPs, storage resources, 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.

Deleted instances will be no longer billed. For details, see **Billing Termination**.

3 Resource and Disk Management

3.1 Which Types of Logs and Files Occupy RDS for PostgreSQL Storage Space?

The following logs and files occupy RDS for PostgreSQL storage space.

Table 3-1 PostgreSQL database file types

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

Solution

1. If the original storage space is insufficient as your services grow, scale up storage space of your DB instance.
2. If data occupies too much storage space, run **DROP** or **TRUNCATE** 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 WAL logs are generated and occupy space if there are large amounts of insert, delete, and update operations in a short period.
4. Use Cloud Eye to monitor the size, usage, and utilization of storage space of your DB instance and set alarm policies.

3.2 Which Items Occupy the Storage Space of My RDS for PostgreSQL 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, WAL logs, and indexes) take up storage space on your DB instances. The storage space includes the file system overhead required for inode, reserved blocks, and database operations. Log files generated by RDS for PostgreSQL database servers also occupy storage space.

These files ensure the stability of RDS for PostgreSQL instances.

3.3 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).

3.4 What Are the Differences Between the Storage Space and Backup Space of an RDS for PostgreSQL Primary/Standby Instance?

In an RDS for PostgreSQL primary/standby instance, the node accessed by applications is called the primary instance, and data on the primary instance is synchronized to the other node (called the standby instance) in real time. The standby instance acts as a failover target for the primary. If the primary instance fails, RDS for PostgreSQL promotes the standby instance to primary for high availability.

- Storage space

  Storage space of the standby instance is the same as that of the primary instance. Scaling up the storage space of the primary instance will also scale up that of the standby instance.

  Data on the primary instance may not be synchronized to the standby instance fast enough when there are a large number of data writes or a long replication delay. If this happens, the primary instance retains WAL logs for replication. WAL logs will be stacked and occupy storage space.

- Backup space

  Backup space is used to store automated backups, manual backups, and SQL audit logs. You can get a free backup space of the same size as your purchased storage space. If the free backup space is used up, the additional space will be billed. You can configure a custom backup policy to best fit your workloads' needs.

To release backup space, see **How Do I Clear RDS Backup Space?**

4 Database Connection

4.1 What Do I Do If There Are Too Many Database Connections?

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.

   For details, see **Connecting to an RDS for PostgreSQL Instance Through a Private Network**.
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.

4.2 What Is the Maximum Number of Connections to an RDS for PostgreSQL Instance?

RDS for PostgreSQL does not have constraints on how many connections are supported. It depends on the default values and value ranges of certain parameters in your DB engine.

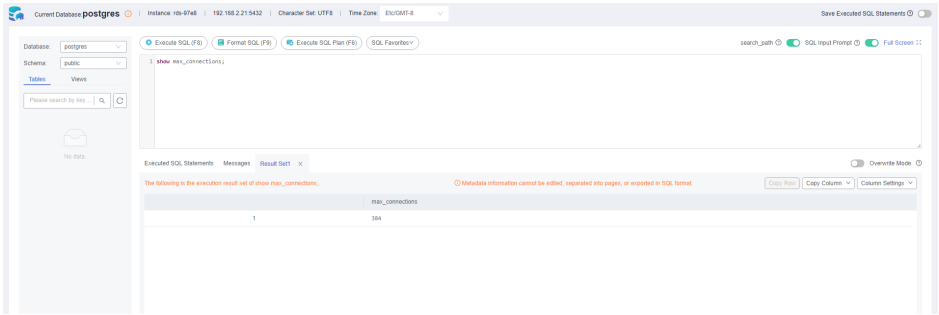
Definition

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

How to Change It

- You can change the maximum number of connections allowed on the console. For details, see **Modifying Parameters of an RDS for PostgreSQL Instance**.
- You can run the following command to query the maximum number of connections allowed:

```
show max_connections;
```



If you want to change the maximum number of connections by running commands, **submit a service ticket** to apply for required permissions.

Setting the Maximum Number of Connections to an Appropriate Value

The **max_connections** parameter is closely related to the memory (GB) of the DB instance. The calculation formula is as follows:

Table 4-1 Calculation formula

Parameter	Formula	Version Involved	Unit
max_connections	min((total_mem_kb - shared_buffer) * 1024.0 / 16MB, 5000)	All versions	Count

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

Table 4-2 Default values of max_connections for different memory specifications

Memory (GB)	Max. Client Connections (max_connections)
512	5,000
384	5,000
256	5,000
128	5,000
64	3,072
32	1,536
16	768
8	384
4	192
2	96

4.3 What Should I Do If an ECS Cannot Connect to an RDS for PostgreSQL Instance Through a Private Network?

Perform the following steps to identify the problem:

Step 1 Check whether the ECS and RDS for PostgreSQL instance are located in the same VPC.

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

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

For details, see **Configuring a Security Group Rule**.

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

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

```
curl -kv EIP:5432
```

- If the ECS can connect to the DB instance, no further action is required.
- If the ECS cannot connect to the DB instance, contact technical support.

----End

4.4 What Should I Do If My RDS for PostgreSQL Instance Fails to Be Connected Due to Database Client Problems?

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

1. ECS Security Policy

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

2. Application Configuration

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

3. Username or Password

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

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

NOTE

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

4.5 What Should I Do If an RDS for PostgreSQL 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 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 the ECS. If you connect to the 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 for PostgreSQL resource monitoring to check if the CPU usage and the number of connections are within the allowed ranges. If either of them has reached the maximum, reboot, disconnect, or upgrade the specifications of the RDS for PostgreSQL instance.

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

4.6 Do Applications Need to Support Reconnecting to an 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.

4.7 Why Can't I Ping My EIP After It Is Bound to an RDS 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.
   c. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
   d. On the **Instances** page, click the DB instance name to go to the **Overview** page.
   e. Under **Security Group**, click the security group name.
   f. Check whether the security group allows the inbound ICMP traffic.

Table 4-3 Security group rules

Direction	Action	Type	Protocol & Port	Source/ Destination	Description
Inbound	Allow	IPv4	ICMP: All	Source: 0.0.0.0/0	This rule allows ICMP traffic to RDS instances in this security group over any port to verify network connectivity using the **ping** command.

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 technical support.

4.8 Can I Access an RDS for PostgreSQL Instance over an Intranet 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 details, see **Using psql CLI to Connect 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**.

4.9 Why Did the New Password Not Take Effect After I Reset the Administrator Password of My RDS for PostgreSQL Instance?

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**.

4.10 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.

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

No.

5 Database Migration

5.1 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.

5.2 Why Do I Need to Use the pg_dump Tool for Migration?

The 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 this tool when there is not much data to migrate or if stopping the server for a long period of time is not an issue.

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

6 Database Permission

6.1 Why Does the Root User of My RDS for PostgreSQL Instance Not Have the Super Permissions?

RDS does not provide the super permissions for the **root** user. That's because the super permissions allow you to execute management commands, such as **reset master**, **set global**, and **reset slave**. These operations can 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)...
- Scenario 3: If you cannot create RDS for PostgreSQL extensions due to lack of super permissions, see **Managing Extensions**.

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

Permission	Description
RDS ManageAccess	Permissions used to manage RDS DB instances

Permission	Description
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 How Do I View Authorized Databases After a Local Client Is Connected to an RDS DB Instance?

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

show grants for root@'*ip*';

show grants for root@'%';

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

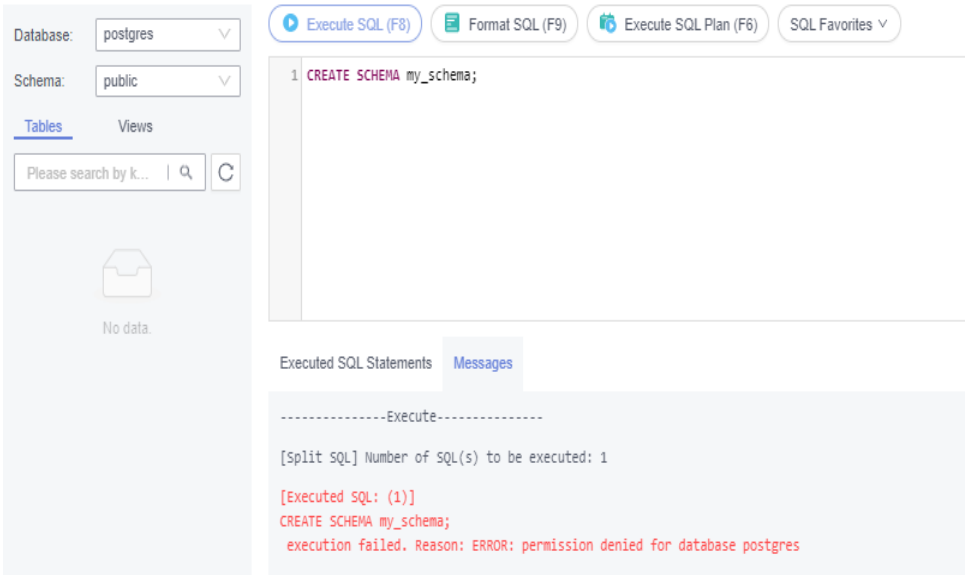
Multiple users can log in to an RDS Instance through DAS at the same time. The passwords will not be locked after multiple failed login attempts.

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.

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

Symptom

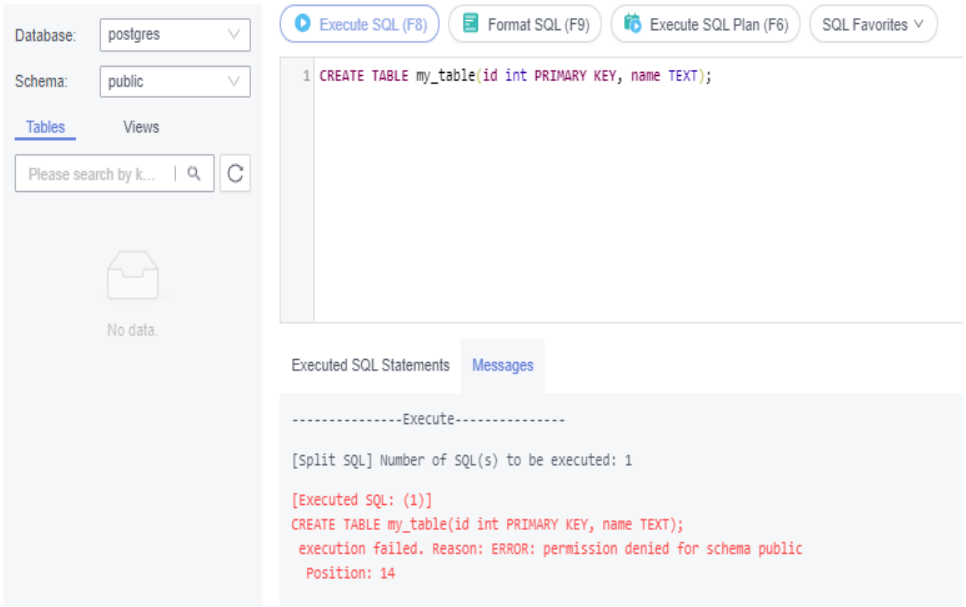
- **Creating a Schema as a Common User**
  Command: **CREATE SCHEMA my_schema;**
  Error: ERROR: permission denied for database postgres



- **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 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
pgcore15	Yes	15.4
pgcore16	Yes	16.2

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 an extension.
- Grant an object permission to a user.

6.6 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.

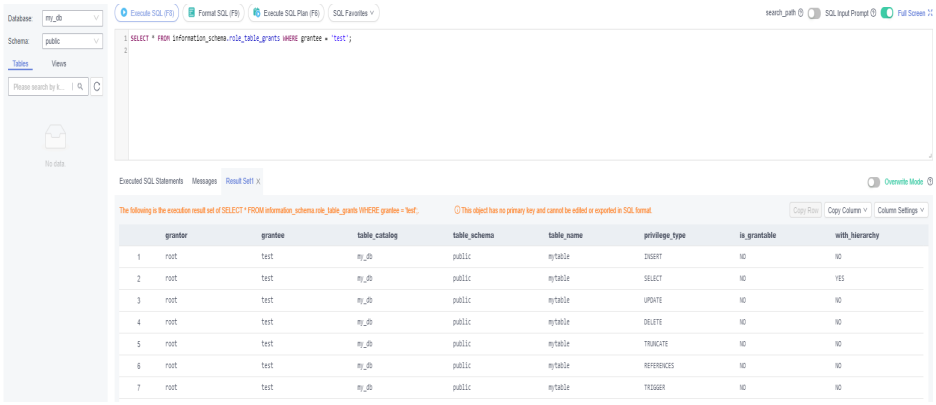
Possible Causes

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.

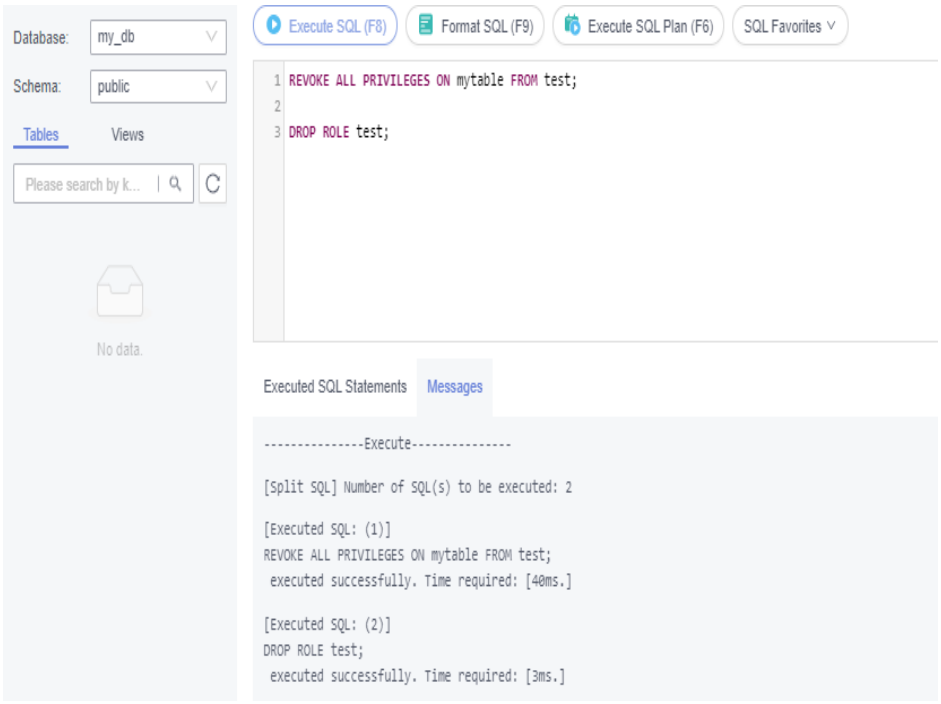
   select * from INFORMATION_SCHEMA.role_table_grants WHERE grantee='test';



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;



6.7 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

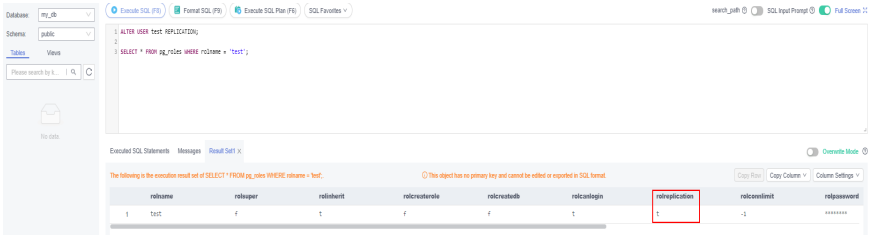
You can run the commands to grant permissions as user **root** only when your database kernel version supports root privilege escalation. For details, see **Privileges of the root User**.

6.8 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

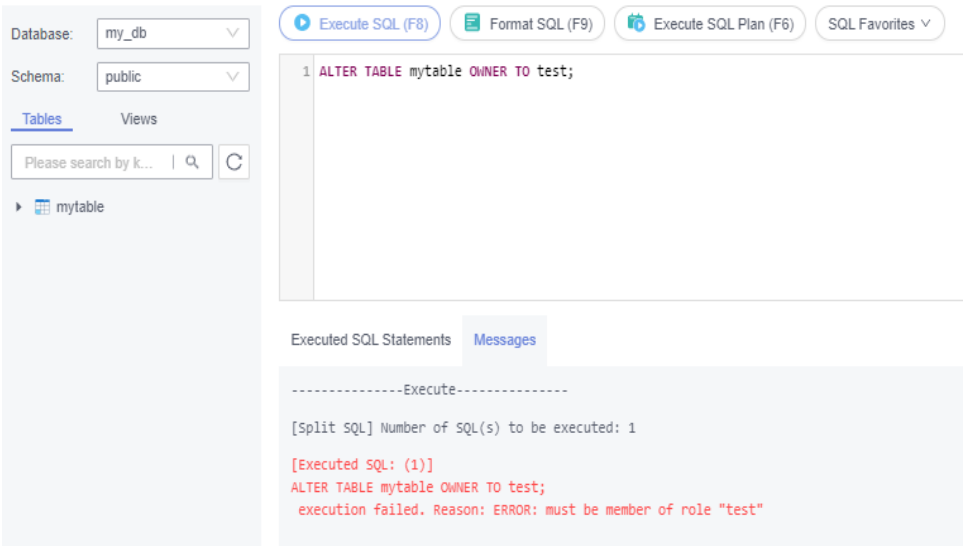
You can run the commands to grant permissions as user **root** only when your database kernel version supports root privilege escalation. For details, see **Privileges of the root User**.

6.9 Why Is An Error Reported When I Attempt to Change a Table Owner of My RDS for PostgreSQL Instance?

Symptom

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

ALTER TABLE mytable OWNER TO test;



Possible Causes

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

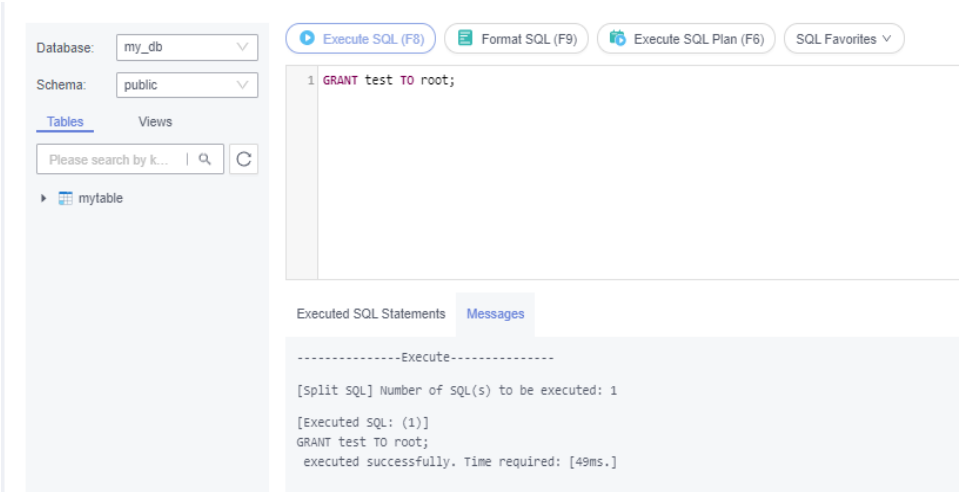
NOTE

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

Solution

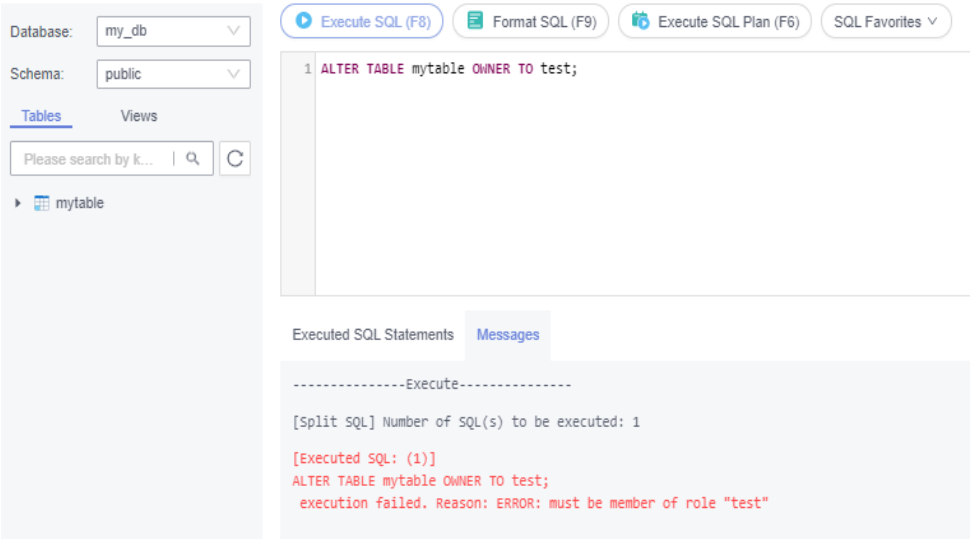
1. Log in to the database as user **test**.
2. Run the following command as user **test**:

   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;



7 Database Storage

7.1 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***.

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

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

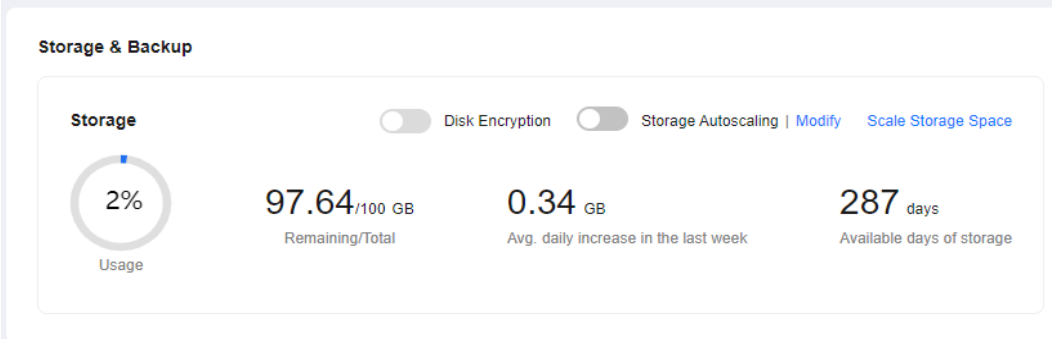
Step 2 Click  in the upper left corner and select a region.

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 **Overview** page, view the storage space usage in the **Storage & Backup** area.

Figure 7-1 Storage space



----End

8 Database Usage

8.1 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.

Procedure

Step 1 Log in to the management console.

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

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**.

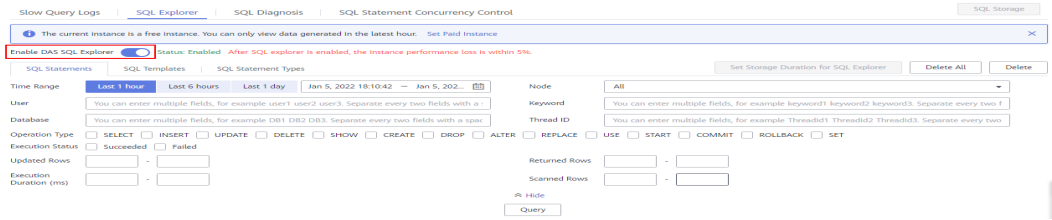
Step 6 In the navigation pane, choose **Cloud DBA (Intelligent O&M)** to go to the **Instance Overview** page.

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 8-1 Enabling SQL Explorer



Step 10 Filter operation types by referring to **Table 8-1** and click **Export** to export the corresponding SQL statements.

Table 8-1 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

8.2 How Do I View Session IDs and Login and Logout Time of an RDS 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 following commands in the database:

```
SELECT
  pid AS session_id,
  usename AS login_user,
  datname AS database_name,
  backend_start AS login_time,
  state,
  query
FROM pg_stat_activity
ORDER BY backend_start DESC;
```


8.3 What Should I Do If Garbled Characters Are Displayed After SQL Query Results Are Exported to an Excel File for My RDS Instance?

The default code is utf8. You need to convert the default code to Unicode in the exported Excel file.

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

When the OPTIMIZE TABLE operation is performed on an RDS DB instance, the tables are locked only for a short period of time. During the table locking period, DML operations can be performed but DDL operations cannot. DML will recreate tables, which consumes CPU and disk resources. If there are a large number of concurrent DML operations, the table will be locked for longer. To avoid impacting services, perform the OPTIMIZE TABLE operation during off-peak hours.

9 Backup and Restoration

9.1 How Do I View My Backup Storage Usage?

Step 1 Log in to the management console.

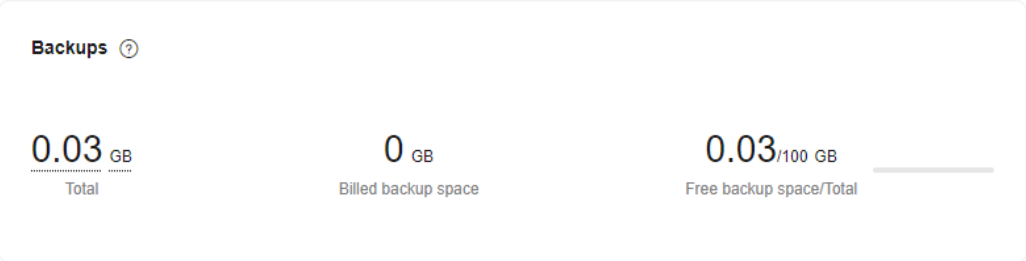
Step 2 Click in the upper left corner and select a region.

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 **Overview** page, view the backup space usage in the **Backups** area.

Figure 9-1 Backups



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

9.2 How Is RDS for PostgreSQL Backup Data Billed?

All the RDS full and incremental 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 **Price Calculator**.

NOTICE

If your storage is frozen, it is no longer billed and the free backup space is also unavailable.

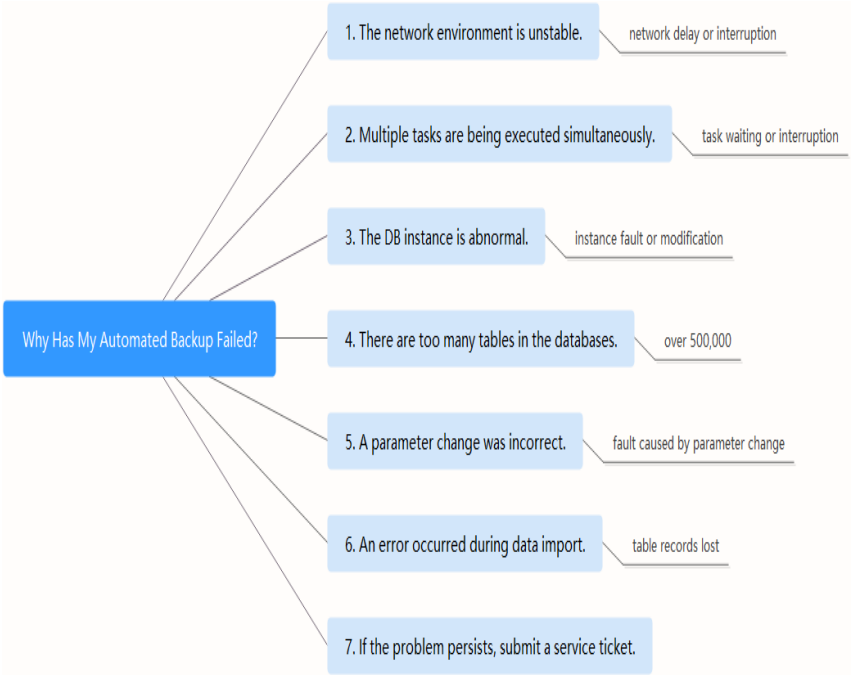
If your DB instance is frozen, no free backup space is available and the original backups generated before the instance is frozen will be billed.

- If you unfreeze the DB instance, the free backup space will be restored.
- If you delete the frozen DB instance, the existing automated backups will also be deleted. You need to manually delete the existing manual backups. After all the backups are removed, the backup space will no longer be billed.

9.3 Why Has Automated Backup of My RDS Instance Failed?

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

Figure 9-2 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.

  If system catalog records are lost due to inappropriate data import, import the data again by referring to **Migration Solution Overview**.
- If the problem persists, **submit a service ticket** for assistance.

9.4 Why Is a Table or Data Missing from My RDS for PostgreSQL Database?

RDS for PostgreSQL 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 **SQL audit has been enabled**, you can view data execution records in audit logs.

Restore data using backup files:

- Use the RDS for PostgreSQL restoration function.
- Import the backup data to RDS for PostgreSQL from an ECS.

9.5 How Long Does RDS for PostgreSQL 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.

9.6 How Do I Clear RDS for PostgreSQL Backup Space?

The RDS for PostgreSQL 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 **configuring a 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 can change the retention period. Audit logs that have expired will be automatically deleted. For details, see **Enabling SQL Audit**.

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

9.7 Can My RDS for PostgreSQL Instance Still Be Used in the Backup Window?

A backup window is a user-specified time during which RDS for PostgreSQL instances are backed up. With these periodic data backups, RDS for PostgreSQL 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.

9.8 How Can I Back Up an RDS for PostgreSQL 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 as the database backup space is not recommended.

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

9.9 Can I Dump RDS for PostgreSQL Backups to My OBS Bucket?

No. Backups cannot be directly dumped to your OBS bucket.

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

9.10 Does RDS for PostgreSQL Support Restoration of Only a Single Table?

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 Read Replicas and Read/Write Splitting

10.1 Can I Change the Replication Mode Between RDS for PostgreSQL Primary Instances and Read Replicas?

Both asynchronous (default) and synchronous replication between the primary and standby instances are supported.

- Asynchronous replication is recommended for applications requiring a guarantee of high availability.
- Synchronous replication is recommended for applications that require strong data consistency and can tolerate a short-time blocking of write operations.

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

10.2 Does RDS for PostgreSQL Support Read/Write Splitting?

Yes. For details, see **Table 10-1**.

Table 10-1 RDS for PostgreSQL read/write splitting

Database	Read/Write Splitting	Database Proxy	Remarks
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 **Introduction to Read Replicas**. For details about how to implement read/write splitting, see **Using Client Drivers to Implement Failover and Read/Write Splitting**.

11 Database Monitoring

11.1 Which RDS for PostgreSQL Instance 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 **Troubleshooting High Storage Space Usage**

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

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

To check the memory usage, access the **Dashboard** page of RDS and select **PostgreSQL** from the drop-down list box in the upper part. Then you can check the memory usage of all RDS for PostgreSQL instances created by the current account.

The formula for calculating the memory usage is as follows:

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

12 Capacity Expansion and Specification Change

12.1 Are My RDS for PostgreSQL Instances Still Available During Storage Scale-up or Instance Class Change?

Currently, you can scale up storage space or change the vCPU and memory of an RDS for PostgreSQL instance.

- When storage space is being scaled up, RDS for PostgreSQL instances are still available and services are not affected. However, you cannot delete or reboot DB instances that are being scaled.
- 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. To prevent service interruption, perform the operation during off-peak hours. Changing an instance class during peak hours will take much more time.

  When you change the instance class of a primary/standby instance, service downtime only occurs during the primary/standby switchover. The duration of the downtime varies from seconds to minutes based on the replication delay and the number of temporary files. Perform the operation during off-peak hours.

References

- **Scaling Up Storage Space of an RDS for PostgreSQL Instance**
- **Changing the vCPU and Memory of an RDS for PostgreSQL Instance**

12.2 Why Does My RDS for PostgreSQL Instance Become Faulty After Its 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.

12.3 Can I Change the VPC or Subnet that My RDS for PostgreSQL Instance Belongs To?

No. The VPC or subnet cannot be changed after the instance is created.

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

13 Database Parameter Modification

13.1 Can I Use SQL Commands to Modify Global Parameters of My RDS Instance?

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.

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

13.2 How Do I Change the Time Zone of My RDS for PostgreSQL Instance?

RDS for PostgreSQL allows you to select a time zone when you create an instance and change the time zone after the instance is created.

NOTICE

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

Step 1 Log in to the management console.

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

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 the time zone parameter **timezone** in the search box.

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

13.3 What Inappropriate Parameter Settings Will Cause Unavailability of My RDS for PostgreSQL Instance?

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.

13.4 How Do I Set the Upper Limit for the Storage Space Occupied by Temporary Files of My RDS for PostgreSQL Instance?

Parameter Description

The **temp_file_limit** parameter specifies the maximum amount of storage space that a PostgreSQL process can use for temporary files.

When SQL statements are executed, temporary files, such as sort files and hash files, are generated. Any transaction using temporary files whose total size exceeds this limit will be terminated. For details, see **temp_file_limit**.

Parameter Modification

You can modify **temp_file_limit** on the RDS console. For details, see **Modifying Parameters of an RDS for PostgreSQL Instance**.

Precautions

Executing SQL statements or backing up or restoring data will generate temporary files. If the total size of temporary files exceeds the value of **temp_file_limit**, the operation fails. The value of **temp_file_limit** should not be too small.

temp_file_limit can be set to **-1**, indicating that the size of temporary files is not limited. To prevent too many temporary files from using up the storage space and causing service unavailability, do not set **temp_file_limit** to **-1**. In most cases, keep the default value for **temp_file_limit**.

13.5 How Do I Configure the test_decoding Extension for My RDS for PostgreSQL Instance?

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

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

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

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

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 instance name to go to the **Overview** page.

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 Network Security

14.1 How Can Secure Data Transmission Be Ensured When I Access an RDS for PostgreSQL Instance Through an EIP?

When you access a DB instance 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 SSL Encryption**. You can also use Direct Connect or VPN to encrypt data transmission.

14.2 How Can I Prevent Untrusted Source IP Addresses from Accessing RDS for PostgreSQL?

- 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 for PostgreSQL security group to ensure that only trusted source IP addresses can access your DB instance.
- To prevent your database password from being cracked, set a strong password according to the password policies of your RDS for PostgreSQL instance and periodically change it.

14.3 How Do I Import the SSL Certificate of an RDS Instance to a Windows or Linux Server?

Importing the Certificate to a Windows Server

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.

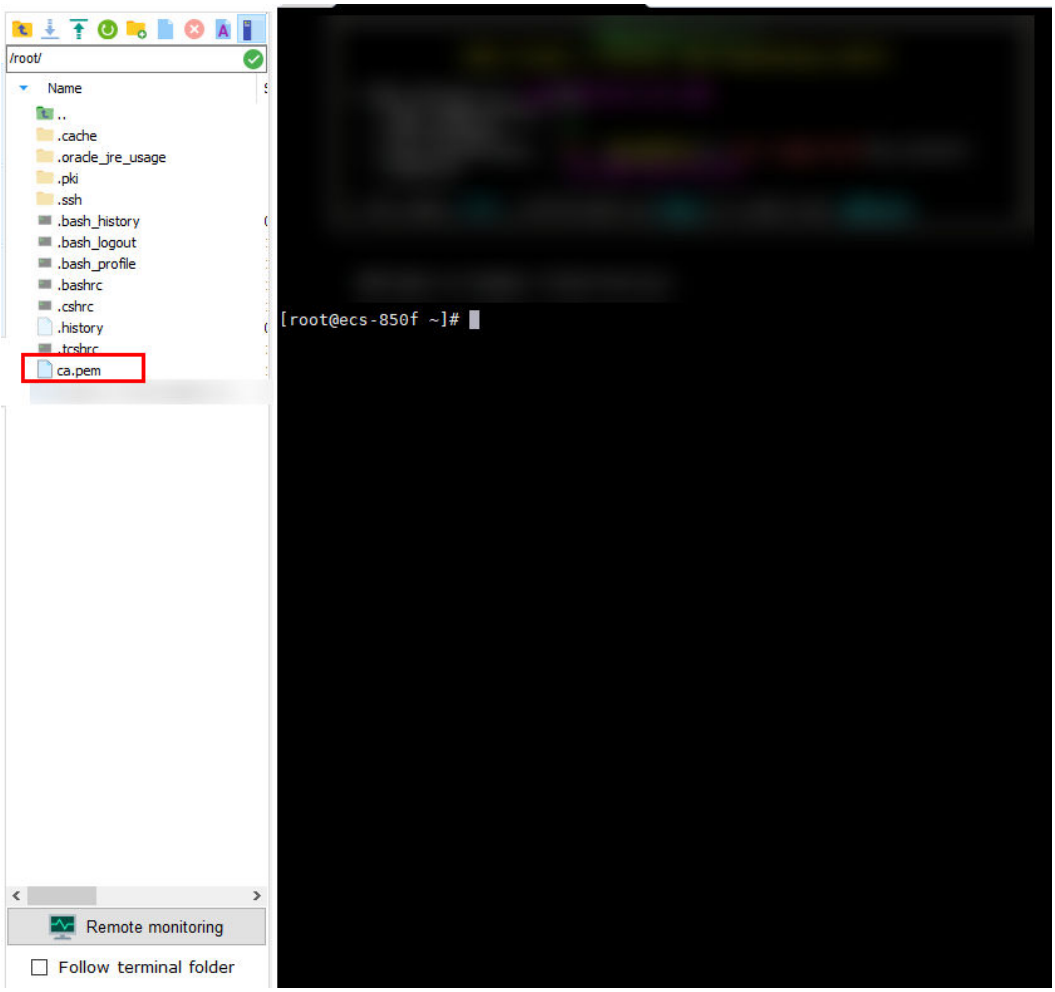
12. Click **Next**.
13. Click **Finish**.
14. Click **OK** to complete the import of the root certificate.

Importing the Certificate to a Linux Server

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

Example:

Figure 14-1 Importing a certificate



14.4 What Are the Possible Causes for Data Corruption of an RDS Instance?

- 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.

- 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. DB instances cannot be accessed during the failover. You need to configure automatic reconnections between applications and DB instances to ensure near-continuous availability.

14.5 After My RDS for PostgreSQL Instance Is Deleted, Why Can't the Associated Security Group Be Deleted Immediately?

When creating a DB instance, you must select a security group. If no security group is available or created, RDS allocates a security group to you by default.

After a DB instance is deleted, it is moved to the recycle bin and retained for seven days by default. To modify the retention period, **configure a recycling policy**.

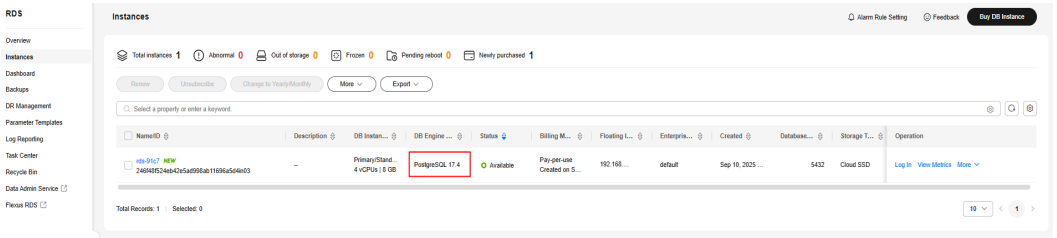
The deleted instance is not removed from the security group immediately until the instance is deleted from the recycle bin. Before deleting a security group, ensure that the security group is not associated with any instance. For details about how to query instances associated with a security group, see **How Do I Know the Instances Associated with a Security Group?**

15 Version Upgrade

15.1 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 15-1 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.

15.2 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 name. On the displayed page, click **Migrate Database** in the upper right corner of the page. If the **Migrate**

Database button is unavailable, **submit a service ticket** to apply for required permissions.

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

16 Developer-Related APIs and SDKs for RDS

Table 16-1 RDS APIs and SDKs

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

