Data Admin Service

faq

Issue 01

Date 2023-12-01

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Security Declaration

Product Lifecycle

Huawei's regulations on product lifecycle are subject to the *Product End of Life Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/ecolumnsweb/en/warranty-policy

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Initial Digital Certificate

The Initial digital certificates on Huawei devices are subject to the *Rights and Responsibilities of Initial Digital Certificates on Huawei Devices.* For details about this document, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789

Huawei Enterprise End User License Agreement

This agreement is the end user license agreement between you (an individual, company, or any other entity) and Huawei for the use of the Huawei Software. Your use of the Huawei Software will be deemed as your acceptance of the terms mentioned in this agreement. For details about this agreement, visit the following web page:
https://e.huawei.com/en/about/eula

Lifecycle of Product Documentation

Huawei after-sales user documentation is subject to the *Product Documentation Lifecycle Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761

Contents

1 Product Consulting

1.1 How Is DAS Billed?

For details, see **Intelligent O&M Billing**.

1.2 Which Data Sources Does DAS Support?

Currently, DAS supports the management of MySQL, RDS for SQL Server, GeminiDB Cassandra, GaussDB, GaussDB(for MySQL), DDM, DDS, and PostgreSQL instances.

1.3 Does DAS Support Multi-Region Access?

Not yet. You must ensure that your DB instance is in the same region where you applied for the DAS service.

1.4 Where Is SQL Execution Records Saved If I Enable This Function?

SQL execution records will be saved on the management hosts of the DAS service.

1.5 What Should I Enter in the Database Column to Log In to a PostgreSQL DB Instance on the DAS Console?

Enter **postgres**.

1.6 Will I Be Changed If I Enable Collect Metadata Periodically and Show Executed SQL Statements on the Add Login Page?

Currently, these functions are free of charge.

2 Managing connections

2.1 What Should I Do If I Can't Connect to My DB Instance Due to Insufficient Permissions?

1. Error message: You do not have the required permission. The policy does not allow action das:connections:xxx.

   Error cause: Your account does not have the DAS FullAccess permission.

   Solution: Add the DAS FullAccess permission by referring to **Creating a User and Granting Permissions**.

2. Error message: You do not have the permission to perform this operation. Contact your administrator to request the required permission.

   Error cause: Your account does not have the DAS FullAccess permission.

   Solution: Add the DAS FullAccess permission by referring to **Creating a User and Granting Permissions**.

3. Error message: Your current account only has the read-only permission and cannot perform this operation. To ensure that you can use DAS smoothly, add the DAS Administrator permission.

   Error cause: Your account does not have the DAS FullAccess permission.

   Solution: Add the DAS FullAccess permission by referring to **Creating a User and Granting Permissions**.

2.2 What Should I Do If I Can't Connect to My RDS for MySQL Instance?

1. Error message: **Access denied for user 'user_name'@'100.xxx.xx.xx' (using password: YES)**

   a. Error cause: The username or password of the RDS instance is incorrect.

      Solution: Check whether the username and password are correct. If you are not sure, log in to the RDS console to reset the password.

NOTICE

Changing the password may affect services.

If the username and password are correct, log in to the database using a client or CLI tool and run **select * from mysql.user where user = 'user_name'** to view the account. Make sure that the DAS CIDR block is within the CIDR block of the user. **user_name @ %** and **user_name @100.%** are two different users whose passwords and permissions are independent. Enter the password of **user user_name @100.%**.

b. Error cause: The IP address of the DAS server is not in the whitelist of the login user.

Solution: Log in to the database using the client or CLI tool, and create a user account that can be used to access the database through DAS.

```
create user 'user_name'@'100.%' identified by 'password';
grant select on *.* to 'user_name'@'100.%';
```

NOTE

- Ensure that the IP address of the DAS server is in a CIDR block starting with 100. Add the IP address to the whitelist of the login user.
- Grant permissions to user **user_name@100.%** based on service requirements.

c. Error cause: The SSL function is not enabled on the server.

Solution: Run the following statement to check whether the user is an SSL user. If yes, enable SSL on the RDS instance details page. The user is an SSL user if the **ssl_type** field has a value.

```
select user, host, ssl_type from mysql.user where user = 'user_name';
```

2. Error message: **Trying to connect with ssl, but ssl not enabled in the server**

Error cause: The SSL function is not enabled on the server.

Solution: Run the following SQL statement to check whether the user is an SSL user. If yes, enable SSL on the RDS instance details page. The user is an SSL user if the **ssl_type** field has a value.

```
select user, host, ssl_type from mysql.user where user = 'user_name';
```

3. Error message: **Client does not support authentication protocol requested by server.** plugin type was = 'sha256_password'

Error cause: DAS does not allow you to connect to the database whose password is encrypted with SHA-256.

Solution: Execute the following SQL statements to change the password encryption method to mysql_native_password.

```
alter user 'user_name'@'%' identified with mysql_native_password by 'password';
```

4. Error message: **Communications link failure The last packet sent successfully to the server was 0 milliseconds ago.** The driver has not received any packets from the server

Error cause: The network between the DAS server and the target instance is disconnected.

Solution: **Submit a work ticket** to contact customer service.

5. Error message: **Instance connect timeout, please login again**

Error cause: The connection to the DAS server timed out.

Solution: **Submit a work ticket** to contact customer service.

6. Error information: **RSA public key is not available client side (option serverRsaPublicKeyFile not set).**

   Error cause: The identity authentication mode of the database user has high requirements on password security. The password transmitted over the network during user authentication must be encrypted.

   - If the connection is an SSL encrypted connection, the SSL certificate and key pair are used to exchange the symmetric encryption key pair (generated in the TSL handshake). Later, the symmetric encryption key pair is used to encrypt the password and data.
   - For a non-SSL encrypted connection, the client uses the RSA public key of the MySQL server to encrypt the user password, and the server uses the RSA private key to decrypt and verify the password. This protects the password against snooping during network transmission.

   Solution: Enable SSL for the instance or change the identity authentication mode of the database user.

2.3 What Should I Do If I Can't Connect to My ECS (MySQL) Instance?

1. Error message: **Access denied for user 'user_name'@'100.xxx.xx.xx' (using password: YES)**

   a. Error cause: The username or password of the self-built database on the ECS is incorrect.

      Solution: Check whether the username and password are correct. If the username and password are correct, log in to the database using a client or the CLI tool and run **select * from mysql.user where user = 'user_name'** to view the account. Make sure that the DAS CIDR block is within the CIDR block of the user. **user_name @ %** and **user_name @100.%** are two different users whose passwords and permissions are independent. Enter the password of **user user_name @100.%**.

   b. Error cause: The IP address of the DAS server is not in the whitelist of the login user.

      Solution: Log in to the database using the client or CLI tool, and create a user account that can be used to access the database through DAS.

      ```
      create user 'user_name'@'100.%' identified by 'password';
      grant all privileges on *.* to 'user_name'@'100.%';
      ```

      NOTE

      - Ensure that the IP address of the DAS server is in a CIDR block starting with 100. Add the IP address to the whitelist of the login user.
      - Grant permissions to user **user_name@100.%** based on service requirements.

   c. Error cause: The SSL function is not enabled on the server.

      Solution: Run the following statement to check whether the user is an SSL user. If yes, enable SSL on the RDS instance details page. The user is an SSL user if the **ssl_type** field has a value.

      ```
      select user, host, ssl_type from mysql.user where user = 'user_name';
      ```

2. Error message: **Host 'xxx.xxx.xx.xx' is not allowed to connect to this MySQL server**

Error cause: The database username you entered does not support remote login. For example, if you enter username **root**, but only username **root@localhost** is configured in the **mysql.user** table, the specified user can only log in locally.

Solution: Use a client or CLI tool to log in to the self-built database and create a user account that supports remote login.

```
create user 'user_name'@'100.%' identified by 'password';
grant all privileges on *.* to 'user_name'@'100.%';
```

NOTE

- Ensure that the IP address of the DAS server is in a CIDR block starting with 100. Add the IP address to the whitelist of the login user.
- Grant permissions to user **user_name@100.%** based on service requirements.

3. Error message: **Communications link failure The last packet sent successfully to the server was 0 milliseconds ago. The driver has not received any packets from the server.**

   a. Error cause: The security group rules do not allow inbound traffic on the port.

      Solution: Modify the security group rules by referring to **How Do I View and Modify ECS Security Group Rules?**

   b. Error cause: The firewall policy does not allow inbound traffic on the port.

      Solution: Modify the firewall policy by referring to **How Do I View and Modify Firewall Rules?**

   c. Error cause: The remote login times out because the DNS resolution takes a long period of time.

      Solution: Rectify the fault by performing the following operations:

      i. Search for the configuration file of the self-built database in directory **/etc/my.cn**, enter the following content in **[mysqld]**, save the change and exit.

      ```
      skip-name-resolve
      ```

      NOTE

      The default location of the configuration file is **/etc/my.cnf**. If you store the file in the specified path, modify the directory accordingly.

      ii. Run **systemctl restart mysqld** to restart the database and log in again.

4. Error message: **Communications link failure The last packet sent successfully to the server was 0 milliseconds ago.** The driver has not received any packets from the server

   Error cause: The network between the DAS server and the target instance is disconnected.

   Solution: Check whether the firewall of the instance is correctly configured and whether the required port is enabled. If the firewall is abnormal or the port is not enabled, rectify the fault and try again. If the fault persists, **Submit a work ticket** to contact customer service.

5. Error message: **Instance connect timeout, please login again.**

Error cause: The connection to the DAS server timed out.

Solution: Rectify the fault by performing the following operations:

a. Log in to a remote ECS and run the **iptables -S | grep input** command to view firewall configurations of the instance. If the self-built database port is not included in the firewall whitelist, add an iptables rule or run the **systemctl stop iptables** command to disable the firewall to allow traffic through this port, and try again.
b. Log in to the ECS again and run the **ps -ef | grep mysql** command to check whether the database process is running. If processes **mysqld_safe** and **mysqld** are both running, the database process is normal. If the process is not running, run **systemctl start mysqld** to restart the database and try again.
c. If the fault persists, **submit a work ticket** to contact customer serviceContact technical support.

2.4 What Should I Do If I Can't Connect to My RDS for SQL Server Instance?

Error message: **Login failed for user 'rdsuser'. ClientConnectionId:xxx.**

Error cause: The username or password of the RDS DB instance is incorrect.

Solution: Ensure that the username and password are correct. If you are not sure, view the username and reset the password on the RDS console.

NOTICE

Changing the password may affect services.

2.5 What Should I Do If I Can't Connect to My ECS (Microsoft SQL Server) Instance?

Error message: **The TCP/IP connection to the host 100.xxx.xx.xx, port xxx has failed.**

Error cause: The port number of the self-built database is incorrect, or the network is disconnected.

Solution: Ensure that the port number of the self-built database is correct and that the port is included in the security group rule and firewall whitelist. For details, see **How Do I View and Modify ECS Security Group Rules?** and **How Do I View and Modify Firewall Rules?**.

2.6 What Should I Do If I Can't Connect to My RDS for PostgreSQL Instance?

Error message: **FATAL: Invalid username/password,login denied.**

Error cause: The username or password of the RDS DB instance is incorrect.

Solution: Check whether the username or password is correct. If you are not sure, view the username and reset the password on the RDS console.

NOTICE

Changing the password may affect services.

2.7 What Should I Do If I Can't Connect to My ECS (PostgreSQL) Instance?

Error message: **Connection refused (Connection refused).**

Error cause: The port number of the self-built database is incorrect, or the network is disconnected.

Solution: Ensure that the port number of the self-built database is correct and that the port is included in the security group rule and firewall whitelist. For details, see **How Do I View and Modify ECS Security Group Rules?** and **How Do I View and Modify Firewall Rules?**.

2.8 What Should I Do If I Can't Connect to My DDS Instance?

Error message: Command failed with error 18 (AuthenticationFailed): 'Authentication failed.' on server xxx.xxx.xx.xx:xxxx. The full response is { 'ok' : 0.0, 'errmsg' : "Authentication failed.", "code" : 18, "codeName" : "AuthenticationFailed" }

1. Error cause: The username or password of the DDS DB instance is incorrect.

   Solution: Check whether the username or password is correct. If you are not sure, view the username or reset the password on the DDS console.

   NOTICE

   Changing the password may affect services.

2. Error cause: The entered username does not have the permission to access the database.

   Solution: Check whether the username has the permission to access the database. If you are not sure, connect to the admin database as user **rwuser**. Then check whether the entered username has the required permission.

2.9 What Should I Do If I Can't Connect to My GaussDB(for MySQL) Instance?

1. Error message: **Access denied for user 'user_name'@'100.xxx.xx.xx' (using password: YES).**

   a. Error cause: The username or password of the GaussDB(for MySQL) instance is incorrect.

   Solution: Check whether the username and password are correct. If you are not sure, log in to the GaussDB(for MySQL) console to view the username and reset the password.

   NOTICE

   Changing the password may affect services.

   If the username and password are correct, log in to the database using a client or CLI tool and run **select * from mysql.user where user = 'user_name'** to view the account. Make sure that the DAS CIDR block is within the CIDR block of the user. **user_name @ %** and **user_name @100.%** are two different users whose passwords and permissions are independent. Make sure to enter the password of **user user_name @100.%**.

   b. Error cause: The IP address of the DAS server is not in the whitelist of the login user.

   Solution: Log in to the database using the client or CLI tool, and create a user that can be used to access the database through DAS.

   ```
   create user 'user_name'@'100.%' identified by 'password';
   grant all privileges on *.* to 'user_name'@'100.%';
   ```

   NOTE

   1. Ensure that the IP address of the DAS server is in a CIDR block starting with 100. Add the IP address to the whitelist of the login user.
   2. Grant permissions to user **user_name@100.%** based on service requirements.

2. Error message: **Trying to connect with ssl, but ssl not enabled in the server**

   Error cause: The SSL function is not enabled on the server.

   Solution: Run the following SQL statement to check whether the user is an SSL user. If yes, enable SSL on the GaussDB(for MySQL) instance details page. The user is an SSL user if the **ssl_type** field has a value.

   ```
   select user, host, ssl_type from mysql.user where user = 'user_name';
   ```

3. Error message: **Client does not support authentication protocol requested by server.** plugin type was = 'sha256_password'

   Error cause: DAS does not allow you to connect to the database whose password is encrypted with SHA-256.

   Solution: Execute the following SQL statements to change the password encryption method to mysql_native_password.

   ```
   alter user 'user_name'@'%' identified with mysql_native_password by 'password';
   ```


4. Error message: **Communications link failure The last packet sent successfully to the server was 0 milliseconds ago. The driver has not received any packets from the server.**

   Error cause: The network between the DAS server and the instance is disconnected.

   Solution: Contact technical support.

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

Error message: **FATAL: Invalid username/password,login denied.**

Error cause: The username or password of the GaussDB instance is incorrect.

Check whether the username or password is correct. If you are not sure, view the username and reset the password on the GaussDB console.

NOTICE

Changing the password may affect services.

2.11 What Should I Do If I Can't Connect to My DDM Instance?

Error message: **User has no databases**

Error cause: The DDM account has not been associated with any schema.

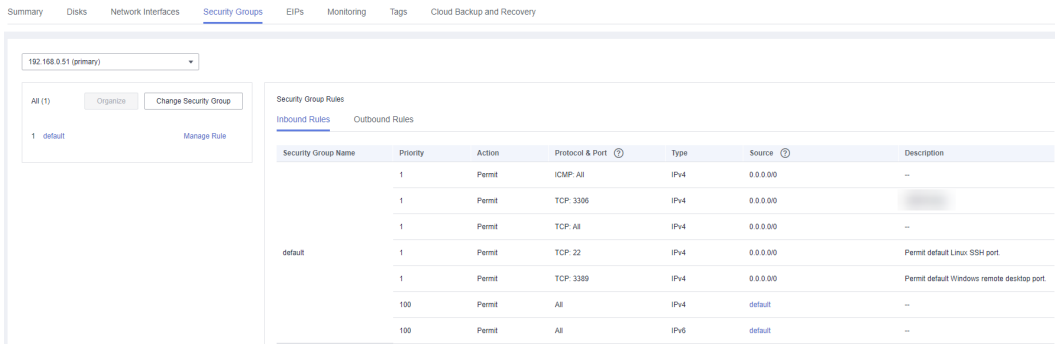
Solution: On the DDM instance basic information page, choose **Accounts** in the navigation pane on the left and associate the DDM account with the required schema.

2.12 How Do I View and Modify ECS Security Group Rules?

To enable DAS to access the self-built DB instances on ECSs, you need to add an inbound rule with the port set to 3306 (example) and source to 100.125.0.0/16 and 100.79.0.0/16.

Step 1 On the ECS details page, click the **Security Groups** tab and view security group rules.

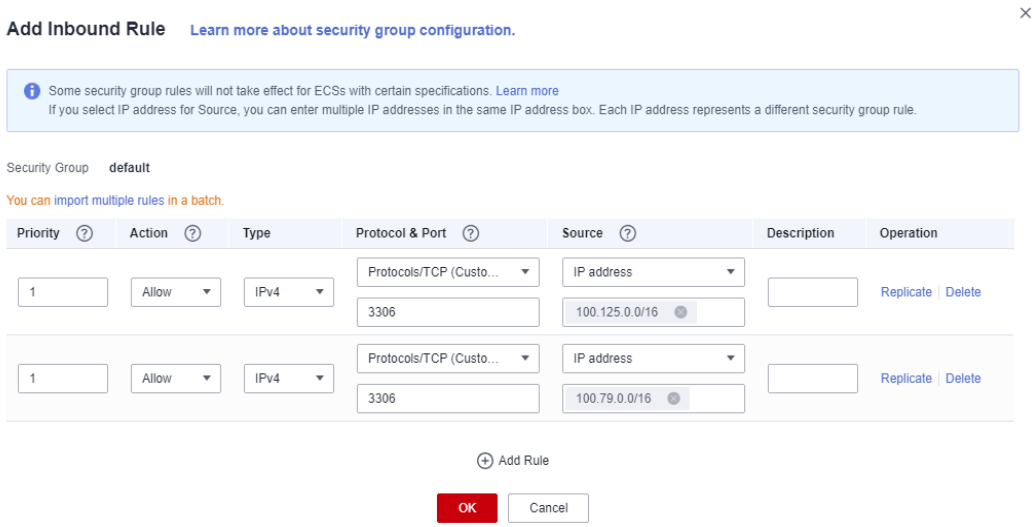
Figure 2-1 Security group rules



Step 2 Click **Manage Rule** on the left.

Step 3 On the **Inbound Rules** tab page, click **Add Inbound Rule**. For details, see **Configuring Security Group Rules**.

Figure 2-2 Adding an inbound rule

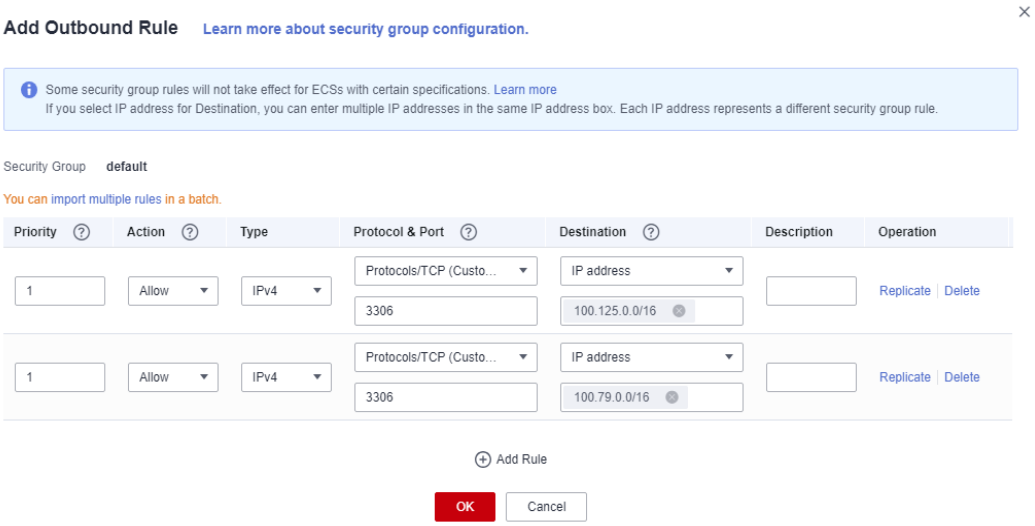


NOTE

Recommended configuration: Select **TCP** for **Protocols & TCP (Custom ports)**, enter the port number of the self-built database, and set the source to 100.125.0.0/16 and 100.79.0.0/16 respectively.

Step 4 On the **Outbound Rules** tab page, click **Add Outbound Rule**. For details, see **Configuring Security Group Rules**.

Figure 2-3 Adding an outbound rule



NOTE

Recommended configuration: Select **TCP (Custom ports)** for **Protocol & Port**, enter the port number of the self-built database, and set the source to 100.125.0.0/16 and 100.79.0.0/16 respectively.

----End

2.13 How Do I View and Modify Firewall Rules?

Step 1 In the ECS list, locate the required ECS and click **Remote Login**.

Step 2 Enter the username and password. After the login is successful, run the following command to check the iptables configuration:

```
iptables -S
```

```
-A INPUT -p tcp -m tcp --dport 49537 -j ACCEPT
```

NOTE

- The port next to **--dport** indicates the port that can be accessed.
- Perform the following operations to ensure that the port can be accessed:
  - Add an iptables rule to allow access to the port.
  - Run the following command to disable the firewall:
    ```
    systemctl stop iptables
    ```

----End

2.14 What Should I Do If My Connection Fails?

Error information: The connection does not exist.

Error cause: The shared connection is associated with the project of a shared user, which does not match the login project of the shared connection used by the current user.

Solution: In the upper left corner on the console, select another project in the current region and log in to the DB instance again.

3 Usage

3.1 What Can I Do If Garbled Characters Are Displayed in the Exported Database Result Set?

CSV files exported from DAS are encoded in UTF-8, whereas Excel files are encoded in ANSI. Encoding inconsistency resulted in garbled characters.

You are advised to open the CSV file using a text editor and save the file in ANSI encoding.

3.2 What Are the Precautions for Connecting DAS to a Third-Party Client?

After operations are performed on a third-party client, refresh the DAS console to view the generated data.

3.3 What Are the Username and Password for DAS?

The username and password for adding a login are those used for creating the DB instance.

3.4 What Should I Do If Table Obtaining Times Out?

The possible cause is that the instance load is heavy. As a result, the table data collection on DAS times out. You are advised to kill a thread and perform the operation again.

3.5 How Do I Modify the Collation?

DAS does not support the SQL Server modification on the GUI. You can run commands to implement the modification.

Go to the SQL Window page of the database and run the following commands:

In this example, the character set of the **test** database is set to simplified Chinese.

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

3.6 When a user creates a data tracking task, an error message indicating that the current user does not have the OBS operator permissions is displayed.

Symptom

After you enter the basic information, perform the pre-checks and reading logs function, an error message indicating that the current user does not have global OBS operator permissions is displayed.

Solutions

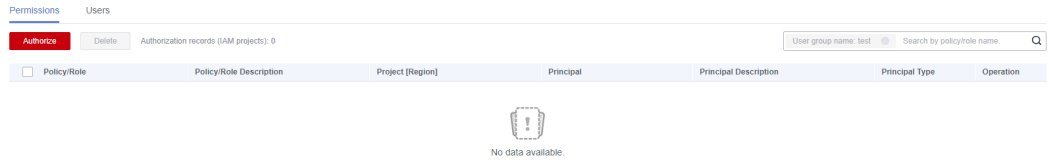
Step 1 Log in to the IAM console.

Step 2 Select the user group that the current user belongs to and click the user group name.

Figure 3-1 User group

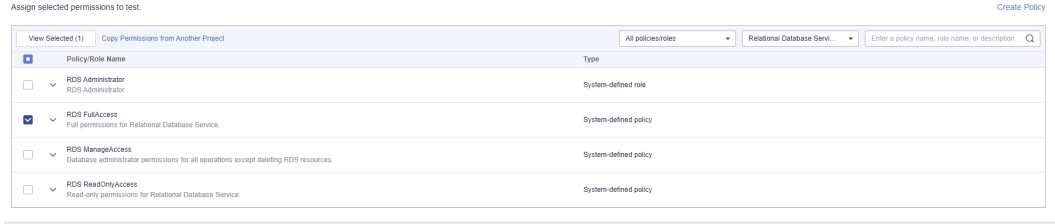
Step 3 Click **Authorize**.

Figure 3-2 Authorization button



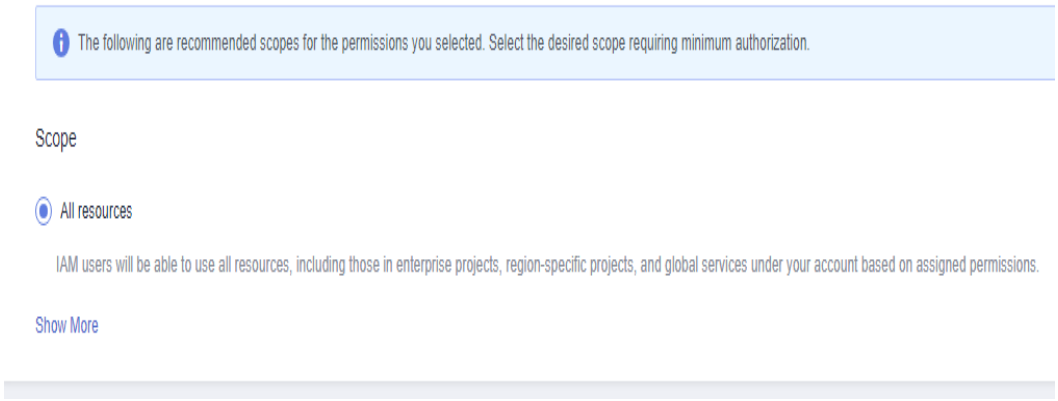
Step 4 Search for **Relational Database Service**, select **RDS FullAccess**, and click **Next**.

Figure 3-3 Adding privileges



Step 5 Select a scope and click **OK**.

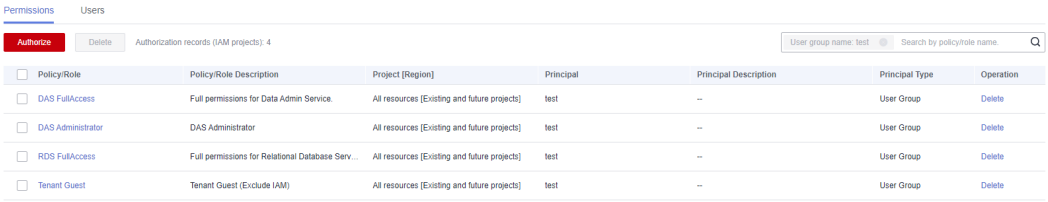
Figure 3-4 Authorization scope



Step 6 Return to the authorization record page and confirm the permissions of the current user group.

Ensure that the current user group has **DAS FullAccess**, **DAS Administrator**, **RDS FullAccess**, and **Tenant Guest** permissions.

Figure 3-5 Viewing permissions



----End

4 Resource Freezing, Release, Deletion, and Unsubscription

Why Are My Resources on DAS Released?

If your subscriptions have expired but not been renewed, or if you are in arrears, your cloud resources enter a grace period. If you do not complete the payment or renewal after the grace period expires, your resources will enter a retention period and become unavailable. If you still do not renew them or top up your account after the retention period ends, your resources will be released and your data stored will be deleted. For details, see **Service Suspension and Resource Release**.

Why Are My Resources on DAS 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 Instance Is Frozen?

No. If your instance is frozen because your account is in arrears, go to top up your account to unfreeze your instance and then back up instance data.

How Do I Unfreeze My Resources?

DAS is free of charge. If your instances managed on DAS are frozen due to arrears, you can renew the instances or top up your account to unfreeze them.

What Impacts Does Resource Freezing, Unfreezing or Release Have on My Instances?

- After a resource is frozen:
  - It cannot be accessed, and your services will be interrupted. Database management functions provided by DAS become unavailable either, for example, after an RDS instance is frozen, you cannot log in to the instance and execute SQL statements on it using DAS any more.
  - No changes can be performed on it if it is a yearly/monthly instance.
  - It can be unsubscribed from or deleted manually.

- After a frozen resource is unfrozen, you can connect to it using DAS again.
- After a resource is released, it will be deleted.

Can My Resources Be Recovered After They Are Released or Unsubscribed From?

Deleted instances cannot be recovered.

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

