RDS for SQL Server

FAQs

Issue 01

Date 2025-08-21

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 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 SQL Server Instance?

- RDS for SQL Server:
  - Creating a single-node instance takes about 12 to 15 minutes.
  - Creating a primary/standby instance takes about 15 to 18 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 choosing **Service Tickets > Create Service Ticket** in the upper right corner of the management console.

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, 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 recovery model is set to **Simple**, the primary/standby relationship cannot be established and the maximum value of the **Replication Delay** metric will be reported.

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 SQL Server: To check data consistency between the primary and standby DB instances, view **Replication Delay** on the Cloud Eye console to obtain the value of the primary/standby replication delay.

1.7 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 Instance?

If you enable disk encryption when creating an RDS for SQL Server instance, the disk encryption status and the key cannot be changed later. Disk encryption will not encrypt backup data stored in OBS.

NOTICE

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

- If disk encryption is enabled but backup data encryption is not enabled, you can **restore data to a new instance from backups**.
- If both disk encryption and backup data encryption are enabled, data cannot be restored.

1.9 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 Can RDS Primary/Standby DB Instances Be Changed to Single-Node DB Instances?

No. But you can change single-node instances to primary/standby instances. For details, see **Changing a DB Instance Type from Single-Node to Primary/**

Standby. You can use Data Replication Service (DRS) or the export and import tool of the client to migrate data from primary/standby DB instances to single-node DB instances.

1.11 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.

1.12 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.

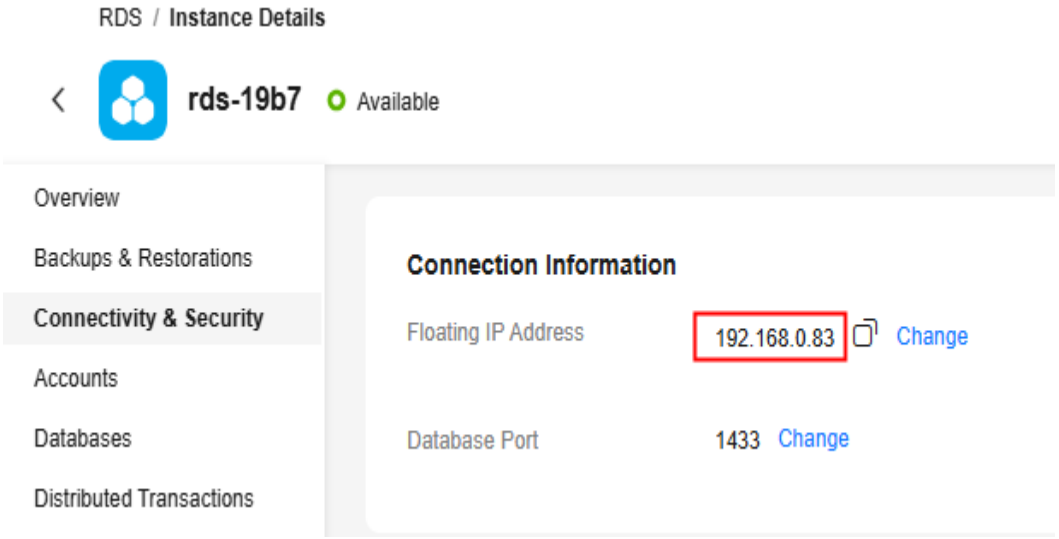
For more information, see **What Are the Differences Between EIPs, Private IP Addresses, and Virtual IP Addresses?**

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.

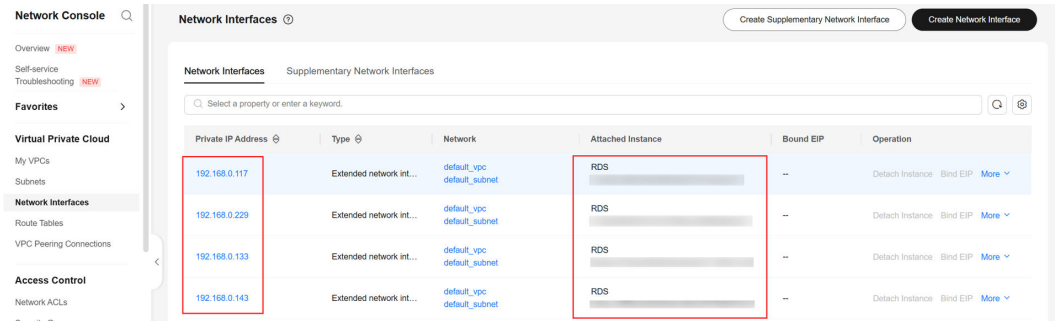
Figure 1-1 Floating IP address



- 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 1-2 Checking the private IP addresses



1.13 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.

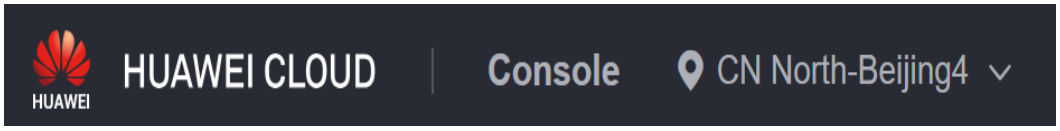
Possible Causes

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

Solution 1

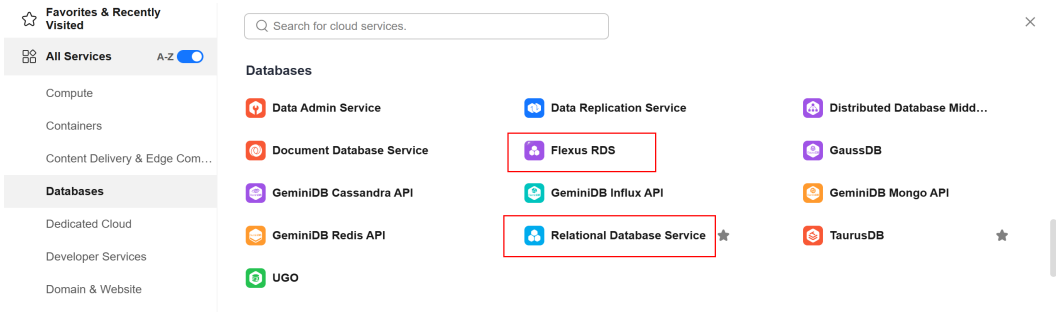
1. **Log in to the management console**.
2. In the upper part of the page, switch to the region that your RDS resources belong to.

Figure 1-3 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**.

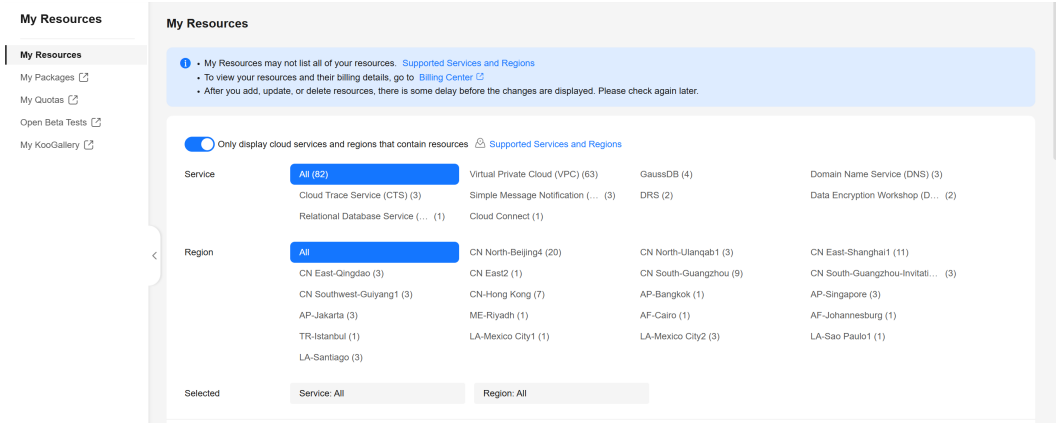
Figure 1-4 Selecting a service



Solution 2

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

Figure 1-5 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 SQL Server Storage Space?

The following logs and files occupy RDS for SQL Server storage space.

Table 3-1 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** 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 incremental backups 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 Does RDS for SQL Server Support Storage Scale-Down of DB Instances?

No. You can create a DB instance with less storage and use Data Replication Service (DRS) to synchronize your data to the instance. For details, see **From Microsoft SQL Server to Microsoft SQL Server**.

3.3 Which Items Occupy the Storage Space of My RDS for SQL Server Instance?

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

These files ensure the stability of RDS for SQL Server instances.

3.4 How Much Storage Space Is Required for DDL Operations?

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

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

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

- Method 1

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

- Method 2

  Before pushing data, set **Recovery model** of your database to **Simple**. In this model, data is not synchronized between the primary and standby instances, and no incremental backups are generated. During this period, point-in-time recovery (PITR) cannot be performed. After the data is pushed, set **Recovery**

model of your database to **Full** to resume the replication between the primary and standby instance. For details, see **How Do I Remove and Re-establish a Replication of My RDS for SQL Server Instance?**

- Solution 3

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

4 Database Connection

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

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

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

Fault Locating

1. Check whether applications are connected, optimize the connections, and release unnecessary connections.
2. Check the specifications and scale them up if needed.
3. On the Cloud Eye console, view metrics of your DB instance to identify performance issues and set alarms for metric thresholds. Cloud Eye monitors metrics of different categories, including CPU, memory, storage, and connections. For details, see the *Cloud Eye User Guide*.

Solution

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

   For details, see **Buying an RDS for SQL Server Instance and Connecting to It Using the SSMS Client**.
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 Should I Do If an ECS Cannot Connect to an RDS for SQL Server Instance Through a Private Network?

Perform the following steps to identify the problem:

Step 1 Check whether the ECS and RDS for SQL Server 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 SQL Server instance is located.

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

For details, see **Configuring Security Group Rules**.

Step 3 On the ECS, check whether the RDS for SQL Server instance can be connected.

The default port of RDS for SQL Server is **1433**.

```
telnet <IP address> {port number}
```

- If the DB instance can be connected, the network between the ECS and the DB instance is normal and no further action is required.
- If the DB instance cannot be connected, contact technical support.

----End

4.3 What Should I Do If My RDS for SQL Server Instance Fails to Be Connected Due to Database Client Problems?

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

1. ECS Security Policy

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

2. Application Configuration

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

3. Username or Password

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

   Login failed for user 'username'

NOTE

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

4.4 What Should I Do If an RDS for SQL Server Database Problem Causes a Connection Failure?

Check whether any of the following problems occurred on the RDS for SQL Server 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 SQL Server 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 SQL Server 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.

4.5 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.

4.6 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 target DB instance name to go to the **Overview** page.
   e. Under **Security Group**, click the security group name.
   f. Check whether the ECS NIC security group allows the inbound ICMP traffic.

      Table 4-1 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 technical support.

4.7 Can I Access an RDS for SQL Server 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 **Connecting to a DB 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**.

4.8 Why Did the New Password Not Take Effect After I Reset the Administrator Password of My RDS for SQL Server 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**.

4.9 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.

4.10 Will I Be Logged Out If the Connection to an RDS for SQL Server Instance Times Out?

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

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

Fault Location

- Check whether the RDS DB instance can be pinged from an ECS.

  If no, check whether the ECS and RDS DB instance are located in the same VPC and security group.

  If you intend to connect to a DB instance through a private network, the ECS and RDS DB instance must be in the same VPC and the DB instance can be accessed only through the ECS. If you intend to connect to a DB instance through a public network, they can belong to different VPCs.
- Check whether the IP address and port are correct.

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

Solution

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

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

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 name. On the **Overview** and **Backups & Restorations** pages, check connection and backup information.

Step 5 On the **Overview** page, check the administrator account.

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

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

----End

4.12 Will My Access Be Restricted by Bandwidth When I Connect to My RDS for SQL Server 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.

6 Database Permission

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

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

6.2 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@'%';

6.3 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.

6.4 How Are the Login Name Permissions of an RDS for SQL Server 2017 Enterprise Edition Primary/Standby Instance Synchronized to Its Read Replicas?

- The Login Name permissions created by the primary DB instance are automatically synchronized to read replicas once per minute. Wait for about a minute until the synchronization is complete, and you can use the Login Name permission or changing password permission on read replicas.
- You can add, delete, or modify the Login Name on read replicas because the Login Name permissions are automatically synchronized to read replicas once a minute. The additional Login Names and permissions on the read replicas are not deleted due to the time difference. You can delete them from read replicas manually.
- If a database account exists on both the primary DB instance and read replicas, the account password is synchronized to read replicas from the primary instance. Changing the Login Name permissions on read replicas will not have any effect.

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

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

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**.

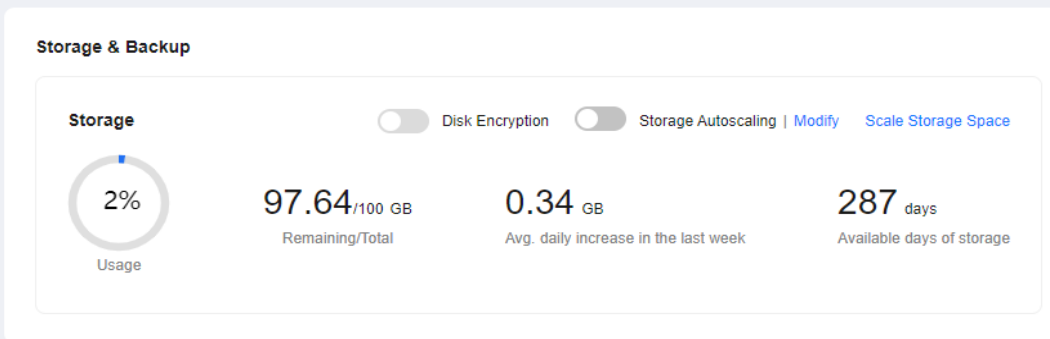
Step 2 Click  in the upper left corner and select a region.

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

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

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

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

8 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**.

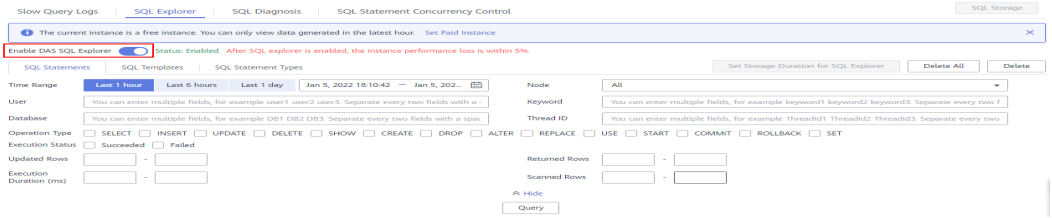
Step 6 In the navigation pane, choose **Cloud DBA (Intelligent O&M)** to go to the **Instance Overview** page.

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?

- You can check the login and logout time of an account from **audit logs**.
- To view sessions, run the **show processlist** command in the database.

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.

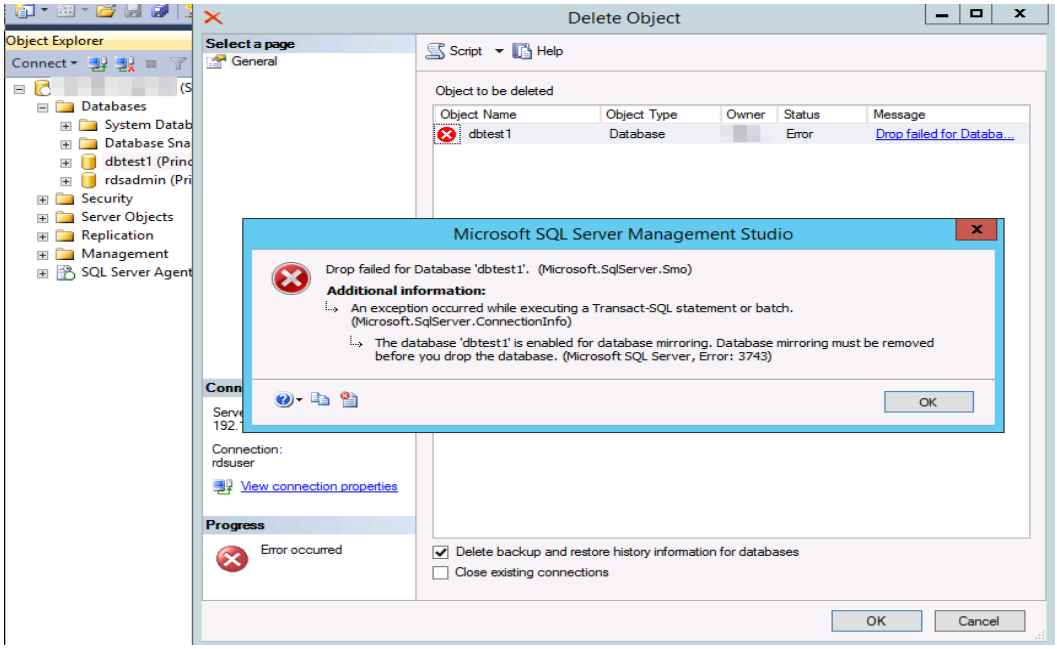
8.5 Why Is an Error Reported When I Attempt to Delete a Database from My RDS for SQL Server Primary/Standby DB Instance?

Symptom

The error shown in **Figure 8-2** is reported on SQL Server Management Studio when a database is being deleted from an RDS for SQL Server primary/standby DB instance.

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

Figure 8-2 Error



Possible Causes

The error details indicate that the RDS for SQL Server DB instance type is primary/standby and database mirroring is enabled for the standby DB instance. As a result, the database cannot be deleted.

Solution

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

Use master

go

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

GO

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

9 Backup and Restoration

9.1 How Do I View My Backup Storage Usage?

Step 1 Log in to the management console.

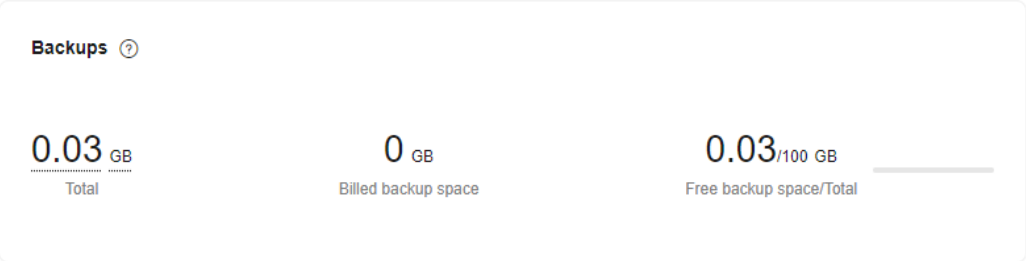
Step 2 Click in the upper left corner and select a region.

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 SQL Server 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.

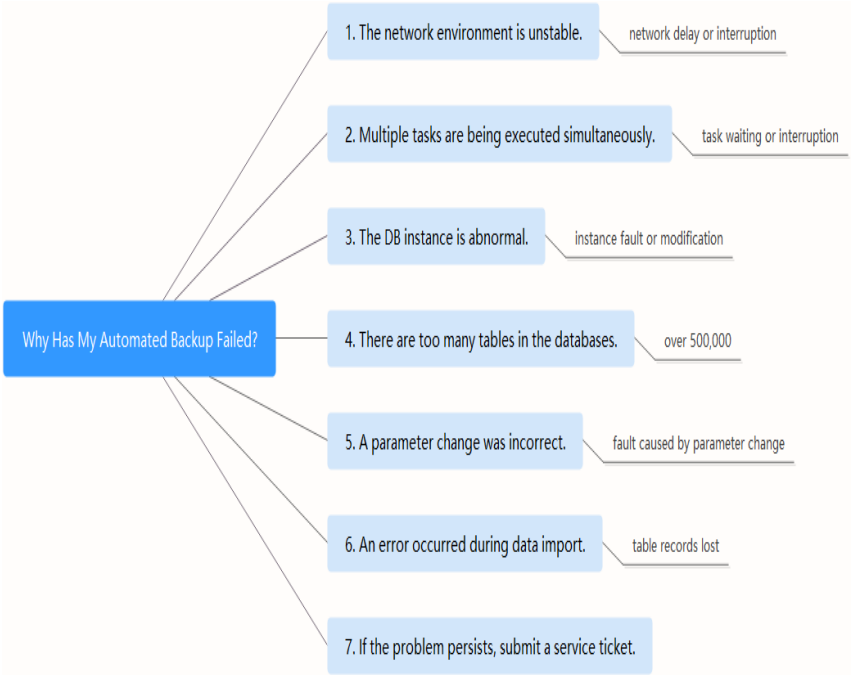
If your DB instance is frozen, no free backup space is available and the original backups generated before the instance is frozen will be billed.

- 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 Data Lost or Deleted from My RDS Instance?

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.

Review the data execution records in audit logs to check for potential misoperations.

Restore data using backup files:

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

9.5 How Long Does RDS for SQL Server 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 SQL Server Backup Space?

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

- **Automated full and incremental backups**

  Automated backups cannot be manually deleted. You need to change the backup retention period by **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**.

9.7 Can My RDS 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.

9.8 How Can I Back Up an RDS for SQL Server 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 RDS **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 SQL Server Backups to My OBS Bucket?

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

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

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

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

NOTE

To obtain the most recent backup, **submit a service ticket** to contact customer service.

9.11 What Should I Do If I Failed to Obtain a Backup Because the Name of the Bucket for Storing My RDS Backups Was Changed?

Symptom

Due to background backup bucket switchovers, new backups generated for RDS DB instances may use a different backup bucket from the previous one. If you use the function of adding an external bucket or a similar function and access a backup using the bucket name, the backup may fail to be obtained. In this case, perform the following steps to check whether the bucket name needs to be updated.

Solution

1. Use either of the following methods to query the name of the bucket where the target backup is stored:

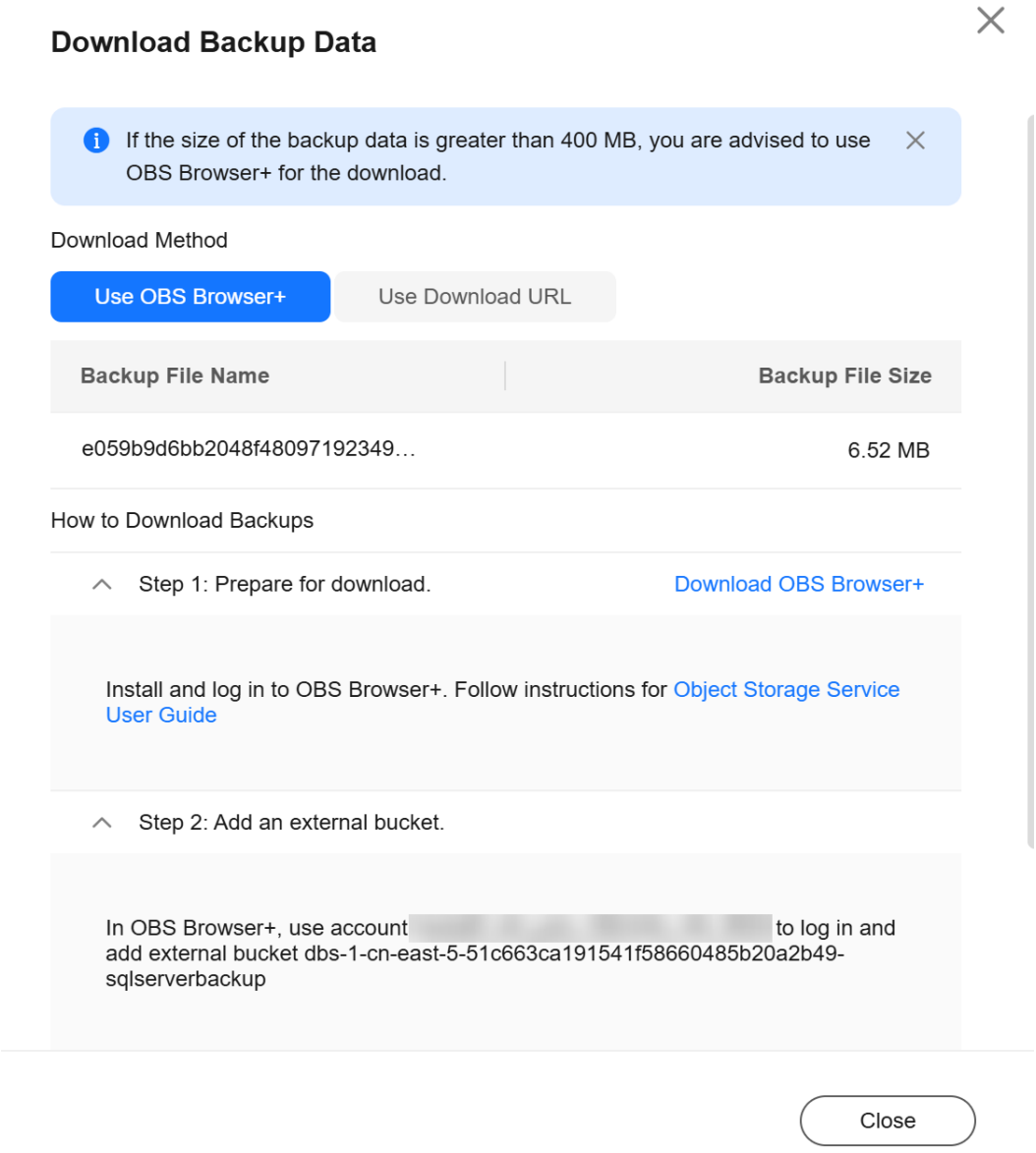
   Method 1: Query the bucket name on the console.

   a. On the **Backups** page of the RDS console, locate the backup and click **Download** in the **Operation** column.

   b. In the displayed dialog box, select **Use OBS Browser+** for **Download Method**.

   c. Obtain the bucket name in Step 2 on the download guide page. For more operations, see **Downloading a Full Backup File**.

Figure 9-3 Checking the bucket name



Method 2: Query the bucket name using an API.

Query the link for downloading a full or incremental backup based on the backup ID by calling the API for **obtaining the link for downloading a backup**. The value of **bucket** in the response is the name of the bucket where the backup is stored.

NOTE

The backup ID can be obtained from the console or by calling the API for **obtaining backups**.

2. Change the bucket name.

   Compare the bucket name obtained in the previous step with the bucket name you used for adding an external bucket or similar functions. If they are different, the backup has been stored in a new backup bucket. Use the new

bucket name and add the new bucket. Then, you can access the backup in the new bucket.

NOTE

Historical backups are still stored in the original backup bucket and will not be migrated to the new backup bucket.

10 Read Replicas and Read/Write Splitting

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

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

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

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

11 Database Monitoring

11.1 Which RDS for SQL Server 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 **What Should I Do If an RDS DB Instance Is Abnormal Due to Full Storage Space?**

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

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

On the **Instances** page of the RDS console, locate the target DB instance and click **View Metrics** in the **Operation** column. On the displayed Cloud Eye console, you can view the memory usage metric.

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 SQL Server Instances Still Available During Storage Scale-up or Instance Class Change?

Currently, you can scale up storage space or change the vCPUs and memory of RDS for SQL Server instances.

- When storage space is being scaled up, RDS for SQL Server 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 SQL Server Instance**
- **Changing the Instance Class of an RDS for SQL Server Instance**

12.2 Why Does My RDS for SQL Server 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 SQL Server 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 SQL Server Instance?

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

13.3 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**.

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

- A database-level collation can be specified during database creation. If it is not specified, an instance-level collation is automatically used. You can change the database-level collation as user **rdsuser** at any time. You are advised to change the collation on the DAS console.
  a. **Log in to the management console**.
  b. Click  in the upper left corner and select a region.
  c. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
  d. On the **Instances** page, locate the DB instance and click **Log In** in the **Operation** column.
     Alternatively, click the DB instance name on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner.
  e. Enter the username and password and click **Log In**.
  f. Select the target database and choose **SQL Operations** > **SQL Query**. In the displayed SQL window, run required commands.
     (In this example, the collation of the **test** database is set to simplified Chinese.)

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


14 Log Management

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

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

Step 2 Run the following statement to query error logs:

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

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

Example:

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

Figure 14-1 shows the query results.

Figure 14-1 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

15 Network Security

15.1 How Can Secure Data Transmission Be Ensured When I Access an RDS for SQL Server Instance 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.

15.2 How Can I Prevent Untrusted Source IP Addresses from Accessing RDS for SQL Server?

- 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 SQL Server 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 SQL Server instance 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 deleted. In this case, you can restrict the source connections and change the database username and password to prevent further damage.

  NOTE

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

15.3 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.

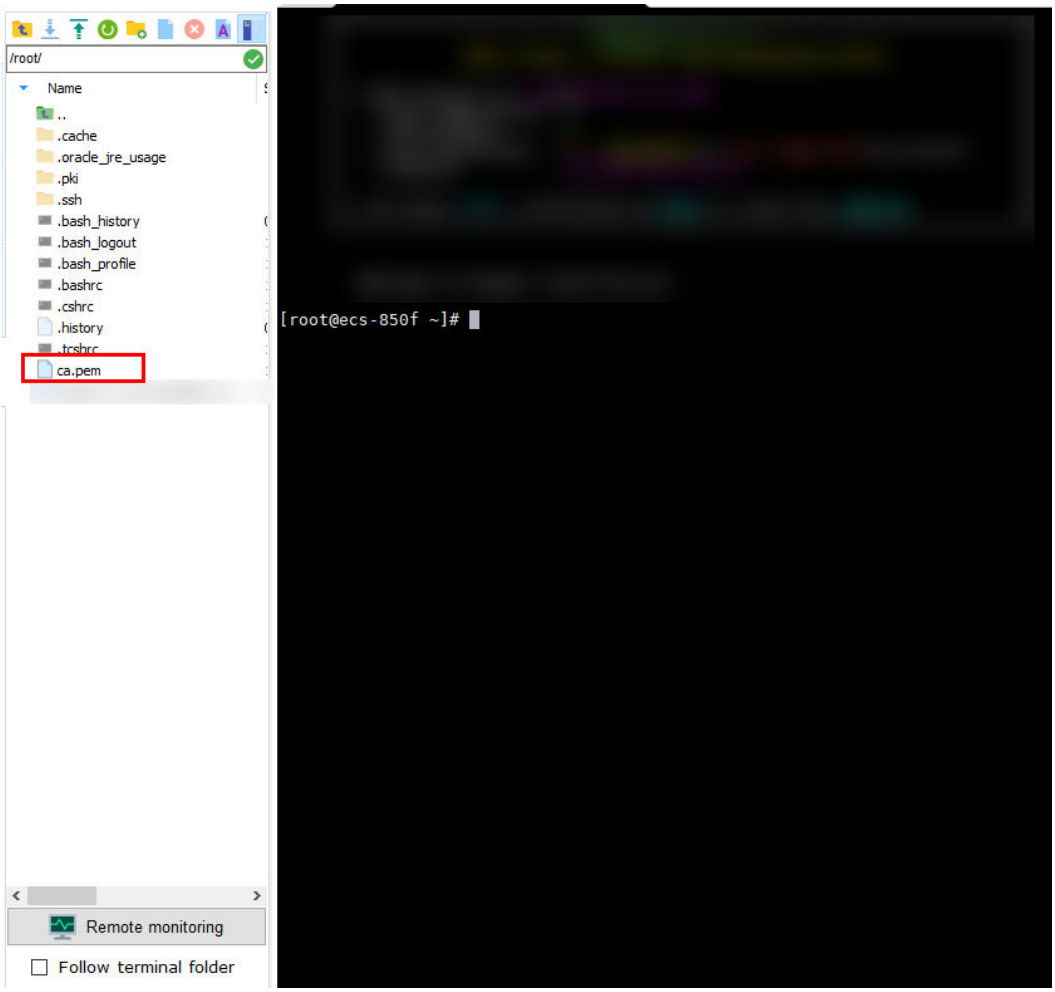
12. Click **Next**.
13. Click **Finish**.
14. Click **OK** to complete the import of the root certificate.

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 15-1 Importing a certificate



15.4 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, the system 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.

15.5 After My RDS for SQL Server 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?**

16 Version Upgrade

16.1 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.
- On the DAS console, perform the following steps to view the version of the target DB instance:
  a. Log in to the target DB instance.
  b. On the top menu bar, choose **SQL Operations** > **SQL Query**.
  c. Run **select @@version;** to view the version of the DB instance.

17 Developer-Related APIs and SDKs for RDS

Table 17-1 RDS APIs and SDKs

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

