GaussDB

FAQs

Issue 01

Date 2025-08-18

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.

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 Are There Any Special Points to Note 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. When 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.

WARNING

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. These resources are the instance specifications selected when you buy an instance.

1.9 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, 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 data masking, fully-encrypted processing, anti-tampering, GTM-Lite mode, NUMA-aware architecture, and geo-redundant and intra-city dual-cluster DR solutions.

1.10 Can Multiple Users Log In to a GaussDB 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 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**.

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

Will Pay-per-Use Instances Be Billed When Not in Use?

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?

Your instance will enter a grace period if you do not renew the subscription or your account is in arrears. 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.

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 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**.

4.2 Do Applications Need to Support Automatic Reconnections to GaussDB Databases?

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.

4.3 Why Can't I Ping My EIP After It Is Bound to a GaussDB Instance?

Troubleshooting Process

1. Check security group rules.
2. 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  in the upper left corner and select a region and project.
   c. Click  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 name in the **Security Group** field.
   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 **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. 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, **submit a service ticket** to contact technical support.

5 Database Storage

5.1 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 your instance becomes read-only, **submit a service ticket** to contact technical support to remove the read-only restriction 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.

5.2 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 usage in the **Storage/Backup Space** area.

----End

6 Database Usage

6.1 How Do I Use DAS to Query SQL Statements Executed in GaussDB?

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.

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.

Step 9 Filter operation types by referring to **Table 6-1** and click **Export** to export the corresponding SQL statements.

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.

Table 6-1 Common SQL statement types

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

----End

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

The default encoding of exported data UTF-8. You need to convert the default encoding to Unicode in the exported Excel file.

6.3 What Do I Do If the root Account of My GaussDB 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 **DB Information** area, click **Reset Password** next to the **Administrator** field.

Step 3 Enter a new password and confirm the password.

----End

6.4 Why Did the New Password Not Take Effect After I Reset the Administrator Password of a GaussDB Instance?

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**.

6.5 What Do I Do If Replay Speed of Standby DNs Cannot Catch Up with Write Speed of Primary DN?

Symptom

When workloads on a DB instance are heavy, the replay speed of standby DNs cannot catch up with the write speed of the primary DN. After the system runs for a long time, logs are accumulated on the standby DNs. If the primary DN 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 DN is faulty and improve availability.

To enable ultimate RTO, **submit a service ticket**.

Precautions

- Ultimate RTO focuses only on whether the RTO of the standby DN meets the requirements. Ultimate RTO has no inherent flow control and uses the **recovery_time_target** parameter for flow control instead.
- Ultimate RTO uses multi-page redo threads to accelerate the replay progress. When the replay on the standby DN catches up with that on the primary DN and the standby DN is unloaded, the CPU usage of a single page redo thread is about 15% (the actual value depends on the hardware and parameter configuration). Total CPU usage of the replay on the standby DN = CPU usage of a single page redo thread x Number of page redo threads. Because more threads are started, the CPU and memory consumption is higher than that of parallel replay and serial replay.
- Ultimate RTO supports read on standby nodes. Because historical data pages are read, the query performance on the standby DNs is worse than that on the primary DN and worse than that of read on standby nodes during parallel redo. However, query blocking is alleviated.
- The replay speed of DDL logs is much slower than that of page modification logs. Frequent DDL operations may increase the primary/standby latency.
- When the I/O and CPU usage of a node is too high (it is recommended that the I/O and CPU usage be less than or equal to 70%), the performance of replay and read on standby nodes deteriorates significantly.

6.6 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**.

7 Backup and Restoration

7.1 How Long Does GaussDB Store Backup Data?

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

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

7.2 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**.

  After the manual backups are deleted, you can go to the **Instances** page and click the name of the target instance to go to the **Basic Information** page. In the **Storage/Backup Space** area, you can check the backup space usage.

7.3 Can My GaussDB 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. However, you cannot perform operations such as 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.

7.4 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**.

CAUTION

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.

7.5 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.

7.6 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.

7.7 Why Does Automated Backup for a GaussDB Instance Fail?

The possible causes and solutions for automatic backup failures are as follows:

- 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 an automated backup when the instance status becomes available. Alternatively, you can perform a manual backup immediately.
- 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, **submit a service ticket** to contact customer service.

7.8 Why Is Data Table Lost or Data Deleted from My GaussDB Instance?

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.

7.9 Does GaussDB Support Restoring Data for Individual Tables?

No. GaussDB does not support table-level restoration.

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

7.10 How Can I Delete the GaussDB Backup Policy?

Sorry, you cannot delete the GaussDB backup policy.

When you create a GaussDB instance, the instance-level automated backup policy is enabled by default. You can modify the backup cycle and retention period on the console. For operation details, see **Configuring an Automated Backup Policy for Instances**.

8 Database Monitoring

8.1 Which Monitoring Metrics of GaussDB Instances Do I Need to Pay Most Attention To?

For a GaussDB instance, you need to pay the most attention to the CPU, memory, and storage space (disk) 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 average CPU 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 average memory 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 maximum storage usage reaches or exceeds a specific value (for example, 85%) multiple times (for example, 2 times) within a set period (for example, 5 minutes).

Measures:

- If a CPU or memory alarm is reported, you can scale up the CPU or memory by changing the DB instance specifications.
- If a storage space usage alarm is reported, you can scale up the storage space.

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

8.2 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 of a physical machine – (Available memory + Buffer memory + Cache memory))/Total memory of a physical machine

9 Scaling and Specification Change

9.1 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 V2.0-3.100, the instances will be rebooted after their specifications are changed. During the reboot, services are unavailable. For instances of version V2.0-3.100 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 Database Parameter Modification

10.1 How Can I Change the Time Zone of a GaussDB Instance?

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**.

----End

10.2 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.

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.

11 Log Management

11.1 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.

- 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 Network Security

12.1 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.

12.2 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**.

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

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

Importing the Root Certificate to 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.

