GaussDB

FAQs

Issue   01
Date   2024-07-09

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 About GaussDB

1.1 What Should I Pay Attention to When Using GaussDB?

1. DB instance 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 OBS and the ECS used by GaussDB are invisible to you. They are visible only in the GaussDB instance management system.

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

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

   a. The CPU, IOPS, and storage space are abundant for the GaussDB instances. If any of these becomes insufficient, you will have to change the CPU/memory specifications or scale up the storage.

   b. The performance of the GaussDB instance is adequate, a large number of slow SQL queries exist, SQL statements need to be optimized, or if any indexes are redundant or missing.

1.2 What Is the Availability of GaussDB Instances?

Formula for the GaussDB instance availability:

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

1.3 Will My GaussDB Instances Be Affected by Other Users' Instances?

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

1.4 What Can I Do About Slow Responses of Websites When They Use GaussDB?

To solve this problem:

- You can check the performance of GaussDB on the management console.
- Compare the database connection status of local databases and GaussDB instances. This problem depends on web applications.

1.5 Can Multiple ECSs Connect to the Same GaussDB Instance?

Within the limits of database capability, multiple ECSs can connect to the same GaussDB instance.

1.6 Can I Encrypt the Disk After Purchasing a GaussDB Instance?

You can enable disk encryption when purchasing a GaussDB instance. For details, see **Buying a DB Instance**.

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

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

- Restore instance backup to a new instance and enable disk encryption for the new instance.
- Use the Data Replication Service (DRS) migration function to migrate instance data to other encrypted instances.

1.7 Will Backups Be Encrypted After Disk Encryption Is Enabled for My GaussDB 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 instance backup data to a new instance**
> - If both disk encryption and backup data encryption are enabled, data cannot be restored.

1.8 Will Different GaussDB Instances Share CPU and Memory Resources?

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

1.9 How Many Databases Can Run on a GaussDB Instance?

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

If there are enough CPU, memory, and storage resources, there are no limitations to the number of databases running on a DB instance.

1.10 What Is the Relationship Between GaussDB and PostgreSQL?

Based on the Postgres-XC architecture of open-source PostgreSQL 9.2, the earliest GaussDB kernel developed a multi-CN architecture, on which some major features, such as distributed execution framework (stream operators) and vectorized engine, are provided. Currently, GaussDB only uses standard APIs and common functions of PostgreSQL. It has developed its own ecosystem, architecture, and key technologies. Its centralized instances are open-source, and the storage engine and optimizer have been rearchitected. The differences between GaussDB and PostgreSQL are as follows:

- PostgreSQL uses a process model, and GaussDB uses a thread pool model.

- PostgreSQL supports only row-store. GaussDB supports row-store, column-store, and Ustore.

- PostgreSQL supports only centralized deployment. GaussDB supports both centralized and distributed deployment.

- Compared with PostgreSQL, GaussDB has many unique features, such as dynamic masking, full encryption, anti-tampering, GTM-Lite mode, NUMA-aware architecture, and geo-redundant and intra-city dual-cluster DR solutions.

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

Will Pay-per-Use Instances Be Charged When They Are Not Used?

Yes. The pay-per-use billing mode is a postpaid mode in which your DB instance will be billed based on the usage duration. The billing starts from the time when your instance is purchased to the time when it is deleted.

Why Are My Resources Released?

If your subscriptions have expired but not been renewed, or you are in arrears due to insufficient balance, your resources enter a grace period. If you still do not complete the payment or renewal after the grace period expires, you will enter a retention period. During the retention period, the resources are not available. 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 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 instance is frozen due to arrears, you need to unfreeze the instance first.

How Do I Unfreeze My Resources?

Frozen due to arrears: You can renew your resources or top up your account. Instances frozen due to arrears can be renewed, released, or deleted. Yearly/Monthly instances that have expired cannot be unsubscribed from, while those that have not expired can be unsubscribed from.

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 instance is frozen, it cannot be connected.
  - 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, GaussDB determines whether to **move the instance to the recycle bin** based on the recycling policy you specified.

How Do I Renew My Resources?

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

Can My Resources Be Recovered After Being Released? /Can I Retrieve an Incorrect Unsubscription?

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.

When you unsubscribe from an instance, confirm the instance information carefully. If you have unsubscribed from a DB instance by mistake, you are advised to purchase a new one.

How Do I Delete My Instance?

- For pay-per-use instances, see **Deleting a DB Instance**.
- For yearly/monthly instances, see **Unsubscribing a Yearly/Monthly DB Instance**.

3 Resource and Disk Management

3.1 Can I Scale Down the Storage Space of My GaussDB Instances?

No.

3.2 Which Items Occupy the Storage Space of My GaussDB Instances?

Both your common data (excluding backup data) and the data required for the operation of your DB instances (such as system database data, rollback logs, redo logs, and indexes) occupy the storage space on your purchased GaussDB instances. The storage space includes the file system overhead required for inodes, reserved blocks, and database operations. It also includes the log files generated by the GaussDB database.

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 the storage space is at least twice the tablespace size plus 10 GB. For example, if your tablespace is 500 GB, ensure that the storage space is at least 1,010 GB (500 GB x 2 + 10 GB).

4 Database Connections

4.1 Can I Connect to GaussDB over SSL?

Yes, GaussDB is compatible with SSL. For details, see **SSL Connection**.

4.2 What Should I Do If I Can't Connect to My GaussDB Instance?

Problem Analysis

Locate the fault by considering the following aspects:

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

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

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

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

    Check whether the following parameters are configured correctly: connection address, port number, username, and password.

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

    For a private network connection:
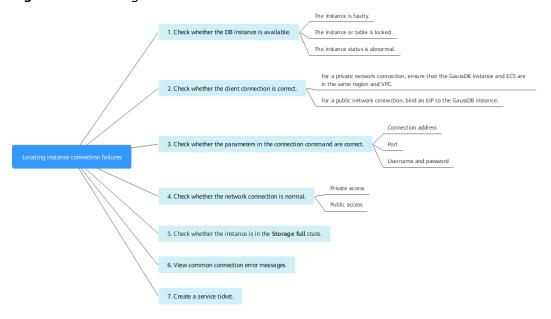
    a. Ensure that the ECS and GaussDB instance are in the same region and VPC.

    b. Check security group rules.

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

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

For a public network connection:

a.   Check security group rules.

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

b.   Check network ACL rules.

c.   Ping the ECS to the instance in the same region.

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

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

6.   **View common connection error messages.**

Find corresponding solutions based on connection error messages.

Troubleshooting Process

Figure 4-1 Locating instance connection failures

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

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

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

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

Figure 4-2 Checking DB instance status

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

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

Table 4-1 Connection methods

Connect Through	Description	Example
Private network	A private IP address is provided by default. If your applications are deployed on an ECS that is in the same region and VPC as your DB instance, use a private IP address to connect to the ECS and the DB instance.	For example, to connect to the **postgres** database, run the following command: **gsql -d** *postgres* **-h** *10.0.0.0* **-U** *root* **-p** *8000* NOTE *postgres* indicates the database name, *10.0.0.0* indicates the CN IP address of a distributed DB instance or the primary DN IP address of a primary/standby DB instance, *root* is the username for logging in to the database, and *8000* is the port number of the CN.
Public network	If you cannot access a GaussDB instance over a private IP address, bind an EIP to the GaussDB instance and connect it to the ECS (or a host from the public network) over the EIP.	For example, to connect to the **postgres** database, run the following command: **gsql -d** *postgres* **-h** *10.0.0.0* **-U** *root* **-p** *8000* NOTE **postgres** is the name of the database to be connected; **10.0.0.0** is the EIP bound to the DB instance; **root** is the username for logging in to the database; **8000** is the port number of the DB instance.

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

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

Connection through a private network

a. Connection address

Private IP Address in the **Connection Information** area of the **Basic Information** page of the target instance

Figure 4-3 Private IP address

b. Database port

Database Port of the target instance

c. Username and password
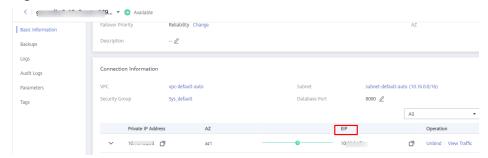
User **root** and its password

Connection through a public network

a. Connection address

EIP in the **Connection Information** area of the **Basic Information** page of the target instance

Figure 4-4 EIP

b. Database port

Database Port of the target instance

c. Username and password

User **root** and its password

4. **Check the network connection.**

Private network connection

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

- The ECSs and instances in different regions cannot communicate with each other. To reduce network latency, deploy your DB instance in the region nearest to your workloads.

- If the ECS and your instance are deployed in different VPC, see **What Should I Do If the ECS and GaussDB Instance Are Deployed in Different VPCs and They Cannot Communicate with Each Other?**

Figure 4-5 Viewing the VPC of an ECS
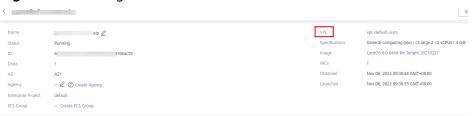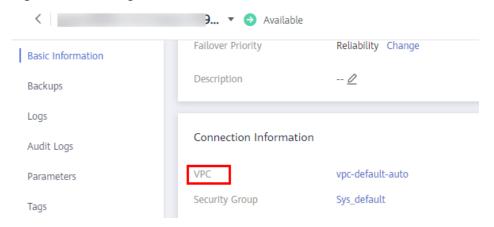
Figure 4-6 Viewing the VPC of a GaussDB instance

b. Check security group rules.

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

Figure 4-7 ECS security group

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

Figure 4-8 GaussDB security group

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

telnet *<IP address> <port number>*

- If the ECS can connect to the DB instance, the network between them is normal.

- If the ECS cannot connect to the DB instance, choose **Service Tickets > Create Service Ticket** in the upper right corner of the management console to submit a service ticket for help.

Public network connection

a. Check security group rules.

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

  Figure 4-9 ECS security group

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

  Figure 4-10 GaussDB security group

b. Check network ACL rules.

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

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

iii. Check whether the network ACL is enabled.

  If it is enabled, **add an ICMP rule to allow traffic**.

The default network ACL rule denies all inbound and outbound packets. This default rule is still applied even if the network ACL is disabled.

c. Ping the ECS to the instance in the same region.

If you cannot ping the EIP on the original ECS, select another ECS in the same region and ping the EIP again. If the ping is successful, the virtual network is functional. In this case, choose **Service Tickets > Create Service Ticket** in the upper right corner of the management console to submit a service ticket for help.
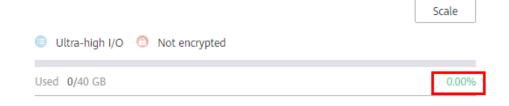
5. **Check whether the DB instance is in the Storage full state.**

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

   – On the management console

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

      Figure 4-11 Checking the disk usage

   – On Cloud Eye

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

      Possible cause: If the kernel system detects that the disk usage exceeds the specified threshold, the instance is set to read-only and no data can be written to the DB instance.

      Solution: See **Scaling Up Storage Space**.

6. **View common connection error messages.**

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

   gsql: ERROR: dn_6001_6002_6003: Invalid username/password,login denied.

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

7. If the problem persists, **create a service ticket** to contact customer service for help.

4.3 Can an External Server Access GaussDB Instances?

DB Instance Bound with an EIP

If the GaussDB instance is publicly accessible, you can access the DB instance over public networks.

DB Instance Not Bound with an EIP

- Enable a VPN in a VPC and use the VPN to connect to the GaussDB instance.

- Create a GaussDB instance and an ECS in the same VPC and access the GaussDB instance through the ECS.

For details, see **Using gsql to Connect to an Instance**.

4.4 How Can I Create and Connect to an ECS?

1. For details about how to create an ECS, see *Elastic Cloud Server User Guide*.
   - If you connect to a GaussDB instance through a private network, the ECS must be in the same VPC as the instance. If you connect to a GaussDB instance through a public network, the ECS and the instance can be in different VPCs.
   - Configure a security group to allow the ECS to access the GaussDB instance over a private network.
2. For details about how to connect to the ECS, see *Elastic Cloud Server User Guide*.

4.5 What Should I Do If an ECS Cannot Connect to a GaussDB Instance Through a Private Network?

Perform the following steps to locate the problem:

Step 1 Check whether the ECS and the GaussDB instance are in the same VPC.

- If yes, go to **Step 2**.
- If they are in different VPCs, create an ECS instance in the same VPC as the GaussDB instance.

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

For details, see **Configuring Security Group Rules**. Then, go to **Step 3**.

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

The default port number of a GaussDB instance is 8000.

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

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

----End

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

Identify a GaussDB connection failure caused by a client problem from the following aspects:

1. ECS security policy

On a Windows server, check whether the GaussDB instance port is enabled in the Windows security policy. On a Linux server, run **iptables** to check whether the instance port is enabled in firewall settings.

2. Incorrect application configuration

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

3. Incorrect username or password

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

   gsql: ERROR: dn_6001_6002_6003: Invalid username/password,login denied.

> 📖 **NOTE**
>
> If the problem persists, contact technical support.

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

Check whether any of the following problems occur on the GaussDB instance:

1. The GaussDB instance is not properly connected.

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

2. The maximum number of connections has been reached.

   Solution: Check whether the CPU usage and the number of current connections are normal by using GaussDB resource monitoring. If either of them reaches the maximum, reboot, disconnect, or change the CPU and memory of the GaussDB instance.

3. The DB instance is abnormal. For example, the instance is suspended during reboot, the GaussDB system is faulty, or the instance or table is locked.

   Solution: Reboot the instance to see if the problem is resolved. If the problem persists, contact technical support.

4.8 How Do My Applications Access a GaussDB Instance in a VPC?

Ensure that the ECS where your applications are located and the target GaussDB instance are in the same VPC. If they are in different VPCs, modify the VPC route table and network ACL to ensure the ECS can access the GaussDB instance.

4.9 Do Applications Need to Support Reconnecting to the GaussDB 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.
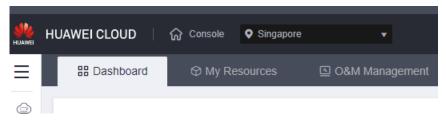
4.10 Why Can't I Ping My EIP After It Is Bound to an Instance?

Fault Locating

1. Check security group rules.
2. Check network ACL rules.
3. Ping the ECS to the instance in the same region.

Solution

1. Check security group rules.

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

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

   c. Click [image] in the upper left corner of the page and choose **Databases** > **GaussDB**.

   d. On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.

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

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

Table 4-2 Security group rules

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

2. Check network ACL rules.

   a. Check whether the network ACL is enabled or disabled.

   b. Check whether the NIC to which the EIP bound belongs to the subnet associated with the network ACL.

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

   📖 **NOTE**

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

3. Ping the ECS to the instance in the same region.

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

4.11 Can I Access a GaussDB Instance Over an Intranet Connection Across Regions?

By default, 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, or Virtual Private Network (VPN) to connect to instances across regions.

● You can access GaussDB instances across regions using EIP. For details, see **Using gsql to Connect to an Instance**.

● Cloud Connect allows you to connect two VPCs in the same account or in different accounts even if they are in different regions. For details, see **Connecting VPCs in 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 Internet connections. For details, see **Connecting to a VPC Through a VPN**.

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

No.

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

Possible Causes

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

Locating Method

Check whether the DB instance is restored after the administrator password is reset.

Solution

On the GaussDB console, reset the administrator password again. For details, see **Resetting the Administrator Password**.

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

1. Change the VPC hosting the ECS to the same as that hosting the GaussDB instance.
2. Create a VPC peering connection to set up a network connection between the two VPCs.

5 **Database Permissions**

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

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

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

6 Database Storage

6.1 What Types of Storage Does GaussDB Use?

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

GaussDB backup files are stored in OBS and do not occupy your purchased storage space. For details on the GaussDB instance storage configuration, see the *Object Storage Service User Guide*.

6.2 What Should I Do If My Data Exceeds the Available Storage of a GaussDB Instance?

Symptom

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

Possible Causes

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

Solution

1. For insufficient storage caused by increased workload data, **scale up storage space**.
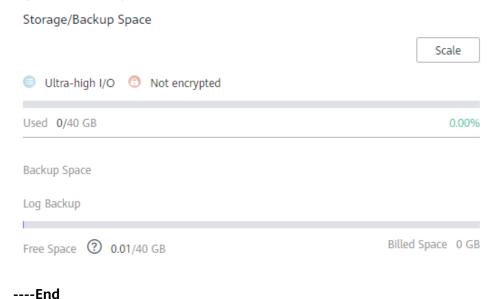
   If the original storage has reached the maximum, **upgrade the instance specifications** first.

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

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

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

   To delete data of an entire table, use the **DROP** or **TRUNCATE** statement. To delete part of table data, use the **DELETE** statement.

3. If log files occupy too much storage, clear log files to release storage space.

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

6.3 How Do I View the Storage Usage of My GaussDB Instance?

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

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

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

Step 4 On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.

Step 5 On the **Basic Information** page, view the storage type and usage in the **Storage/Backup Space** area.

Figure 6-1 Storage space

----End

7 Database Usage

7.1 How Do I Use DAS to Query SQL Statements?

DAS is a professional database management tool with a graphical user interface. You can enable SQL Explorer to query related SQL statements.
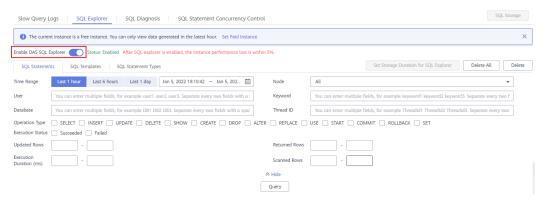
Step 1 **Log in to the management console**.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Data Admin Service** The DAS console is displayed.

Step 4 In the navigation pane, choose **Intelligent O&M** > **Instance List** to go to the **Instance Overview** page.

Step 5 On the **Instance Overview** page, select **GaussDB Instances** in the filter area.

Figure 7-1 Instance overview

| Enable Intelligent O&M Quota | Configure Concurrency Control Rules of SQL Statements | | GaussDB Instanc... ∨ | GaussDB | ∨ |

Instance Overview

| Total Instances | Instances Without Login Accounts | Instances with Slow Query Log Disabled | Instances with SQL Explorer Disabled |
| 41 Set Login Account | 41 Set Login Account | 41 | 41 |

Step 6 Locate the instance you want to view and click **Details**.

Step 7 Choose **SQL** > **SQL Explorer** to view full SQL query details of the instance.

Step 8 On the **SQL Statements** tab, toggle on **Enable DAS SQL Explorer**. Query the SQL statements executed by the current instance by time range, user, keyword, operation type, database, or other filters.

Figure 7-2 Enabling SQL Explorer

Step 9 Filter operation types by referring to **Table 7-1** and click **Export** to export the corresponding SQL statements.

Table 7-1 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**.

A maximum of 100,000 records can be exported.

----End

7.2 What Should I Do If Garbled Characters Are Displayed After SQL Query Results Are Exported to an Excel File?
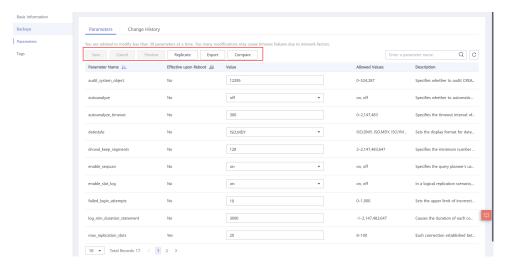
The default encoding of exported data UTF-8. You need to convert the default encoding to Unicode in the exported Excel file.

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

You can restore the deleted **root** account by resetting its password. For details, see **Resetting the Administrator Password**.

7.4 What Do I Do If a DB Instance Is Locked?
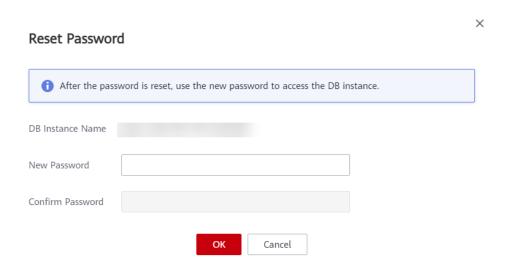
Step 1 On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.

Step 2 In the navigation pane on the left, choose **Parameters**.

Step 3 Set **password_lock_time** to **0** and **failed_login_attempts** to **0** to unlock the database.

For database security purposes, change the parameter values to the default values after the password is reset.

Step 4 In the **DB Information** area, click **Reset Password** next to the **Administrator** field.

Step 5 Enter a new password and confirm the password.

Step 6 Change the values of **password_lock_time** and **failed_login_attempts** to the default values.

----End

7.5 What Do I Do If Replay Speed of Standby Nodes Cannot Catch Up with Write Speed of Primary Nodes?

Symptom

When workloads on a DB instance are heavy, the playback speed of standby nodes cannot catch up with write speed of primary nodes. After the system runs for a long time, logs are accumulated on the standby nodes. If a primary node is faulty, data restoration takes a long time and the database is unavailable, severely affecting system availability.

Solution

GaussDB provides ultimate RTO to minimize the data recovery time after a primary node is faulty and improve availability.

To use ultimate RTO, submit an application by choosing **Service Tickets > Create Service Ticket** in the upper right corner of the console.

Precautions

- Ultimate RTO focuses only on whether the RTO of standby nodes meets the requirements.
- Enabling ultimate RTO consumes CPU and memory resources of standby nodes.
- In 1.4 and earlier versions, flow control takes effect when ultimate RTO is enabled.
- Standby nodes do not support read operations after ultimate RTO is enabled. If you send read requests to a standby node, the standby node may fail to return the results.

8 Backup and Restoration

8.1 Does GaussDB Support Both Cold Backup and Hot Backup?

No. Currently, GaussDB supports hot backup only.

8.2 How Long Does GaussDB Store Backup Data?

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

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

8.3 How Do I Clear GaussDB Backup Space?

- **Automated full and incremental backups**

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

- **Manual full backups**

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

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

A backup window is a user-specified time segment during which backup of GaussDB instances is performed. With these periodic data backups, GaussDB 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 GaussDB instance except rebooting it on the console.
- When starting a full backup task, GaussDB first tests connectivity to your instance. If either of the following conditions is met, the test fails and a retry is performed. If the retry fails, the backup task fails.
  - DDL operations are being performed on the DB instance.
  - The backup lock fails to be obtained from the DB instance.

8.5 How Is GaussDB Backup Data Billed?

All the GaussDB backups are stored on OBS without occupying the storage of your DB instances. GaussDB provides free backup space of the same size as your purchased storage. If the backup storage usage exceeds 100% of your provisioned database storage, tiered pricing starts. For details, see **Billing**.

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

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

8.6 How Do I View My Backup Storage Usage?

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

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

Step 3 Click ≡ in the upper left corner of the page and choose **Databases** > **GaussDB**.

Step 4 On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.

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

Figure 8-1 Backup space

----**End**

8.7 How Can I Back Up a GaussDB Database to an ECS?

You can back up data to an ECS in 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 database backup data on an ECS. However, you are advised not to use an ECS as the database backup space.

You are advised to use the **automated backup** and **manual backup** functions of GaussDB to store backups to a professional storage object, such as the OBS, to ensure high data reliability and service assurance.

8.8 Will Backups Be Retained After My GaussDB Instance Is Deleted?

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

Automated backups and their related files are automatically deleted.

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

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

8.10 Why Does Automated Backup Fail?

Automated backups may fail for the following reasons:

- The network environment may be unstable due to problems such as network delay or interruptions.

  If the system 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 the system 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 the system 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 there are more than 500,000 tables, the backup will fail.

- A parameter change was incorrect.

  If your 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 instance.

- If the problem persists, contact customer service.

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

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

Restore data using backup files:

- Use the GaussDB restoration function to restore data.
- Import backup data from the ECS to GaussDB.

8.12 How Do I Restore a Local Database Backup to GaussDB?

You can use the migration function of Data Replication Service (DRS) to restore a local database backup to a cloud database.

For more backup and restoration details, see **Data Restoration**.

8.13 Does GaussDB Support Table PITR?

No, GaussDB does not support table-level restoration.

You can use an automated or manual backup to restore data to the status when the backup was created. The restoration is at the instance level. For details, see **Data Restoration**.

8.14 Can I Dump Backup Files to My OBS Buckets?

No. Backup files 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+.

8.15 Does GaussDB Support Table-Level Backup to a Specified OBS Bucket?

No, GaussDB does not support table-level backup to a specified OBS bucket.

GaussDB supports full backups and incremental backups. Both of them are stored in OBS.

8.16 Can I Delete the GaussDB Backup Policy?

Sorry, you cannot delete the GaussDB backup policy.

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

9 Database Monitoring

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

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

You can configure the system to report alarms as needed and take measures to clear any reported alarms.

Configuration examples:

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

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

- Configure the system to report alarms to Cloud Eye if its storage space usage 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 CPU or memory by changing the DB instance specifications.

  For details, see **Changing CPU and Memory Specifications**.

- If a storage space usage alarm is reported, you can scale up the storage space.

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

9.2 How Can I Calculate the Memory Usage of a GaussDB Instance?

The formula for calculating the memory usage is as follows:

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

10 Scaling and Specification Change

10.1 Are My GaussDB Instances Still Available During Storage Scale-up and Instance Specification Change?

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

- When storage space scale-up, GaussDB instances are available and services are not interrupted. However, you cannot delete or reboot the instances that are being scaled.

- During CPU and memory specification change, the network is intermittently disconnected for one or two times in seconds. A failover may occur during this period and services may be briefly interrupted.

  For DB instances earlier than 3.100, the instances will be rebooted after their specifications are changed. During the reboot, services are unavailable. For instances of version 3.100 or later, no reboot is required, which greatly reduces the impact of intermittent disconnections. To prevent service interruption, perform the operation during off-peak hours. Rebooting a DB instance will clear the cached memory in it. You are advised to reboot it during off-peak hours.

10.2 Can I Change the VPC to Which My GaussDB Instance Belongs?

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

However, you can change a VPC by restoring the full backup of your instance to the VPC you want to use. For details, see **Data Restoration**.

11 Database Parameter Modification

11.1 How Can I Change the Time Zone?

You can set the time zone only on the GaussDB console. To change the time zone for an instance, perform the following steps:

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

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

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

Step 4 On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.

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

Step 6 Search for the **timezone** parameter 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

11.2 How Can I Configure a Password Expiration Policy?

You can set the global variable **password_effect_time** to control the default validity period of a user password.

You can change the value of the **password_effect_time** parameter on the GaussDB console. For operation details, see **Modifying Parameters in a Parameter Template**.

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

12 Log Management

12.1 How Do I View All SQL Logs Executed by GaussDB?

You can use the visualized database management service Data Admin Service (DAS) to quickly search for target SQL execution records.

Procedure

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

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

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

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

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

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

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

Figure 12-1 SQL History

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

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

----End

12.2 How Do I View Deadlock Logs of GaussDB?

Database deadlock logs are recorded in error logs. If **Error Log Collection** is enabled, you can download error logs and quickly locate deadlock-related records by searching for keywords **Lock wait timeout** in the logs.

Procedure

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

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

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

Step 4 On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.

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

Step 6 On the **Error Logs** tab, select a specified time period and click **Download** in the **Operation** column to download the error log file.

Step 7 Open the error log file, and search for **Lock wait timeout** to quickly locate deadlock errors.

----End

13 Network Security

13.1 What Security Protection Policies Does GaussDB Have?

Networking

- GaussDB allows you to run your instances in a VPC, ensuring that the DB instances are isolated from other services.
- GaussDB uses security groups to ensure that only trusted sources can access your DB instances.
- GaussDB supports SSL connections to encrypt data during transmission.

Management

You can use the Identity and Access Management (IAM) service to manage GaussDB permissions.

13.2 How Can I Prevent Untrusted Source IP Addresses from Accessing GaussDB Instances?

- 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 GaussDB security group to ensure that only trusted source IP addresses can access your DB instances.
- To prevent your database password from being cracked, set a strong password and periodically change it.

13.3 How Do I Configure a Security Group to Enable Access to GaussDB Instances?

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

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

    - ECS: The default security group rule allows all outbound data packets. In this case, you do not need to configure a security rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an outbound rule for the ECS to allow all outbound packets.

- When you attempt to connect to a GaussDB instance through an EIP, you need to configure an **inbound rule** for the security group associated with the DB instance.

13.4 How Can I Import the Root Certificate to a Windows or Linux Server?

Importing the Root Certificate to a Windows Server

1. Press **Win+R** to open the **Run** dialog box, enter **MMC**, and press **Enter**.
2. On the displayed console, choose **File** > **Add/Remove Snap-in**.
3. In the **Available snap-ins** pane to the left 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. Click **Next**.
10. Click **Browse** to change the file type to **All Files (*.*)**.
11. Locate the downloaded root certificate (a 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.

1. Click **Next**.
2. Click **Finish**.
3. Click **OK** to complete the import of the root certificate.

Importing the Root 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.

13.5 How Do I Manage and Ensure GaussDB Security?

For security reasons, do not use the username and password of your Huawei Cloud account. We recommend that you use your Huawei Cloud account to create IAM users for database user accounts. You can also use your account to create other user accounts, if necessary.

An error may occur if you do not have sufficient permissions or your account configuration is incorrect. Example:

You may have no permission to perform specific operations, such as creating a DB instance. In this case, contact your IAM administrator to grant the necessary permissions to your account.