Data Replication Service

Real-Time Disaster Recovery

Issue 29

Date 2023-11-30

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://www.huawei.com

Email: support@huawei.com

Security Declaration

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

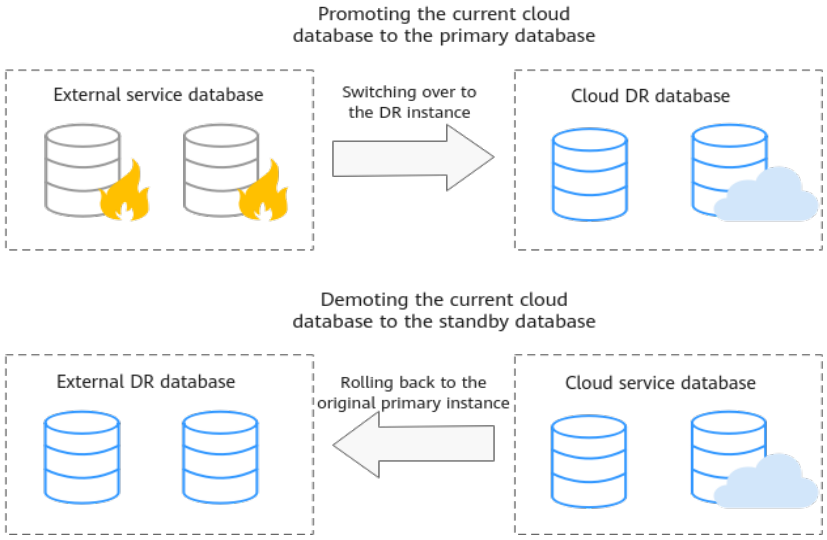
Contents

1 DR Overview

To prevent service unavailability caused by regional faults, DRS provides disaster recovery to ensure service continuity. You can easily implement disaster recovery between on-premises and cloud, without the need to invest a lot in infrastructure in advance.

The disaster recovery architectures, such as two-site three-data-center and two-site four-data center, are supported. A primary/standby switchover can be implemented by promoting a standby node or demoting a primary node in the disaster recovery scenario.

Figure 1-1 Real-time DR switchover



Supported Database Types

The following table lists the database types supported by DRS.

Table 1-1 DR schemes

Service Database	DR Database	Documentation
• On-premises MySQL databases • MySQL databases on an ECS • MySQL databases on other clouds • RDS for MySQL	RDS for MySQL	• **From MySQL to MySQL (Single-Active DR)** • **From MySQL to MySQL (Dual-Active DR)**
	GaussDB(for MySQL)	**From MySQL to GaussDB(for MySQL) (Single-Active DR)**
DDM	DDM	**From DDM to DDM (Single-Active DR)**
GaussDB(for MySQL)	GaussDB(for MySQL)	• **From GaussDB(for MySQL) to GaussDB(for MySQL) (Single-Active DR)** • **From GaussDB(for MySQL) to GaussDB(for MySQL) (Dual-Active DR)**

Basic Principles of Real-Time Disaster Recovery

DRS uses the real-time replication technology to implement disaster recovery for two databases. The underlying technical principles are the same as those of real-time migration. The difference is that real-time DR supports forward synchronization and backward synchronization. In addition, disaster recovery is performed on the instance-level, which means that databases and tables cannot be selected.

2 DR Scenarios

2.1 From MySQL to MySQL (Single-Active DR)

Supported Source and Destination Databases

Table 2-1 Supported databases

Service databases	DR Database
• On-premises MySQL databases • MySQL databases on an ECS • MySQL databases on other clouds • RDS for MySQL	• RDS for MySQL

Database Account Permission Requirements

To start a DR task, the service and DR database users must meet the requirements in the following table. Different types of DR tasks require different permissions. For details, see **Table 2-2**. DRS automatically checks the database account permissions in the pre-check phase and provides handling suggestions.

Table 2-2 Database account permission

Type	Permission Required
Service database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION. The user **root** of the RDS for MySQL instance has the preceding permissions by default. If the service database version is 8.0.14 to 8.0.18, the SESSION_VARIABLES_ADMIN permission is required.
DR database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION. The user **root** of the RDS for MySQL instance has the preceding permissions by default. If the DR database version is 8.0.14 to 8.0.18, the SESSION_VARIABLES_ADMIN permission is required.

NOTE

- You are advised to create an independent database account for DRS task connection to prevent task failures caused by database account password modification.
- After changing the account passwords for the service and DR databases, **modify the connection information** in the DRS task as soon as possible to prevent automatic retry after a task failure. Automatic retry will lock the database accounts.
- **Table 2-2** lists the minimum permissions required by a DRS task. If you need to migrate the grant permission through a DRS task, ensure that the connection account of the DRS task has the corresponding permission. Otherwise, the destination database user may not be authorized due to grant execution failure. For example, if the connection account of the DRS task does not require the process permission, but you need to migrate the process permission through a DRS task, ensure that the connection account of the DRS task has the process permission.

Prerequisites

- **You have logged in to the DRS console.**
- Your account balance is greater than or equal to $0 USD.
- For details about the supported DB types and versions, see **Supported Databases**.
- If a subaccount is used to create a DRS task, ensure that an agency has been added. For details about how to create an agency, see **Agency Management**.

Suggestions

CAUTION

- During the DR initialization, do not perform DDL operations on the service database. Otherwise, the task may be abnormal.
- During DR initialization, ensure that no data is written to the DR database to ensure data consistency before and after DR.

- The success of DR depends on environment and manual operations. To ensure a smooth DR, perform a DR trial before you start the DR task to help you detect and resolve problems in advance.
- It is recommended that you start your DR task during off-peak hours to minimize the impact on your services.
  - If the bandwidth is not limited, initialization of DR will increase query workload of the source database by 50 MB/s and occupy 2 to 4 vCPUs.
  - To ensure data consistency, tables without a primary key may be locked for 3s during disaster recovery.
  - The data in the DR process may be locked by other transactions for a long period of time, resulting in read timeout.
  - If DRS concurrently reads data from a database, it will use about 6 to 10 sessions. The impact of the connections on services must be considered.
  - If you read a table, especially a large table, during DR, the exclusive lock on that table may be blocked.
  - For more information about the impact of DRS on databases, see **What Is the Impact of DRS on Source and Destination Databases?**
- Data-Level Comparison

  To obtain accurate comparison results, start data comparison at a specified time point during off-peak hours. If it is needed, select **Start at a specified time** for **Comparison Time**. Due to slight time difference and continuous operations on data, data inconsistency may occur, reducing the reliability and validity of the comparison results.

Precautions

Before creating a DR task, read the following precautions:

Table 2-3 Precautions

Type	Constraint
Disaster recovery objects	• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery. • System tables are not supported. • Triggers and events do not support disaster recovery. • Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery. • Disaster recovery cannot be configured for a specific service database.
Service database configuration	• The binlog of the MySQL service database must be enabled and use the row-based format. • If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days. – For self-built MySQL databases, you can set the **expire_logs_days** parameter to specify the binlog retention period. – If the source database is an RDS for MySQL instance, set the binlog retention period by following the instructions provided in **RDS User Guide**. • The service database username or password cannot be empty. • **server_id** in the MySQL service database must be set. If the service database version is MySQL 5.6 or earlier, the **server_id** value ranges from **2** to **4294967296**. If the service database is MySQL 5.7 or later, the **server_id** value ranges from **1** to **4294967296**. • During disaster recovery, if the session variable **character_set_client** is set to **binary**, some data may include garbled characters. • GTID must be enabled for the database. • The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_). • The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '<>/\ • If the **expire_logs_days** value of the service database is set to **0**, the disaster recovery may fail. • If tables that have no primary key contain hidden primary keys in the service database, the DR task may fail or data may be inconsistent.

Type	Constraint
DR database configuration	• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal. • The DR DB instance must have sufficient storage space. • The major version of the DR database must be the same as that of the service database. • The binlog of the DR database must be enabled and use the row-based format. • GTID must be enabled for the DR database. • Except the MySQL system database, the DR database must be empty. After a DR task starts, the DR database is set to read-only.

Type	Constraint
Precautions	• If the DCC does not support instances with 4 vCPUs and 8 GB memory or higher instance specifications, the DR task cannot be created. • If a physically generated column in a table is generated based on a time type, the data in the column may be inconsistent. • Cascade operations cannot be performed on tables with foreign keys. If the foreign key index of a table is a common index, the table structure may fail to be created. You are advised to use a unique index. • The service database does not support point-in-time recovery (PITR). • Binlogs cannot be forcibly deleted. Otherwise, the DR task fails. • The service database does not support the **reset master** or **reset master to** command, which may cause DRS task failures or data inconsistency. • If the network is reconnected within 30 seconds, disaster recovery will not be affected. If the network is interrupted for more than 30 seconds, the DR task will fail. • Resumable upload is supported, but data may be repeatedly inserted into a table that does not have a primary key. • If there is a DR task in a database, you are not allowed to create a migration or synchronization task (The database cannot be used as the source or destination database of the migration or synchronization task). • The parameter modification of the service database is not recorded in logs and is not synchronized to the DR database. Therefore, you need to modify the parameters after the DR database is promoted to the primary. • If the service database and DR database are RDS for MySQL instances, tables with TDE enabled cannot be created. • Before creating a DRS task, if concurrency control rules of SQL statements are configured for the service or DR database, the DRS task may fail. • If a high-privilege user created in an external database is not supported by RDS for MySQL, the user will not be synchronized to the DR database, for example, the super user. • The DR relationship involves only one primary database. If the external database does not provide the superuser permission, it cannot be set to read-only when it acts as a standby database. Ensure that the data of the standby node is synchronized only from the primary node. Any other write operations will pollute the data in the standby database, data conflicts may occur in the DR center and cannot be resolved. • If the external database is a standby and read-only database, only the account with the superuser permission can write data

Type	Constraint
	to that database. But you still need to ensure that data is written only by this account. Otherwise, the standby database may be polluted, and data conflicts occur in the DR center and cannot be resolved. • During disaster recovery, if the password of the service database is changed, the DR task will fail. To rectify the fault, you can correct the service database information on the DRS console and retry the task to continue disaster recovery. Generally, you are advised not to modify the preceding information during disaster recovery. • If the service database port is changed during disaster recovery, the DR task fails. Generally, you are advised not to modify the service database port during disaster recovery. • During disaster recovery, if the service database is on an RDS DB instance that does not belong the current cloud platform, the IP address cannot be changed. If the service database is an RDS instance on the current cloud and the DR task fails due to changes on the IP address, DRS automatically changes the IP address to the correct one. Then, you can retry the task to continue disaster recovery. Therefore, changing the IP address is not recommended. • During disaster recovery, you can create accounts for the service database. • During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal. • During disaster recovery initialization, a lot of binlogs are generated in the DR database, occupying too much storage space. Therefore, during disaster recovery initialization, only the latest five binlogs are retained in the DR database by default. After the disaster recovery initialization is complete, the retention period of binlogs in the DR database is restored to the value you configure. If you want to keep the binlog retention period of the DR database to be the value you specify due to service requirements, you need to submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket. • Do not write data to the source database during the primary/standby switchover. Otherwise, data pollution or table structure inconsistency may occur, resulting in data inconsistency between the service database and DR database.

Procedure

Step 1 On the **Disaster Recovery Management** page, click **Create Disaster Recovery Task**.

Step 2 On the **Create Disaster Recovery Instance** page, select a region and project, specify the task name, description, and the DR instance details, and click **Create Now**.

- Task information description

Figure 2-1 DR task information

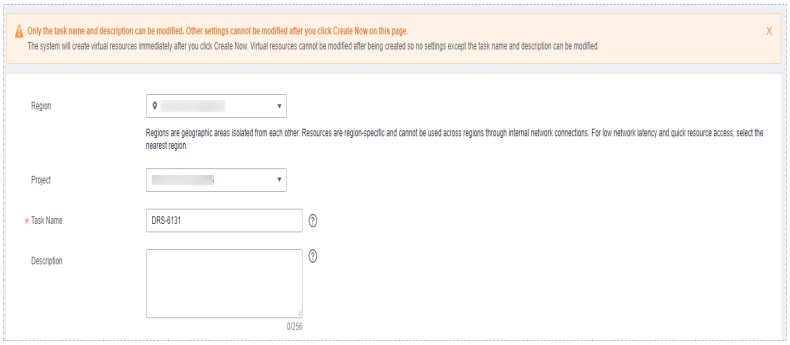


Table 2-4 Task and recipient description

Parameter	Description
Region	The region where your service is running. You can change the region.
Project	The project corresponds to the current region and can be changed.
Task Name	The task name must start with a letter and consist of 4 to 50 characters. It can contain only letters, digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters !=<>'&"\

- DR instance information

Figure 2-2 DR instance information

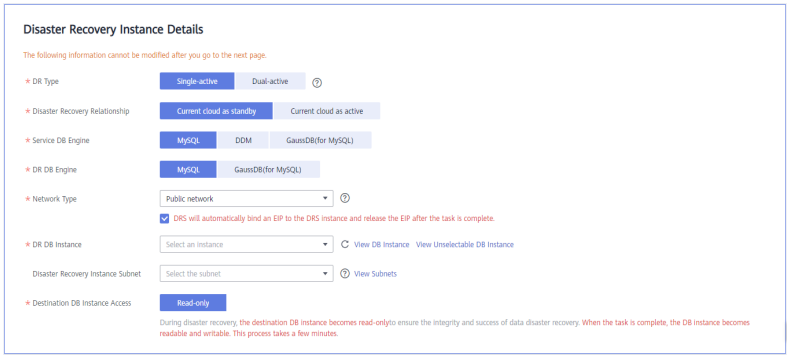


Table 2-5 DR instance settings

Parameter	Description
DR Type	Select **Single-active**. The DR type can be single-active or dual-active. If **Dual-active** is selected, two subtasks are created by default, a forward DR task and a backward DR task. **NOTE** Only whitelisted users can use dual-active DR. To use this function, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket.
Disaster Recovery Relationship	Select **Current cloud as standby**. This parameter is available only when you select **Single-active**. By default, **Current cloud as standby** is selected. You can also select **Current cloud as active**. – **Current cloud as standby**: The DR database is on the current cloud. – **Current cloud as active**: The service database is on the current cloud.
Service DB Engine	Select **MySQL**.
DR DB Engine	Select **MySQL**.
Network Type	The public network is used as an example. Available options: **VPN or Direct Connect** and **Public network**. By default, the value is **Public network**.
DR DB Instance	RDS DB instance you have created as the destination database of the DR task.
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click **View Subnet** to go to the network console to view the subnet where the instance resides. By default, the DRS instance and the destination DB instance are in the same subnet. You need to select the subnet where the DRS instance resides and ensure that there are available IP addresses. To ensure that the disaster recovery instance is successfully created, only subnets with DHCP enabled are displayed.

Parameter	Description
Destination Database Access	Select **Read-only**. This parameter is available only when you select **Single-active**. – During disaster recovery, the entire DR database instance becomes read-only. To change the DR database to **Read/Write**, you can change the DR database (or destination database) to a service database by clicking **Promote Current Cloud** on the **Disaster Recovery Monitoring** tab. – After the DR task is complete, the DR database changes to **Read/Write**. – When the external database functions as the DR database, the user with the superuser permission can set the database to read-only. – If a DRS instance node is rebuilt due to a fault, to ensure data consistency during the DRS task restoration, the current cloud standby database is set to read-only before the task is restored. After the task is restored, the synchronization relationship recovers.

- Specifications

Figure 2-3 Specifications

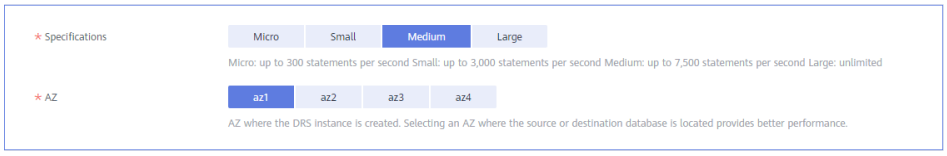


Table 2-6 Specifications

Parameter	Description
Specifications	DRS instance specifications. Different specifications have different performance upper limits. For details, see **Real-Time DR**. **NOTE** DRS allows you to upgrade specifications only for real-time DR tasks from MySQL to MySQL, from MySQL to GaussDB(for MySQL), and from GaussDB(for MySQL) to GaussDB(for MySQL). Task specifications cannot be downgraded. For details, see **Changing Specifications**.
AZ	Select the AZ where you want to create the DRS task. Selecting the one housing the source or destination database can provide better performance.

- Enterprise Project and Tags

Figure 2-4 Enterprise projects and tags

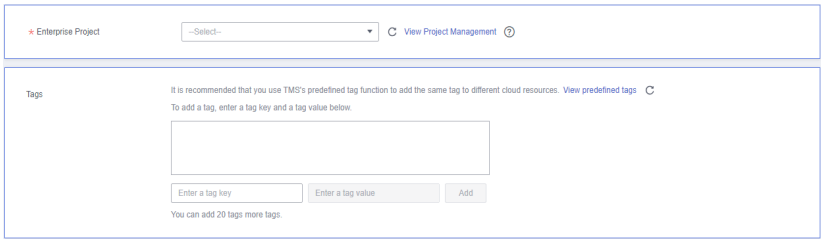


Table 2-7 Enterprise Project and Tags

Parameter	Description
Enterprise Project	An enterprise project you would like to use to centrally manage your cloud resources and members. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise projects, see ***Enterprise Management User Guide***. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Project Management Service** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.
Tags	– Tags a task. This configuration is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 20 tags. – After a task is created, you can view its tag details on the **Tags** tab. For details, see **Tag Management**.

NOTE

If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.

Step 3 On the **Configure Source and Destination Databases** page, wait until the DR instance is created. Then, specify source and destination database information and click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, select the check box before the agreement and click **Next**.

- Select **Current cloud as standby** for **Disaster Recovery Relationship** in **Step 2**.

Figure 2-5 Service database information

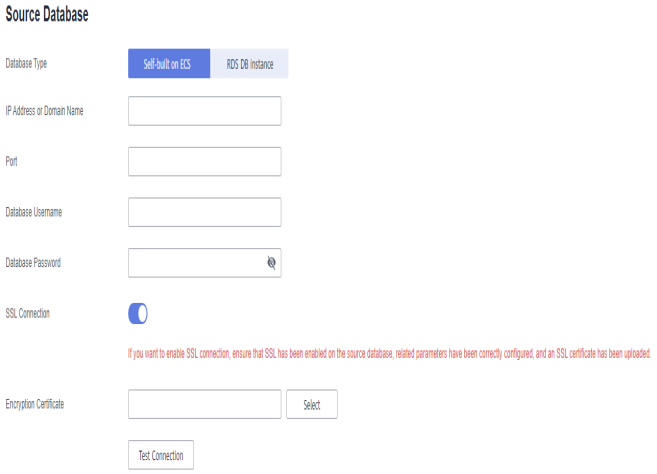


Table 2-8 Service database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The source database can be a **Self-built on ECS** or an **RDS DB instance**. After selecting **RDS DB instance**, select the region where the source database resides and the region cannot be the same as the region where the destination database resides. The region where the destination database is located is the region where you log in to the management console. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the service database.
Port	The port of the service database. Range: 1 – 65535
Database Username	The username for accessing the service database.
Database Password	The password for the service database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **Connection Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password.

Parameter	Description
SSL Connection	SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.
Region	The region where the service DB instance is located. This parameter is selected by default. This parameter is available only when the source database is an **RDS DB instance**.
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an **RDS DB instance**.
Database Username	The username for accessing the service database.
Database Password	The password for the service database username.

NOTE

The IP address, domain name, username, and password of the service database are encrypted and stored in DRS and will be cleared after the task is deleted.

Figure 2-6 DR database information

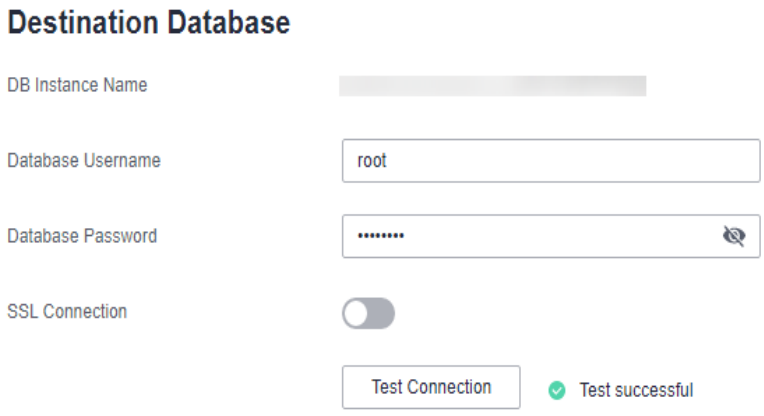


Table 2-9 DR database settings

Parameter	Description
DB Instance Name	The DB instance you selected when creating the DR task and cannot be changed.

Parameter	Description
Database Username	The username for accessing the DR database.
Database Password	The password for the database username. The password can be changed after a task is created. If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.
SSL Connection	If SSL connection is required, enable SSL on the DR database, ensure that related parameters have been correctly configured, and upload an SSL certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.

- Select **Current cloud as active** for **Disaster Recovery Relationship** in **Step 2**.

Figure 2-7 Service database information

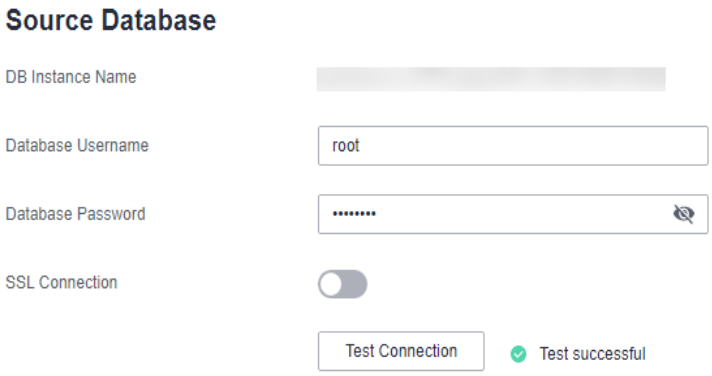


Table 2-10 Service database settings

Parameter	Description
DB Instance Name	The RDS instance selected when you created the DR task. This parameter cannot be changed.
Database Username	The username for accessing the service database.

Parameter	Description
Database Password	The password for the database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in the system and will be cleared after the task is deleted.
SSL Connection	If SSL connection is required, enable SSL on the service database, ensure that related parameters have been correctly configured, and upload an SSL certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.

Figure 2-8 DR database information

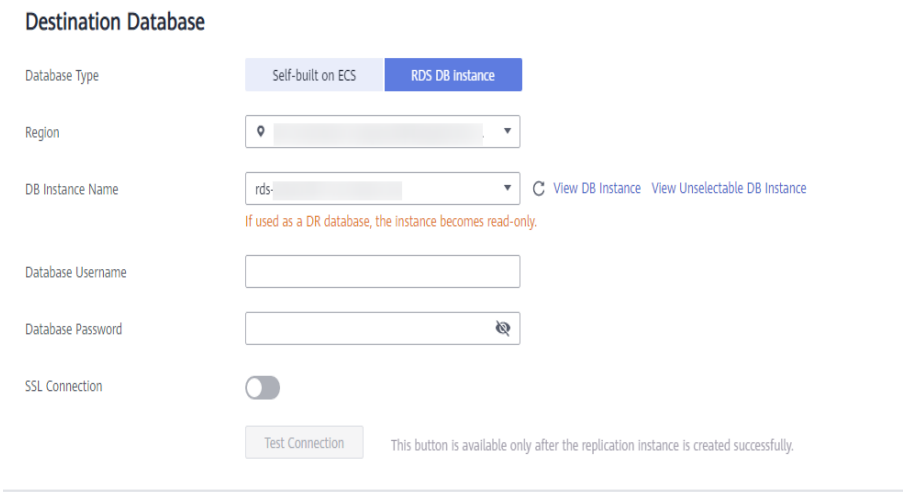


Table 2-11 DR database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The destination database can be a **Self-built on ECS** or an **RDS DB instance**. If you select **RDS DB instance**, you need to select the region where the destination database is located. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the DR database.
Port	The port of the DR database. Range: 1 – 65535
Region	The region where the RDS DB instance is located. This parameter is available only when the destination database is an RDS DB instance.
DB Instance Name	DR instance name. This parameter is available only when the destination database is an RDS DB instance. **NOTE** When the DB instance is used as the DR database, it is set to read-only. After the task is complete, the DB instance can be readable and writable.
Database Username	Username for logging in to the DR database.
Database Password	Password for the database username.
SSL Connection	If SSL connection is required, enable SSL on the DR database, ensure that related parameters have been correctly configured, and upload an SSL certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.

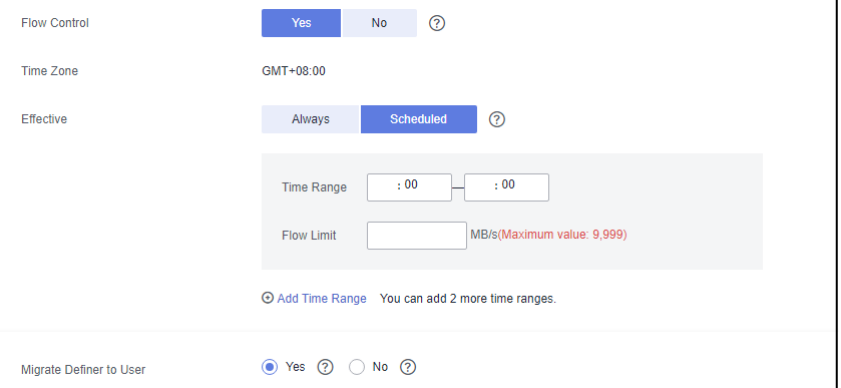
NOTE

The IP address, domain name, username, and password of the DR database are encrypted and stored in DRS and will be cleared after the task is deleted.

Step 4 On the **Configure DR** page, specify flow control and click **Next**.

Figure 2-9 DR settings

Table 2-12 DR settings

Parameter	Description
Flow Control	You can choose whether to control the flow. • **Yes** You can customize the maximum DR speed. In addition, you can set the time range based on your service requirements. The traffic rate setting usually includes setting of a rate limiting time period and a traffic rate value. Flow can be controlled all day or during specific time ranges. The default value is **All day**. A maximum of three time ranges can be set, and they cannot overlap. The flow rate must be set based on the service scenario and cannot exceed 9,999 MB/s. **Figure 2-10** Flow control  • **No** The DR speed is not limited and the outbound bandwidth of the source database is maximally used, which causes read consumption on the source database accordingly. For example, if the outbound bandwidth of the source database is 100 MB/s and 80% bandwidth is used, the I/O consumption on the source database is 80 MB/s. **NOTE** – Flow control mode takes effect only in the DR initialization phase. – You can also change the flow control mode when the task is in the **Configuration** state. For details, see **Modifying the Flow Control Mode**.

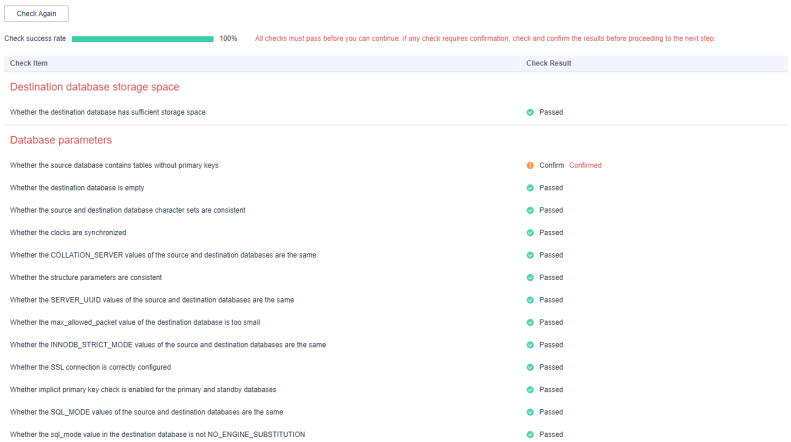
Parameter	Description
Migrate Definer to User	Indicates whether to migrate the Definers of all source database objects to the destination database user entered during the connection test. • Yes The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see **How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?** For example, if the view is CREATE ALGORITHM=UNDEFINED DEFINER=`username`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` before migration, it is converted to CREATE ALGORITHM=UNDEFINED DEFINER=`drsUser`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` after the migration. **drsUser** indicates the destination database user used for testing the connection. • **No** The Definers of all source database objects will not be changed. You need to migrate all accounts and permissions of the source database in the next step. Note that if the Definer account is not found in the destination database, unavailable objects will be created. For details about Definer, see the **MySQL official document**.

Step 5 On the **Check Task** page, check the DR task.

- If any check fails, review the failure cause and rectify the fault. After the fault is rectified, click **Check Again**.

  For details about how to handle check failures, see **Solutions to Failed Check Items** in *Data Replication Service User Guide*.

Figure 2-11 Pre-check



- If the check is complete and the check success rate is 100%, go to the **Compare Parameter** page.

  NOTE

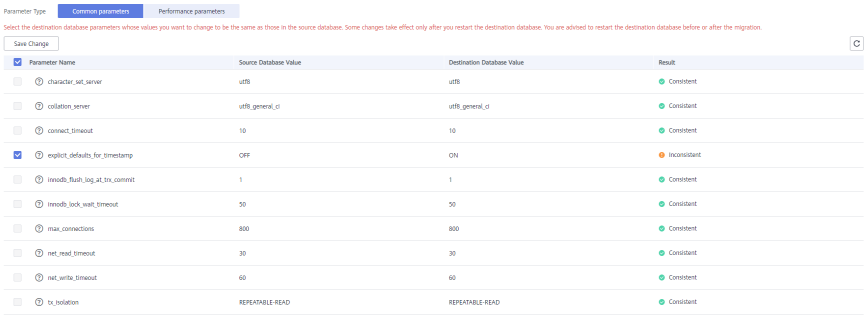
  You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

Step 6 Compare the parameters.

The parameter comparison function helps you check the consistency of common parameters and performance parameters between service and DR databases and show inconsistent values. You can determine whether to use this function based on service requirements. It mainly ensures that services are not affected after the DR task is completed.

- This process is optional, so you can click **Next** to skip the comparison.
- Compare common parameters:
  - For common parameters, if the parameters in the service database are different from those in the DR database, click **Save Change** to make the parameters of the DR database be the same as those in the service database.

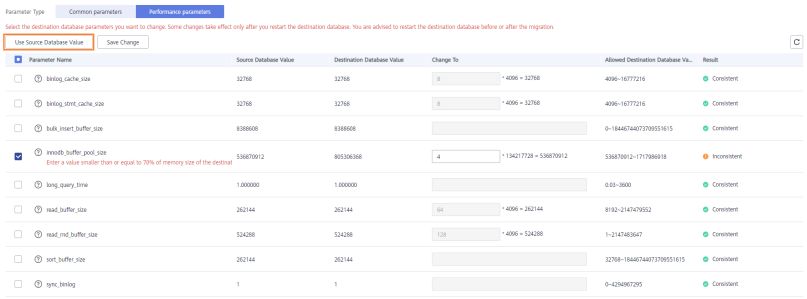
    Figure 2-12 Modifying common parameters

  - Performance parameter values in both the service and DR databases can be the same or different.
    - If you need to adjust the performance parameters, enter the value in the **Change to** column and click **Save Change**.
    - If you want to make the performance parameter values of the source and destination database be the same:
      1) Click **Use Source Database Value**.

         DRS automatically makes the DR database values the same as those of the service database.

Figure 2-13 One-click modification



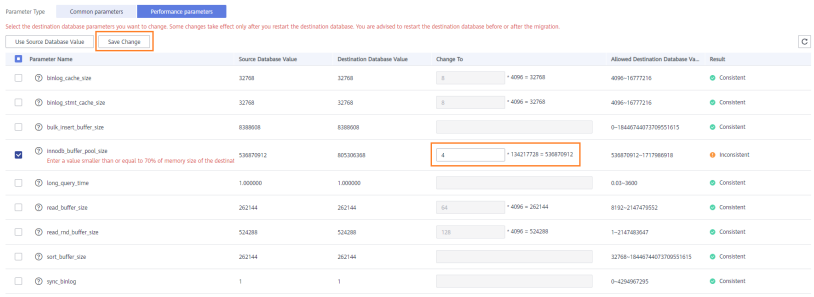
NOTE

You can also manually enter the value as required.

2) Click **Save Change**.

DRS changes the DR database parameter values based on your settings. After the modification, the comparison results are automatically updated.

Figure 2-14 One-click modification



Some parameters in the DR database cannot take effect immediately, so the comparison result is temporarily inconsistent. Restart the DR database before the DR task is started or after the DR task is completed. To minimize the impact of database restart on your services, restart the DR database at the scheduled time after the disaster recovery is complete.

For details about parameter comparison, see **Parameters for Comparison** in the *Data Replication Service User Guide*.

3) Click **Next**.

Step 7 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO Synchronization Delay Threshold**, **Stop Abnormal Tasks After** and DR instance details. Then, click **Submit**.

Figure 2-15 Task startup settings

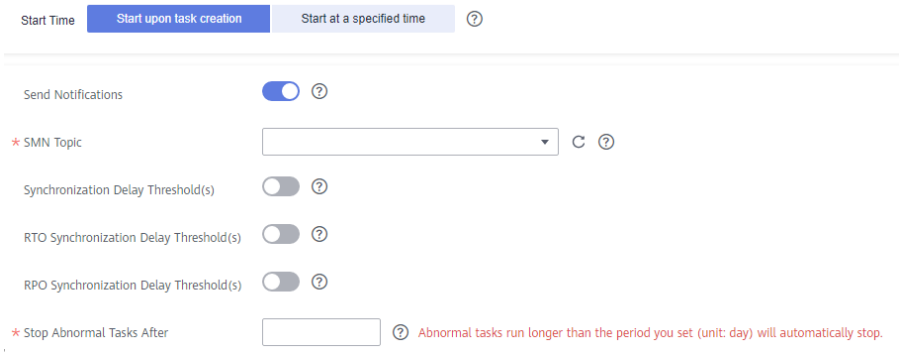


Table 2-13 Task and recipient description

Parameter	Description
Start Time	Set **Start Time** to **Start upon task creation** or **Start at a specified time** based on site requirements. **NOTE** Starting a DR task may slightly affect the performance of the service and DR databases. You are advised to start a DR task during off-peak hours.
Send Notifications	SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.
SMN Topic	This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber. For details, see **Simple Message Notification User Guide**.
Synchronization Delay Threshold	During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.

Parameter	Description
RTO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the DR database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the RTO delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RPO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the service database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient. • In the early stages of an incremental disaster recovery, the synchronization delay is long because a large quantity of data is awaiting synchronization. In this case, no notifications will be sent.
Stop Abnormal Tasks After	Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is **14**. **NOTE** • You can set this parameter only for pay-per-use tasks. • Tasks in the abnormal state are still charged. If tasks remain in the abnormal state for a long time, they cannot be resumed. Abnormal tasks run longer than the period you set (unit: day) will automatically stop to avoid unnecessary fees.

Step 8 After the task is submitted, view and **manage it** on the **Disaster Recovery Management** page.

- You can view the task status. For more information about task status, see **Task Statuses**.
- You can click in the upper-right corner to view the latest task status.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.

----End

2.2 From MySQL to GaussDB(for MySQL) (Single-Active DR)

Supported Source and Destination Databases

Table 2-14 Supported databases

Service Database	DR Database
• On-premises MySQL databases • MySQL databases on an ECS • MySQL databases on other clouds • RDS for MySQL	• GaussDB(for MySQL)

Database Account Permission Requirements

To start a DR task, the service and DR database users must meet the requirements in the following table. Different types of DR tasks require different permissions. For details, see **Table 2-15**. DRS automatically checks the database account permissions in the pre-check phase and provides handling suggestions.

Table 2-15 Database account permission

Type	Permission Required
Service database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION The **root** account of the RDS for MySQL DB instance has the preceding permissions by default.
DR database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION The **root** account of the GaussDB(for MySQL) instance has the preceding permissions by default.

NOTE

- You are advised to create an independent database account for DRS task connection to prevent task failures caused by database account password modification.
- After changing the account passwords for the service and DR databases, **modify the connection information** in the DRS task as soon as possible to prevent automatic retry after a task failure. Automatic retry will lock the database accounts.
- **Table 2-15** lists the minimum permissions required by a DRS task. If you need to migrate the grant permission through a DRS task, ensure that the connection account of the DRS task has the corresponding permission. Otherwise, the destination database user may not be authorized due to grant execution failure. For example, if the connection account of the DRS task does not require the process permission, but you need to migrate the process permission through a DRS task, ensure that the connection account of the DRS task has the process permission.

Prerequisites

- **You have logged in to the DRS console.**
- Your account balance is greater than or equal to $0 USD.
- For details about the supported DB types and versions, see **Supported Databases**.
- If a subaccount is used to create a DRS task, ensure that an agency has been added. For details about how to create an agency, see **Agency Management**.

Suggestions

CAUTION

- During the DR initialization, do not perform DDL operations on the service database. Otherwise, the task may be abnormal.
- During DR initialization, ensure that no data is written to the DR database to ensure data consistency before and after DR.

- The success of DR depends on environment and manual operations. To ensure a smooth DR, perform a DR trial before you start the DR task to help you detect and resolve problems in advance.
- It is recommended that you start your DR task during off-peak hours to minimize the impact on your services.
  - If the bandwidth is not limited, initialization of DR will increase query workload of the source database by 50 MB/s and occupy 2 to 4 vCPUs.
  - To ensure data consistency, tables without a primary key may be locked for 3s during disaster recovery.
  - The data in the DR process may be locked by other transactions for a long period of time, resulting in read timeout.
  - If DRS concurrently reads data from a database, it will use about 6 to 10 sessions. The impact of the connections on services must be considered.
  - If you read a table, especially a large table, during DR, the exclusive lock on that table may be blocked.
  - For more information about the impact of DRS on databases, see **What Is the Impact of DRS on Source and Destination Databases?**

- Data-Level Comparison

  To obtain accurate comparison results, start data comparison at a specified time point during off-peak hours. If it is needed, select **Start at a specified time** for **Comparison Time**. Due to slight time difference and continuous operations on data, data inconsistency may occur, reducing the reliability and validity of the comparison results.

Precautions

Before creating a DR task, read the following precautions:

Table 2-16 Precautions

Type	Restrictions
Disaster recovery objects	• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery. • System tables are not supported. • Triggers and events do not support disaster recovery. • Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery. • Disaster recovery cannot be configured for a specific service database.

Type	Restrictions
Service database configuration	• The binlog of the MySQL service database must be enabled and use the row-based format. • If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days. – For self-built MySQL databases, you can set the **expire_logs_days** parameter to specify the binlog retention period. – If the source database is an RDS for MySQL instance, set the binlog retention period by following the instructions provided in **RDS User Guide**. • The service database username or password cannot be empty. • **server-id** in the MySQL service database must be set. If the service database version is MySQL 5.6 or earlier, the **server-id** value ranges from **2** to **4294967296**. If the service database is MySQL 5.7 or later, the **server-id** value ranges from **1** to **4294967296**. • During disaster recovery, if the session variable **character_set_client** is set to **binary**, some data may include garbled characters. • GTID must be enabled for the database. • The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_). • The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '<>/\ • If the **expire_logs_days** value of the service database is set to **0**, the disaster recovery may fail. • If tables that have no primary key contain hidden primary keys in the service database, the DR task may fail or data may be inconsistent.
DR database configuration	• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal. • The DR DB instance must have sufficient storage space. • The binlog of the DR database must be enabled and use the row-based format. • GTID must be enabled for the DR database. • The DR DB instance cannot contain any service databases except the system database.

Type	Restrictions
Precautions	• The parameter modification of the service database is not recorded in logs and is not synchronized to the DR database. Therefore, you need to modify the parameters after the DR database is promoted to the primary. • If a high-privilege user created in an external database is not supported by RDS for MySQL, the user will not be synchronized to the DR database, for example, the super user. • If a physically generated column in a table is generated based on a time type, the data in the column may be inconsistent. • Cascade operations cannot be performed on tables with foreign keys. If the foreign key index of a table is a common index, the table structure may fail to be created. You are advised to use a unique index. • The service database does not support point-in-time recovery (PITR). • Binlogs cannot be forcibly deleted. Otherwise, the DR task fails. • The service database does not support the **reset master** or **reset master to** command, which may cause DRS task failures or data inconsistency. • If the network is reconnected within 30 seconds, disaster recovery will not be affected. If the network is interrupted for more than 30 seconds, the DR task will fail. • If the DCC does not support instances with 4 vCPUs and 8 GB memory or higher instance specifications, the DR task cannot be created. • Resumable upload is supported, but data may be repeatedly inserted into a table that does not have a primary key. • If there is a DR task in a database, you are not allowed to create a migration or synchronization task (The database cannot be used as the source or destination database of the migration or synchronization task). • The DR relationship involves only one primary database. If the external database does not provide the superuser permission, it cannot be set to read-only when it acts as a standby database. Ensure that the data of the standby node is synchronized only from the primary node. Any other write operations will pollute the data in the standby database, data conflicts occur in the DR center and cannot be resolved. • If the external database is a standby and read-only database, only the account with the superuser permission can write data to that database. But you still need to ensure that data is written only by this account. Otherwise, the standby database may be polluted, and data conflicts occur in the DR center and cannot be resolved. • When DR occurs between an earlier version database and a later version database, service activities must be compatible

Type	Restrictions
	with both the earlier version and the later version. Otherwise, the DR may fail. • If the service database is an RDS for MySQL instance, tables encrypted using Transparent Data Encryption (TDE) cannot be synchronized. • Before creating a DRS task, if concurrency control rules of SQL statements are configured for the service or DR database, the DRS task may fail. • During disaster recovery, if the password of the service database is changed, the DR task will fail. To rectify the fault, you can correct the service database information on the DRS console and retry the task to continue disaster recovery. Generally, you are advised not to modify the preceding information during disaster recovery. • If the service database port is changed during disaster recovery, the DR task fails. Generally, you are advised not to modify the service database port during disaster recovery. • During disaster recovery, if the service database is on an RDS DB instance that does not belong the current cloud platform, the IP address cannot be changed. If the service database is an RDS DB instance on the current cloud and the DR task fails due to changes on the IP address, DRS automatically changes the IP address to the correct one. Then, you can retry the task to continue disaster recovery. Therefore, changing the IP address is not recommended. • During disaster recovery, you can create accounts for the service database. • During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal. • Do not write data to the source database during the primary/standby switchover. Otherwise, data pollution or table structure inconsistency may occur, resulting in data inconsistency between the service database and DR database.

Procedure

Step 1 On the **Disaster Recovery Management** page, click **Create Disaster Recovery Task**.

Step 2 On the **Create Disaster Recovery Instance** page, select a region and project, specify the task name, description, and the DR instance details, and click **Create Now**.

- Task information description

Figure 2-16 DR task information

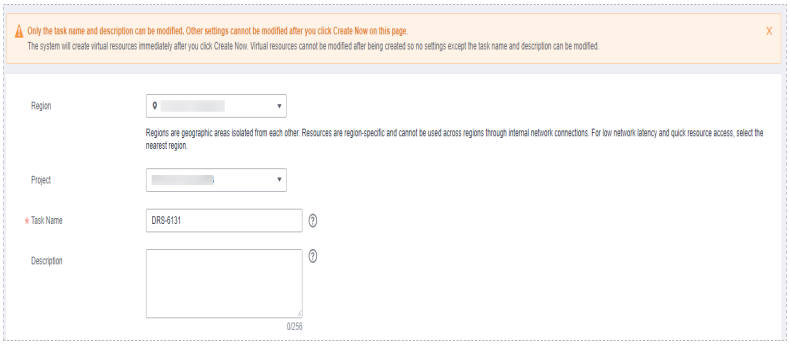


Table 2-17 Task and recipient description

Parameter	Description
Region	The region where your service is running. You can change the region.
Project	The project corresponds to the current region and can be changed.
Task Name	The task name must start with a letter and consist of 4 to 50 characters. It can contain only letters, digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters !=<>'&"\

- DR instance information

Figure 2-17 DR instance information

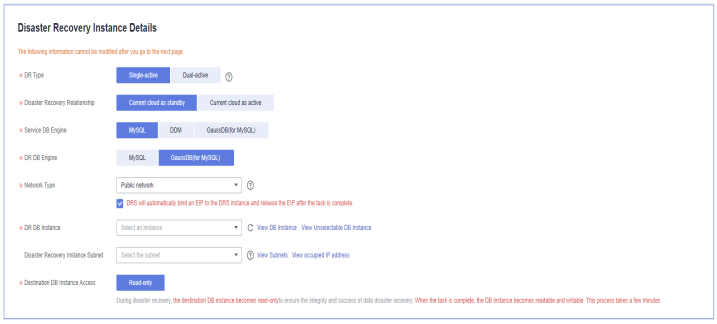


Table 2-18 DR instance settings

Parameter	Description
DR Type	Select **Single-active**. The DR type can be single-active or dual-active. If **Dual-active** is selected, two subtasks are created by default, a forward DR task and a backward DR task. **NOTE** Only whitelisted users can use dual-active DR. To use this function, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket.
Disaster Recovery Relationship	Select **Current cloud as standby**. This parameter is available only when you select **Single-active**. By default, **Current cloud as standby** is selected. You can also select **Current cloud as active**. – **Current cloud as standby**: The DR database is on the current cloud. – **Current cloud as active**: The service database is on the current cloud.
Service DB Engine	Select **MySQL**.
DR DB Engine	Select **GaussDB(for MySQL)**.
Network Type	The public network is used as an example. Available options: **VPN or Direct Connect** and **Public network**. By default, the value is **Public network**.
DR DB Instance	GaussDB(for MySQL) instance you have created as the destination database of the DR task.
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click **View Subnet** to go to the network console to view the subnet where the instance resides. By default, the DRS instance and the destination DB instance are in the same subnet. You need to select the subnet where the DRS instance resides and ensure that there are available IP addresses. To ensure that the disaster recovery instance is successfully created, only subnets with DHCP enabled are displayed.

Parameter	Description
Destination Database Access	Select **Read-only**. This parameter is available only when you select **Single-active**. – During disaster recovery, the entire DR database instance becomes read-only. To change the DR database to **Read/Write**, you can change the DR database (or destination database) to a service database by clicking **Promote Current Cloud** on the **Disaster Recovery Monitoring** tab. – After the DR task is complete, the DR database changes to **Read/Write**. – When the external database functions as the DR database, the user with the superuser permission can set the database to read-only. – If a DRS instance node is rebuilt due to a fault, to ensure data consistency during the DRS task restoration, the current cloud standby database is set to read-only before the task is restored. After the task is restored, the synchronization relationship recovers.

- Specifications

Figure 2-18 Specifications

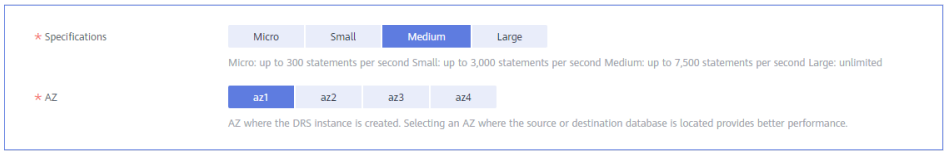


Table 2-19 Specifications

Parameter	Description
Specifications	DRS instance specifications. Different specifications have different performance upper limits. For details, see **Real-Time DR**. **NOTE** DRS allows you to upgrade specifications only for real-time DR tasks from MySQL to MySQL, from MySQL to GaussDB(for MySQL), and from GaussDB(for MySQL) to GaussDB(for MySQL). Task specifications cannot be downgraded. For details, see **Changing Specifications**.
AZ	Select the AZ where you want to create the DRS task. Selecting the one housing the source or destination database can provide better performance.

- Enterprise Project and Tags

Figure 2-19 Enterprise projects and tags

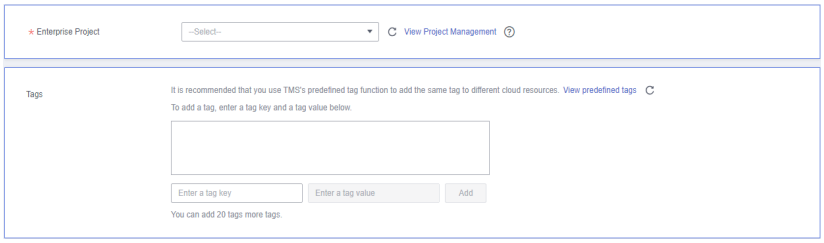


Table 2-20 Enterprise Project and Tags

Parameter	Description
Enterprise Project	An enterprise project you would like to use to centrally manage your cloud resources and members. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise projects, see ***Enterprise Management User Guide***. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Project Management Service** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.
Tags	– Tags a task. This configuration is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 20 tags. – After a task is created, you can view its tag details on the **Tags** tab. For details, see **Tag Management**.

NOTE

If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.

Step 3 On the **Configure Source and Destination Databases** page, wait until the DR instance is created. Then, specify source and destination database information and click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, select the check box before the agreement and click **Next**.

Figure 2-20 Service database information

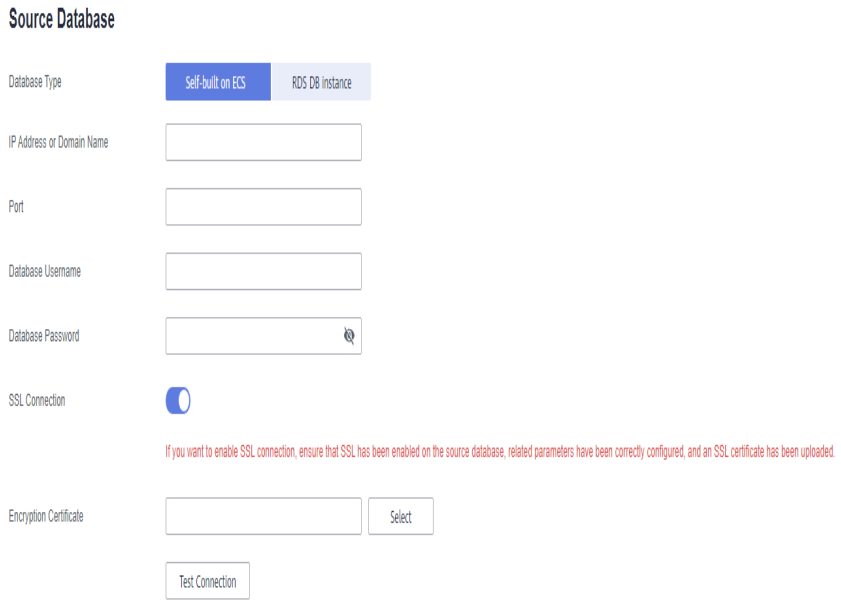


Table 2-21 Service database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The source database can be a **Self-built on ECS** or an **RDS DB instance**. After selecting **RDS DB instance**, select the region where the source database resides and the region cannot be the same as the region where the destination database resides. The region where the destination database is located is the region where you log in to the management console. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the service database.
Port	The port of the service database. Range: 1 – 65535
Database Username	The username for accessing the service database.
Database Password	The password for the service database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **Connection Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password.

Parameter	Description
SSL Connection	SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate. **NOTE** • The maximum size of a single certificate file that can be uploaded is 500 KB. • If SSL is disabled, your data may be at risk.
Region	The region where the service DB instance is located. This parameter is selected by default. This parameter is available only when the source database is an **RDS DB instance**.
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an **RDS DB instance**.
Database Username	The username for accessing the service database.
Database Password	The password for the service database username.

NOTE

The IP address, domain name, username, and password of the service database are encrypted and stored in DRS and will be cleared after the task is deleted.

Figure 2-21 DR database information

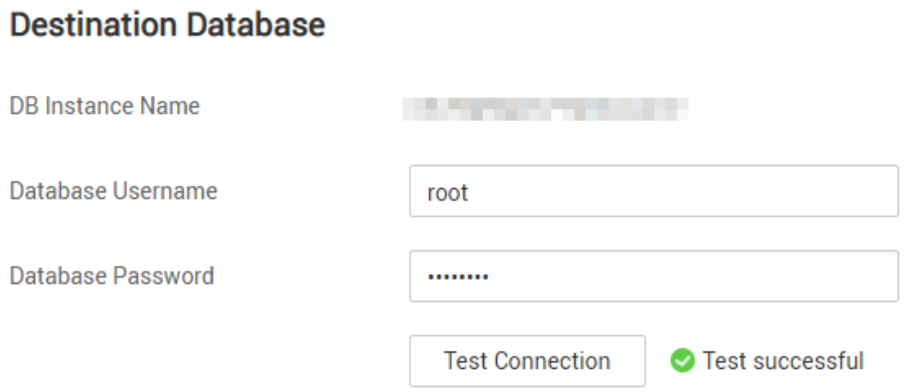


Table 2-22 DR database settings

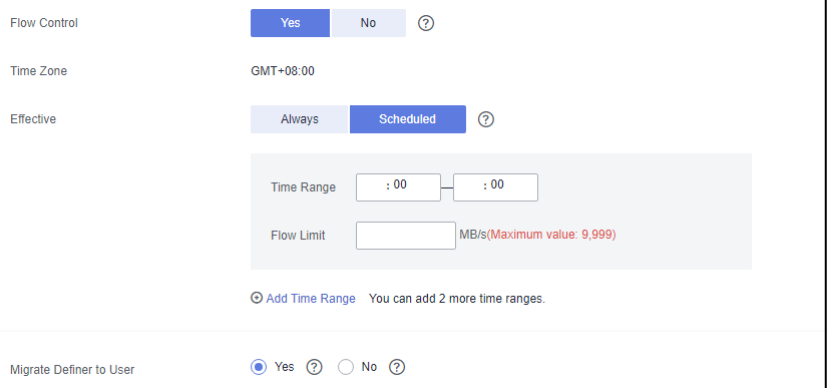
Parameter	Description
DB Instance Name	The GaussDB(for MySQL) instance you selected when creating the DR task. This parameter cannot be changed.

Parameter	Description
Database Username	The username for accessing the DR database.
Database Password	The password for the database username. The password can be changed after a task is created. If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **Connection Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.

Step 4 On the **Configure DR** page, specify flow control and click **Next**.

Figure 2-22 DR settings

Table 2-23 DR settings

Parameter	Description
Flow Control	You can choose whether to control the flow. • **Yes** You can customize the maximum DR speed. In addition, you can set the time range based on your service requirements. The traffic rate setting usually includes setting of a rate limiting time period and a traffic rate value. Flow can be controlled all day or during specific time ranges. The default value is **All day**. A maximum of three time ranges can be set, and they cannot overlap. The flow rate must be set based on the service scenario and cannot exceed 9,999 MB/s. **Figure 2-23** Flow control  • **No** The DR speed is not limited and the outbound bandwidth of the source database is maximally used, which causes read consumption on the source database accordingly. For example, if the outbound bandwidth of the source database is 100 MB/s and 80% bandwidth is used, the I/O consumption on the source database is 80 MB/s. **NOTE** – Flow control mode takes effect only in the DR initialization phase. – You can also change the flow control mode when the task is in the **Configuration** state. For details, see **Modifying the Flow Control Mode**.

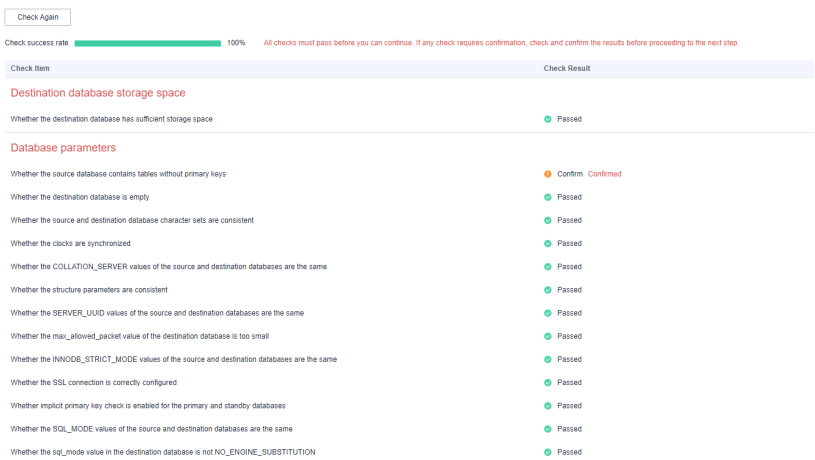
Parameter	Description
Migrate Definer to User	Indicates whether to migrate the Definers of all source database objects to the destination database user entered during the connection test. • Yes The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see **How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?** For example, if the view is CREATE ALGORITHM=UNDEFINED DEFINER=`username`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` before migration, it is converted to CREATE ALGORITHM=UNDEFINED DEFINER=`drsUser`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` after the migration. **drsUser** indicates the destination database user used for testing the connection. • **No** The Definers of all source database objects will not be changed. You need to migrate all accounts and permissions of the source database in the next step. Note that if the Definer account is not found in the destination database, unavailable objects will be created. For details about Definer, see the **MySQL official document**.

Step 5 On the **Check Task** page, check the DR task.

- If any check fails, review the failure cause and rectify the fault. After the fault is rectified, click **Check Again**.

  For details about how to handle check failures, see **Solutions to Failed Check Items** in *Data Replication Service User Guide*.

  Figure 2-24 Pre-check



- If the check is complete and the check success rate is 100%, click **Next**.

  NOTE

  You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

Step 6 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO Synchronization Delay Threshold**, **Stop Abnormal Tasks After** and DR instance details. Then, click **Submit**.

Figure 2-25 Task startup settings

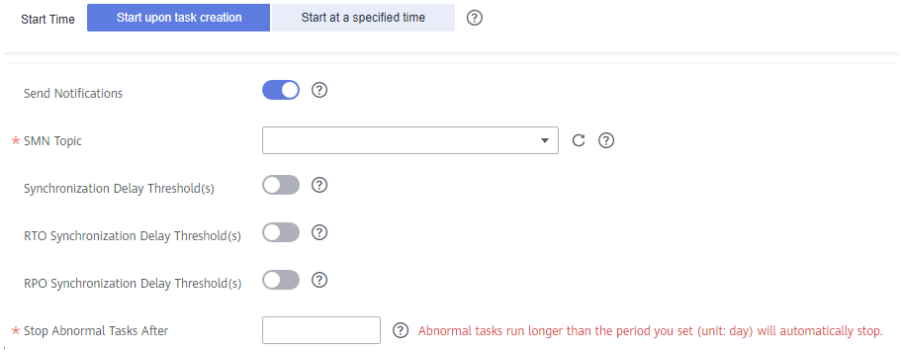


Table 2-24 Task and recipient description

Parameter	Description
Start Time	Set **Start Time** to **Start upon task creation** or **Start at a specified time** based on site requirements. **NOTE** Starting a DR task may slightly affect the performance of the service and DR databases. You are advised to start a DR task during off-peak hours.
Send Notifications	SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.
SMN Topic	This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber. For details, see **Simple Message Notification User Guide**.

Parameter	Description
Synchronization Delay Threshold	During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** ● Before setting the delay threshold, enable **Send Notification**. ● If the delay threshold is set to 0, no notifications will be sent to the recipient.
RTO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the DR database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** ● Before setting the RTO delay threshold, enable **Send Notification**. ● If the delay threshold is set to 0, no notifications will be sent to the recipient.
RPO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the service database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** ● Before setting the delay threshold, enable **Send Notification**. ● If the delay threshold is set to 0, no notifications will be sent to the recipient. ● In the early stages of an incremental disaster recovery, the synchronization delay is long because a large quantity of data is awaiting synchronization. In this case, no notifications will be sent.
Stop Abnormal Tasks After	Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is **14**. **NOTE** ● You can set this parameter only for pay-per-use tasks. ● Tasks in the abnormal state are still charged. If tasks remain in the abnormal state for a long time, they cannot be resumed. Abnormal tasks run longer than the period you set (unit: day) will automatically stop to avoid unnecessary fees.

Step 7 After the task is submitted, view and **manage it** on the **Disaster Recovery Management** page.

- You can view the task status. For more information about task status, see **Task Statuses**.
- You can click in the upper-right corner to view the latest task status.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.

----End

2.3 From DDM to DDM (Single-Active DR)

Supported Source and Destination Databases

Table 2-25 Supported databases

Service database	DR Database
DDM instances	DDM instances

Database Account Permission Requirements

To start a DR task, the service and DR database users must meet the requirements in the following table. Different types of DR tasks require different permissions. For details, see **Table 2-26**. DRS automatically checks the database account permissions in the pre-check phase and provides handling suggestions.

Table 2-26 Database account permission

Type	Permission Required
Service database user	The user of the service database must have at least one permission, for example, SELECT.
DR database user	The user of the DR database must have at least one permission, for example, SELECT.

NOTE

- You are advised to create an independent database account for DRS task connection to prevent task failures caused by database account password modification.
- After changing the account passwords for the service and DR databases, **modify the connection information** in the DRS task as soon as possible to prevent automatic retry after a task failure. Automatic retry will lock the database accounts.

Prerequisites

- **You have logged in to the DRS console.**
- Your account balance is greater than or equal to $0 USD.
- For details about the supported DB types and versions, see **Supported Databases**.
- If a subaccount is used to create a DRS task, ensure that an agency has been added. For details about how to create an agency, see **Agency Management**.

Suggestions

CAUTION

- During the DR initialization, do not perform DDL operations on the service database. Otherwise, the task may be abnormal.
- During DR initialization, ensure that no data is written to the DR database to ensure data consistency before and after DR.

- The success of DR depends on environment and manual operations. To ensure a smooth DR, perform a DR trial before you start the DR task to help you detect and resolve problems in advance.
- It is recommended that you start your DR task during off-peak hours to minimize the impact on your services.
  - If the bandwidth is not limited, initialization of DR will increase query workload of the source database by 50 MB/s and occupy 2 to 4 vCPUs.
  - To ensure data consistency, tables without a primary key may be locked for 3s during disaster recovery.
  - The data in the DR process may be locked by other transactions for a long period of time, resulting in read timeout.
  - If DRS concurrently reads data from a database, it will use about 6 to 10 sessions. The impact of the connections on services must be considered.
  - If you read a table, especially a large table, during DR, the exclusive lock on that table may be blocked.
  - For more information about the impact of DRS on databases, see **What Is the Impact of DRS on Source and Destination Databases?**
- Data-Level Comparison

  To obtain accurate comparison results, start data comparison at a specified time point during off-peak hours. If it is needed, select **Start at a specified time** for **Comparison Time**. Due to slight time difference and continuous operations on data, data inconsistency may occur, reducing the reliability and validity of the comparison results.

Precautions

Before creating a DR task, read the following precautions:

Table 2-27 Environment Constraints

Type	Restrictions
Disaster recovery objects	• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery. • Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery. • System tables are not supported. • Triggers and events do not support disaster recovery. • Disaster recovery cannot be configured for a specific service database. • Disaster recovery of DDM account permissions is not supported.
Service database configuration	• In the public network, EIPs must be bound to each DDM instance and the associated RDS for MySQL instance. • The binlog of the RDS for MySQL instance associated with the DDM instance must be enabled and uses the ROW format and GTID. • If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days. • The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_). • The table name in the service database cannot contain non-ASCII characters, or the following characters: '<>/\
DR database configuration	• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal. • The DR DB instance must have sufficient storage space. • The binlog and GTID of the RDS instance associated with the DDM instance must be enabled. • The minor version of the DR DDM instance must be the same as that of the service DDM instance. • The number of DDM DR instances must be the same as that of the RDS instances associated with the DDM service instance. • The sharding rules of the DDM DR instance must be the same as those of the DDMservice instance. You are advised to use the schema import and export functions to ensure sharding rule consistency.

Type	Restrictions
Precautions	• The parameter modification of the service database is not recorded in logs and is not synchronized to the DR database. Therefore, you need to modify the parameters after the DR database is promoted to the primary. • If a physically generated column in a table is generated based on a time type, the data in the column may be inconsistent. • The service database does not support point-in-time recovery (PITR). • Binlogs cannot be forcibly deleted. Otherwise, the DR task fails. • Resumable upload is supported, but data may be repeatedly inserted into a table that does not have a primary key. • If there is a DR task in a database, you are not allowed to create a migration or synchronization task (The database cannot be used as the source or destination database of the migration or synchronization task). • The DR relationship involves only one primary database. If the external database does not provide the superuser permission, it cannot be set to read-only when it acts as a standby database. Ensure that the data of the standby node is synchronized only from the primary node. Any other write operations will pollute the data in the standby database, data conflicts occur in the DR center and cannot be resolved. • The DDM DR database cannot create schemas automatically. You need to set the schema rules before disaster recovery. • After a task is created, you cannot add schemas to the service database or modify the old schema to associate with the new RDS DB instance. Otherwise, data cannot be backed up and restored or the task fails. • During DR, rebalance and reshard operations cannot be performed on DDM schemas. • During disaster recovery, if the password of the service database is changed, the DR task will fail. To rectify the fault, you can correct the service database information on the DRS console and retry the task to continue disaster recovery. Generally, you are advised not to modify the preceding information during disaster recovery. • If the service database port is changed during disaster recovery, the DR task fails. Generally, you are advised not to modify the service database port during disaster recovery. • During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal. • Do not write data to the source database during the primary/standby switchover. Otherwise, data pollution or table

Type	Restrictions
	structure inconsistency may occur, resulting in data inconsistency between the service database and DR database.

Procedure

Step 1 On the **Disaster Recovery Management** page, click **Create Disaster Recovery Task**.

Step 2 On the **Create Disaster Recovery Instance** page, select a region and project, specify the task name, description, and the DR instance details, and click **Create Now**.

- Task information description

Figure 2-26 DR task information

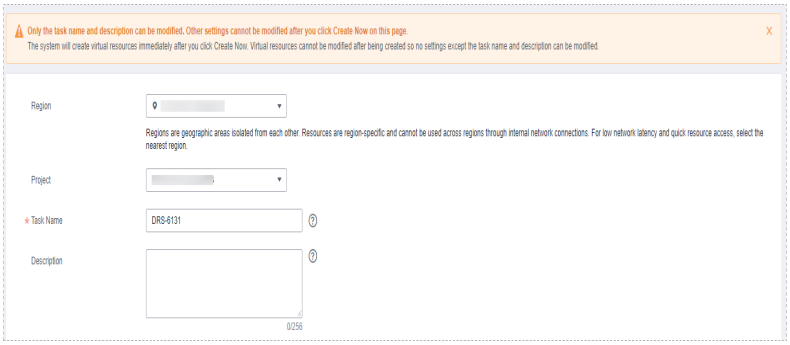


Table 2-28 Task and recipient description

Parameter	Description
Region	The region where your service is running. You can change the region.
Project	The project corresponds to the current region and can be changed.
Task Name	The task name must start with a letter and consist of 4 to 50 characters. It can contain only letters, digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters !=<>'&"\

- DR instance information

Figure 2-27 DR instance information

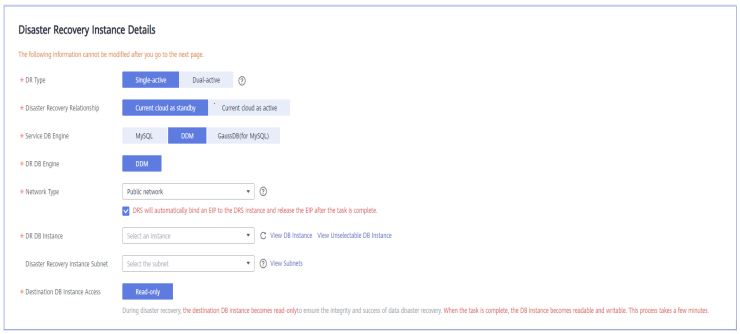


Table 2-29 DR instance settings

Parameter	Description
DR Type	Select **Single-active**. The DR type can be single-active or dual-active. If **Dual-active** is selected, two subtasks are created by default, a forward DR task and a backward DR task. **NOTE** Only whitelisted users can use dual-active DR. To use this function, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket.
Disaster Recovery Relationship	Select **Current cloud as standby**. This parameter is available only when you select **Single-active**. By default, **Current cloud as standby** is selected. You can also select **Current cloud as active**. – **Current cloud as standby**: The DR database is on the current cloud. – **Current cloud as active**: The service database is on the current cloud.
Service DB Engine	Select **DDM**.
DR DB Engine	Select **DDM**.
Network Type	The public network is used as an example. Available options: **VPN or Direct Connect** and **Public network**. By default, the value is **Public network**.
DR DB Instance	The DDM instance you created.

Parameter	Description
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click **View Subnet** to go to the network console to view the subnet where the instance resides. By default, the DRS instance and the destination DB instance are in the same subnet. You need to select the subnet where the DRS instance resides and ensure that there are available IP addresses. To ensure that the disaster recovery instance is successfully created, only subnets with DHCP enabled are displayed.
Destination Database Access	Select **Read-only**. This parameter is available only when you select **Single-active**. – During disaster recovery, the entire DR database instance becomes read-only. To change the DR database to Read/Write, you can change the DR database (or destination database) to a service database by clicking **Batch Operation > Primary/Standby Switchover** on the **Disaster Recovery Management** page. – After the DR task is complete, the DR database changes to **Read/Write**. – When the external database functions as the DR database, the user with the superuser permission can set the database to read-only. – If a DRS instance node is rebuilt due to a fault, to ensure data consistency during the DRS task restoration, the current cloud standby database is set to read-only before the task is restored. After the task is restored, the synchronization relationship recovers.

- AZ

Figure 2-28 AZ

Table 2-30 Task AZ

Parameter	Description
AZ	Select the AZ where you want to create the DRS task. Selecting the one housing the source or destination database can provide better performance.

- Enterprise Project and Tags

Figure 2-29 Enterprise projects and tags

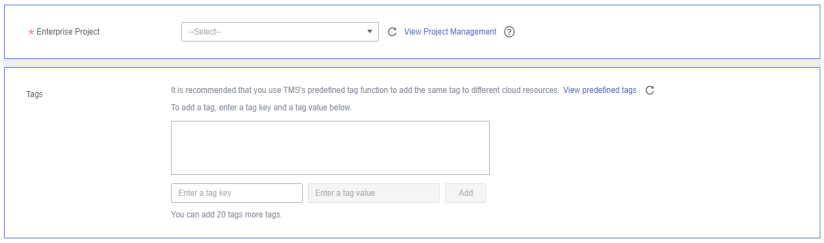


Table 2-31 Enterprise Project and Tags

Parameter	Description
Enterprise Project	An enterprise project you would like to use to centrally manage your cloud resources and members. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise projects, see ***Enterprise Management User Guide***. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Project Management Service** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.
Tags	– Tags a task. This configuration is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 20 tags. – After a task is created, you can view its tag details on the **Tags** tab. For details, see **Tag Management**.

NOTE

If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.

Step 3 On the **Configure Source and Destination Databases** page, wait until the DR instance is created. Then, specify source and destination database information and click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, select the check box before the agreement and click **Next**.

- Select **Current cloud as the standby** for **Disaster Recovery Relationship** in **Step 2**.

Figure 2-30 Service database information

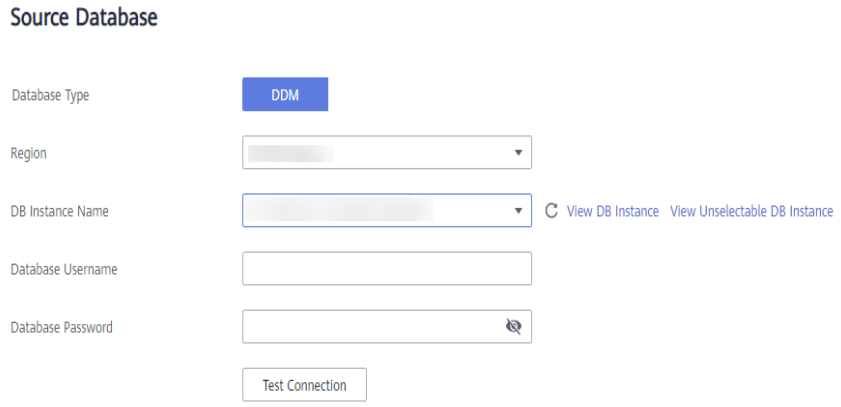


Table 2-32 Service database settings

Parameter	Description
Database Type	Select a service database type.
Region	Indicates the region where the service DB instance is located. The region cannot be the current login region.
DB Instance Name	The name of the service DB instance.
Database Username	The username for accessing the service database.
Database Password	The password for the service database username.

NOTE

The IP address, domain name, username, and password of the service database are encrypted and stored in DRS and will be cleared after the task is deleted.

Figure 2-31 DR database information

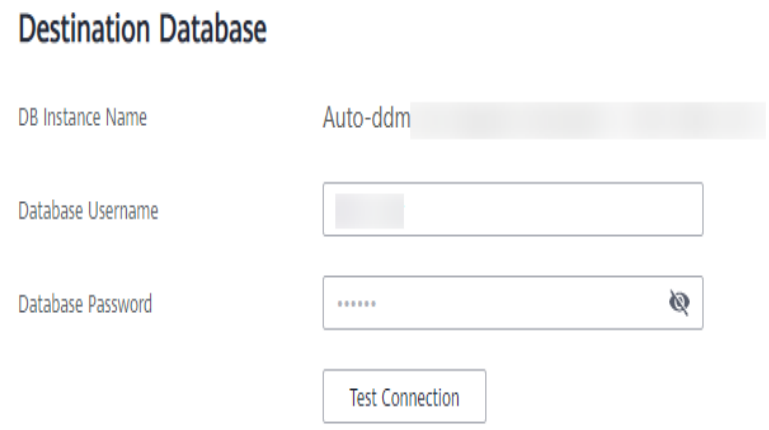


Table 2-33 DR database settings

Parameter	Description
DB Instance Name	The DDM instance you selected when you create the DR task. The instance name cannot be changed.
Database Username	The username for accessing the DR database.
Database Password	The password for the database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in the system, and will be cleared after the task is deleted.

- Select **Current cloud as active** for **Disaster Recovery Relationship** in **Step 2**.

  Figure 2-32 Service database information

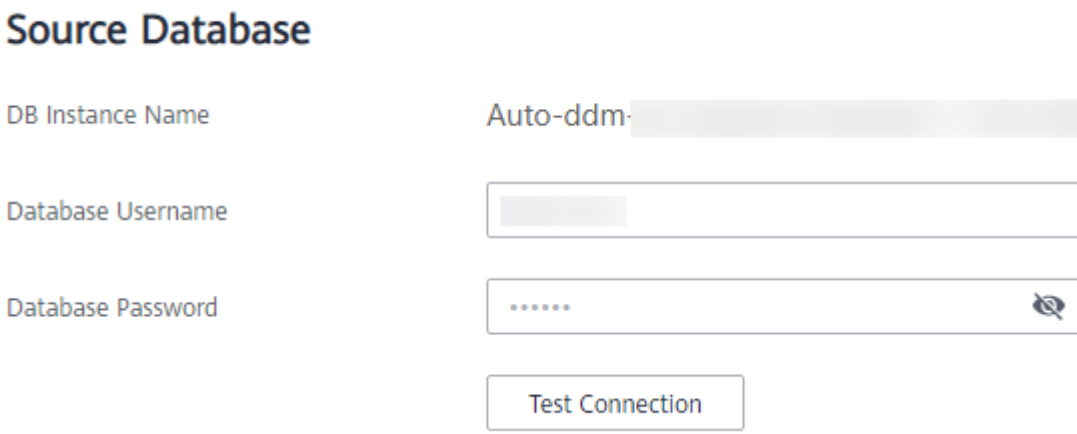
  

  Table 2-34 Service database settings

Parameter	Description
DB Instance Name	The DDM instance you selected when you create the DR task. The instance name cannot be changed.

Parameter	Description
Database Username	The username for accessing the service database.
Database Password	The password for the database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in the system, and will be cleared after the task is deleted.

Figure 2-33 DR database information

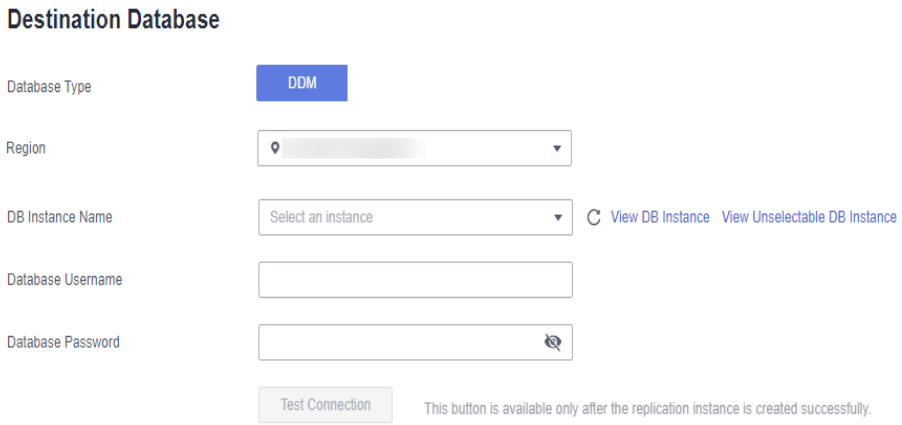


Table 2-35 DR database settings

Parameter	Description
Database Type	Type of the DR database.
Region	The region where the DDM instance is located.
DB Instance Name	Name of the DR instance. **NOTE** When the DB instance is used as the DR database, it is set to read-only. After the task is complete, the DB instance can be readable and writable.
Database Username	Username for logging in to the DR database.

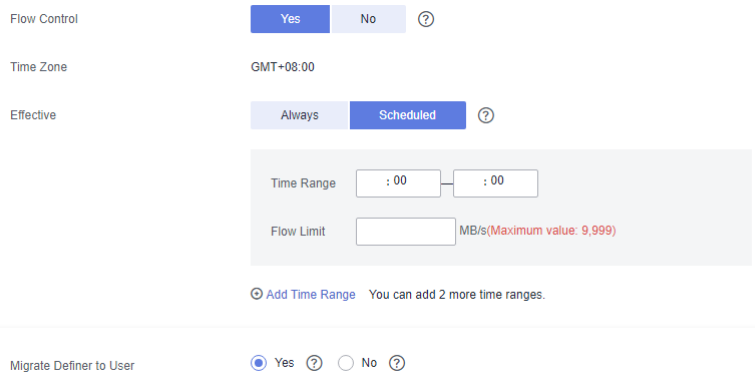
Parameter	Description
Database Password	Password for the database username.

NOTE

The username and password of the DR databases are encrypted and stored in DRS, and will be cleared after the task is deleted.

Step 4 On the **Configure DR** page, specify flow control and click **Next**.

Table 2-36 DR settings

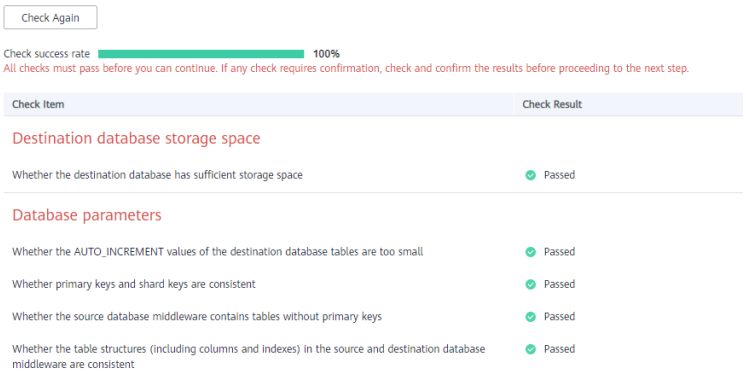
Parameter	Description
Flow Control	You can choose whether to control the flow. • **Yes** You can customize the maximum DR speed. In addition, you can set the time range based on your service requirements. The traffic rate setting usually includes setting of a rate limiting time period and a traffic rate value. Flow can be controlled all day or during specific time ranges. The default value is **All day**. A maximum of three time ranges can be set, and they cannot overlap. The flow rate must be set based on the service scenario and cannot exceed 9,999 MB/s. **Figure 2-34** Flow control  • **No** The DR speed is not limited and the outbound bandwidth of the source database is maximally used, which causes read consumption on the source database accordingly. For example, if the outbound bandwidth of the source database is 100 MB/s and 80% bandwidth is used, the I/O consumption on the source database is 80 MB/s. **NOTE** – Flow control mode takes effect only in the DR initialization phase. – You can also change the flow control mode when the task is in the **Configuration** state. For details, see **Modifying the Flow Control Mode**.

Step 5 On the **Check Task** page, check the DR task.

- If any check fails, review the failure cause and rectify the fault. After the fault is rectified, click **Check Again**.

  For details about how to handle check failures, see **Solutions to Failed Check Items** in *Data Replication Service User Guide*.

Figure 2-35 Pre-check



- If the check is complete and the check success rate is 100%, click **Next**.

  NOTE

  You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

Step 6 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO Synchronization Delay Threshold**, **Stop Abnormal Tasks After** and DR instance details. Then, click **Submit**.

Figure 2-36 Task startup settings

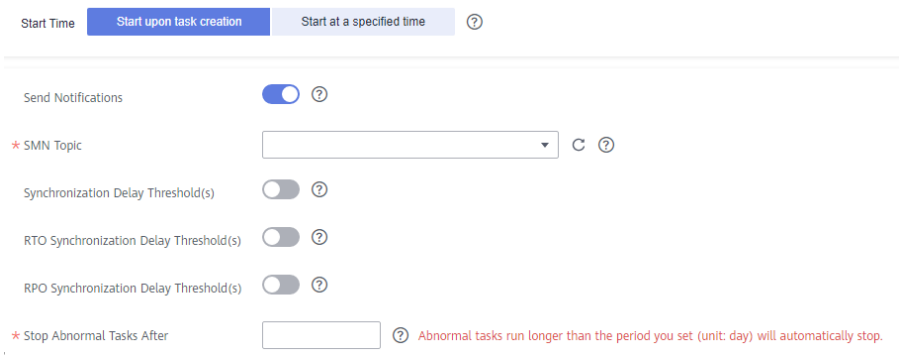


Table 2-37 Task and recipient description

Parameter	Description
Start Time	Set **Start Time** to **Start upon task creation** or **Start at a specified time** based on site requirements. **NOTE** Starting a DR task may slightly affect the performance of the service and DR databases. You are advised to start a DR task during off-peak hours.
Send Notifications	SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.

Parameter	Description
SMN Topic	This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber. For details, see **Simple Message Notification User Guide**.
Synchronization Delay Threshold	During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RTO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the DR database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the RTO delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RPO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the service database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient. • In the early stages of an incremental disaster recovery, the synchronization delay is long because a large quantity of data is awaiting synchronization. In this case, no notifications will be sent.

Parameter	Description
Stop Abnormal Tasks After	Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is **14**. **NOTE** • You can set this parameter only for pay-per-use tasks. • Tasks in the abnormal state are still charged. If tasks remain in the abnormal state for a long time, they cannot be resumed. Abnormal tasks run longer than the period you set (unit: day) will automatically stop to avoid unnecessary fees.

Step 7 After the task is submitted, view and **manage it** on the **Disaster Recovery Management** page.

- You can view the task status. For more information about task status, see **Task Statuses**.
- You can click in the upper-right corner to view the latest task status.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.

----End

2.4 From GaussDB(for MySQL) to GaussDB(for MySQL) (Single-Active DR)

Supported Source and Destination Databases

Table 2-38 Supported databases

Service database	DR Database
GaussDB(for MySQL)	GaussDB(for MySQL)

Database Account Permission Requirements

To start a DR task, the service and DR database users must meet the requirements in the following table. Different types of DR tasks require different permissions. For details, see **Table 2-39**. DRS automatically checks the database account permissions in the pre-check phase and provides handling suggestions.

Table 2-39 Database account permission

Type	Permission Required
Service database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION The **root** account of the GaussDB(for MySQL) instance has the preceding permissions by default.
DR database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION The **root** account of the GaussDB(for MySQL) instance has the preceding permissions by default.

NOTE

- You are advised to create an independent database account for DRS task connection to prevent task failures caused by database account password modification.
- After changing the account passwords for the service and DR databases, **modify the connection information** in the DRS task as soon as possible to prevent automatic retry after a task failure. Automatic retry will lock the database accounts.
- **Table 2-39** lists the minimum permissions required by a DRS task. If you need to migrate the grant permission through a DRS task, ensure that the connection account of the DRS task has the corresponding permission. Otherwise, the destination database user may not be authorized due to grant execution failure. For example, if the connection account of the DRS task does not require the process permission, but you need to migrate the process permission through a DRS task, ensure that the connection account of the DRS task has the process permission.

Prerequisites

- **You have logged in to the DRS console.**
- Your account balance is greater than or equal to $0 USD.
- For details about the supported DB types and versions, see **Supported Databases**.
- If a subaccount is used to create a DRS task, ensure that an agency has been added. For details about how to create an agency, see **Agency Management**.

Suggestions

CAUTION

- During the DR initialization, do not perform DDL operations on the service database. Otherwise, the task may be abnormal.
- During DR initialization, ensure that no data is written to the DR database to ensure data consistency before and after DR.

- The success of DR depends on environment and manual operations. To ensure a smooth DR, perform a DR trial before you start the DR task to help you detect and resolve problems in advance.
- It is recommended that you start your DR task during off-peak hours to minimize the impact on your services.
  - If the bandwidth is not limited, initialization of DR will increase query workload of the source database by 50 MB/s and occupy 2 to 4 vCPUs.
  - To ensure data consistency, tables without a primary key may be locked for 3s during disaster recovery.
  - The data in the DR process may be locked by other transactions for a long period of time, resulting in read timeout.
  - If DRS concurrently reads data from a database, it will use about 6 to 10 sessions. The impact of the connections on services must be considered.
  - If you read a table, especially a large table, during DR, the exclusive lock on that table may be blocked.
  - For more information about the impact of DRS on databases, see **What Is the Impact of DRS on Source and Destination Databases?**
- Data-Level Comparison

  To obtain accurate comparison results, start data comparison at a specified time point during off-peak hours. If it is needed, select **Start at a specified time** for **Comparison Time**. Due to slight time difference and continuous operations on data, data inconsistency may occur, reducing the reliability and validity of the comparison results.

Precautions

Before creating a DR task, read the following precautions:

Table 2-40 Precautions

Type	Restrictions
Disaster recovery objects	• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery. • System tables are not supported. • Triggers and events do not support disaster recovery. • Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery. • Disaster recovery cannot be configured for a specific service database.
Service database configuration	• The service database must be the primary node of the GaussDB(for MySQL) instance. • The binlog of the service database must be enabled and use the row-based format. • If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days. • GTID must be enabled for the database. • The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_). • The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '<>/\
DR database configuration	• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal. • The DR DB instance must have sufficient storage space. • The major version of the DR database must be the same as that of the service database. • The DR database must be an empty instance. After the DR task starts, the DR database is set to read-only. • The binlog of the DR database must be enabled and use the row-based format. • GTID must be enabled for the DR database.

Type	Restrictions
Precautions	• The parameter modification of the service database is not recorded in logs and is not synchronized to the DR database. Therefore, you need to modify the parameters after the DR database is promoted to the primary. • Before creating a DRS task, if concurrency control rules of SQL statements are configured for the service or DR database, the DRS task may fail. • If a physically generated column in a table is generated based on a time type, the data in the column may be inconsistent. • Cascade operations cannot be performed on tables with foreign keys. If the foreign key index of a table is a common index, the table structure may fail to be created. You are advised to use a unique index. • The service database does not support point-in-time recovery (PITR). • Binlogs cannot be forcibly deleted. Otherwise, the DR task fails. • The service database does not support the **reset master** or **reset master to** command, which may cause DRS task failures or data inconsistency. • If the network is reconnected within 30 seconds, disaster recovery will not be affected. If the network is interrupted for more than 30 seconds, the DR task will fail. • If the DCC does not support instances with 4 vCPUs and 8 GB memory or higher instance specifications, the DR task cannot be created. • Resumable upload is supported, but data may be repeatedly inserted into a table that does not have a primary key. • If there is a DR task in a database, you are not allowed to create a migration or synchronization task (The database cannot be used as the source or destination database of the migration or synchronization task). • The DR relationship involves only one primary database. Ensure that the data of the standby node is synchronized only from the primary node. Any other write operations will pollute the data in the standby database, data conflicts occur in the DR center and cannot be resolved. • If the external database is a standby and read-only database, only the account with the superuser permission can write data to that database. But you still need to ensure that data is written only by this account. Otherwise, the standby database may be polluted, and data conflicts occur in the DR center and cannot be resolved. • During disaster recovery, if the password of the service database is changed, the DR task will fail. To rectify the fault, you can correct the service database information on the DRS

Type	Restrictions
	console and retry the task to continue disaster recovery. Generally, you are advised not to modify the preceding information during disaster recovery. • If the service database port is changed during disaster recovery, the DR task fails. Generally, you are advised not to modify the service database port during disaster recovery. • During disaster recovery, if the service database is an RDS DB instance on the current cloud and the DR task fails due to changes on the IP address, DRS automatically changes the IP address to the correct one. Then, you can retry the task to continue disaster recovery. Therefore, changing the IP address is not recommended. • During disaster recovery, you can create accounts for the service database. • During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal. • Do not write data to the source database during the primary/standby switchover. Otherwise, data pollution or table structure inconsistency may occur, resulting in data inconsistency between the service database and DR database.

Procedure

Step 1 On the **Disaster Recovery Management** page, click **Create Disaster Recovery Task**.

Step 2 On the **Create Disaster Recovery Instance** page, select a region and project, specify the task name, description, and the DR instance details, and click **Create Now**.

- Task information description

Figure 2-37 DR task information

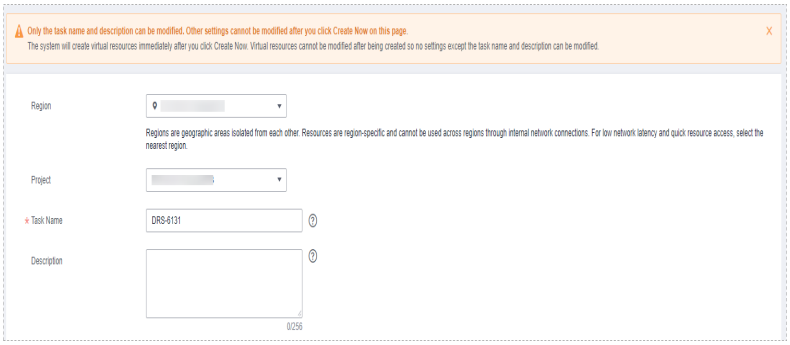


Table 2-41 Task and recipient description

Parameter	Description
Region	The region where your service is running. You can change the region.
Project	The project corresponds to the current region and can be changed.
Task Name	The task name must start with a letter and consist of 4 to 50 characters. It can contain only letters, digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters !=<>'&"\

- DR instance information

Figure 2-38 DR instance information

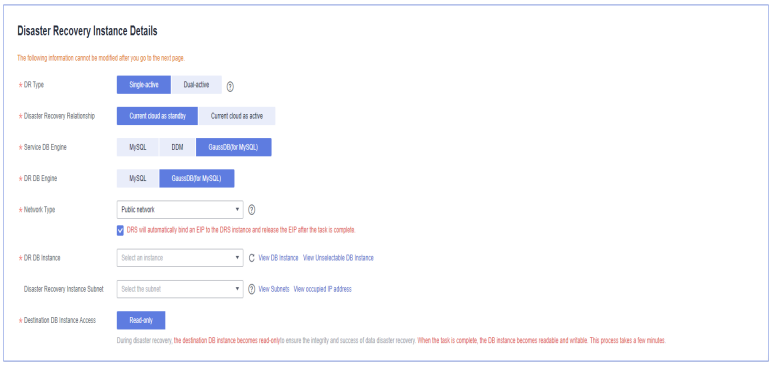


Table 2-42 DR instance settings

Parameter	Description
DR Type	Select **Single-active**. The DR type can be single-active or dual-active. If **Dual-active** is selected, two subtasks are created by default, a forward DR task and a backward DR task. **NOTE** Only whitelisted users can use dual-active DR. To use this function, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket.

Parameter	Description
Disaster Recovery Relationship	Select **Current cloud as standby**. This parameter is available only when you select **Single-active**. By default, **Current cloud as standby** is selected. You can also select **Current cloud as active**. – **Current cloud as standby**: The DR database is on the current cloud. – **Current cloud as active**: The service database is on the current cloud.
Service DB Engine	Select **GaussDB(for MySQL)**.
DR DB Engine	Select **GaussDB(for MySQL)**.
Network Type	The public network is used as an example. Available options: **VPN or Direct Connect** and **Public network**. By default, the value is **Public network**.
DR DB Instance	The GaussDB(for MySQL) instance you created.
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click **View Subnet** to go to the network console to view the subnet where the instance resides. By default, the DRS instance and the destination DB instance are in the same subnet. You need to select the subnet where the DRS instance resides and ensure that there are available IP addresses. To ensure that the disaster recovery instance is successfully created, only subnets with DHCP enabled are displayed.
Destination Database Access	Select **Read-only**. This parameter is available only when you select **Single-active**. – During disaster recovery, the entire DR database instance becomes read-only. To change the DR database to **Read/Write**, you can change the DR database (or destination database) to a service database by clicking **Promote Current Cloud** on the **Disaster Recovery Monitoring** tab. – After the DR task is complete, the DR database changes to **Read/Write**. – When the external database functions as the DR database, the user with the superuser permission can set the database to read-only. – If a DRS instance node is rebuilt due to a fault, to ensure data consistency during the DRS task restoration, the current cloud standby database is set to read-only before the task is restored. After the task is restored, the synchronization relationship recovers.

- Specifications

Figure 2-39 Specifications

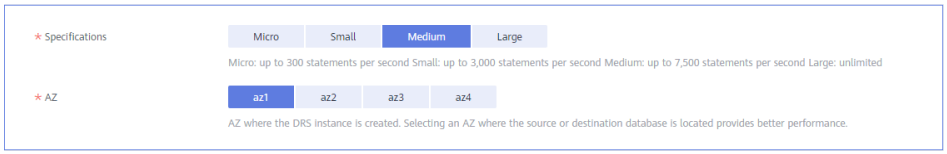


Table 2-43 Specifications

Parameter	Description
Specifications	DRS instance specifications. Different specifications have different performance upper limits. For details, see **Real-Time DR**. **NOTE** DRS allows you to upgrade specifications only for real-time DR tasks from MySQL to MySQL, from MySQL to GaussDB(for MySQL), and from GaussDB(for MySQL) to GaussDB(for MySQL). Task specifications cannot be downgraded. For details, see **Changing Specifications**.
AZ	Select the AZ where you want to create the DRS task. Selecting the one housing the source or destination database can provide better performance.

- Enterprise Project and Tags

Figure 2-40 Enterprise projects and tags

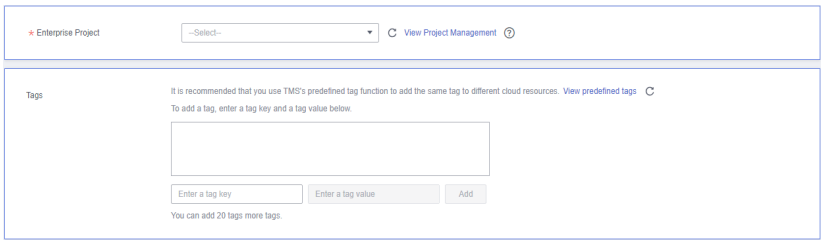


Table 2-44 Enterprise Project and Tags

Parameter	Description
Enterprise Project	An enterprise project you would like to use to centrally manage your cloud resources and members. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise projects, see ***Enterprise Management User Guide***. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Project Management Service** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.
Tags	– Tags a task. This configuration is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 20 tags. – After a task is created, you can view its tag details on the **Tags** tab. For details, see **Tag Management**.

NOTE

If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.

Step 3 On the **Configure Source and Destination Databases** page, wait until the DR instance is created. Then, specify source and destination database information and click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, select the check box before the agreement and click **Next**.

- Select **Current cloud as the standby** for **Disaster Recovery Relationship** in **Step 2**.

Figure 2-41 Service database information

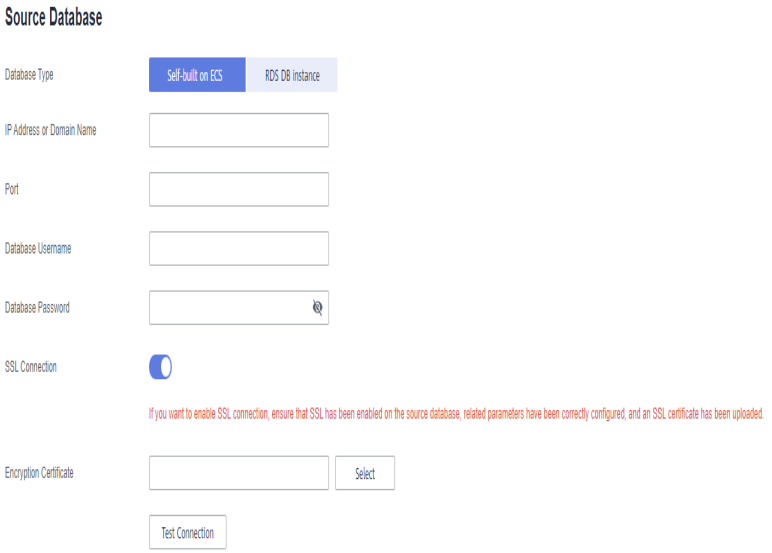


Table 2-45 Service database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The source database can be a **Self-built on ECS** or an **RDS DB instance**. After selecting **RDS DB instance**, select the region where the source database resides and the region cannot be the same as the region where the destination database resides. The region where the destination database is located is the region where you log in to the management console. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the service database.
Port	The port of the service database. Range: 1 – 65535
Database Username	The username for accessing the service database.
Database Password	The password for the service database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password.

Parameter	Description
SSL Connection	SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.
Region	The region where the service DB instance is located. This parameter is selected by default. This parameter is available only when the source database is an **RDS DB instance**.
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an **RDS DB instance**.
Database Username	The username for accessing the service database.
Database Password	The password for the service database username.

NOTE

The IP address, domain name, username, and password of the service database are encrypted and stored in DRS and will be cleared after the task is deleted.

Figure 2-42 DR database information

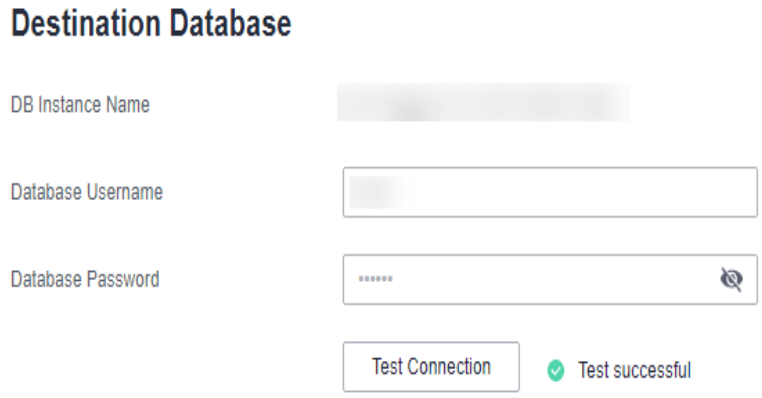


Table 2-46 DR database settings

Parameter	Description
DB Instance Name	The GaussDB(for MySQL) instance you selected when creating the DR task. This parameter cannot be changed.
Database Username	The username for accessing the DR database.
Database Password	The password for the database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in the system, and will be cleared after the task is deleted.

- Select **Current cloud as active** for **Disaster Recovery Relationship** in **Step 2**.

Figure 2-43 Service database information

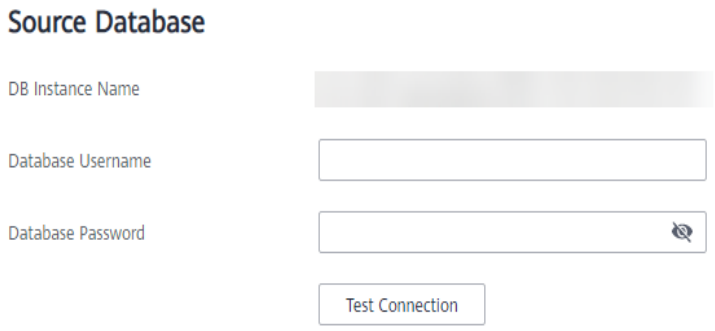


Table 2-47 Service database settings

Parameter	Description
DB Instance Name	The GaussDB(for MySQL) instance you selected when creating the DR task. This parameter cannot be changed.
Database Username	The username for accessing the service database.

Parameter	Description
Database Password	The password for the database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in the system, and will be cleared after the task is deleted.

Figure 2-44 DR database information

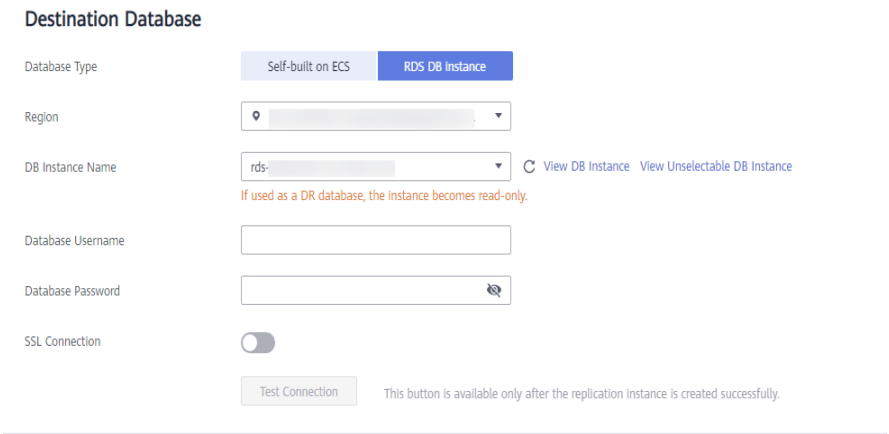


Table 2-48 DR database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The destination database can be a **Self-built on ECS** or an **RDS DB instance**. If you select **RDS DB instance**, you need to select the region where the destination database is located. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the DR database.
Port	The port of the DR database. Range: 1 – 65535
Database Username	The username for accessing the DR database.

Parameter	Description
Database Password	The password for the DR database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password.
SSL Connection	SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate. **NOTE** The maximum size of a single certificate file that can be uploaded is 500 KB.
Region	Region where the GaussDB(for MySQL) instance is located. This parameter is available only when the destination database is an RDS DB instance.
DB Instance Name	DR instance name. This parameter is available only when the destination database is an RDS DB instance. **NOTE** When the DB instance is used as the DR database, it is set to read-only. After the task is complete, the DB instance can be readable and writable.
Database Username	Username for logging in to the DR database.
Database Password	Password for the database username.

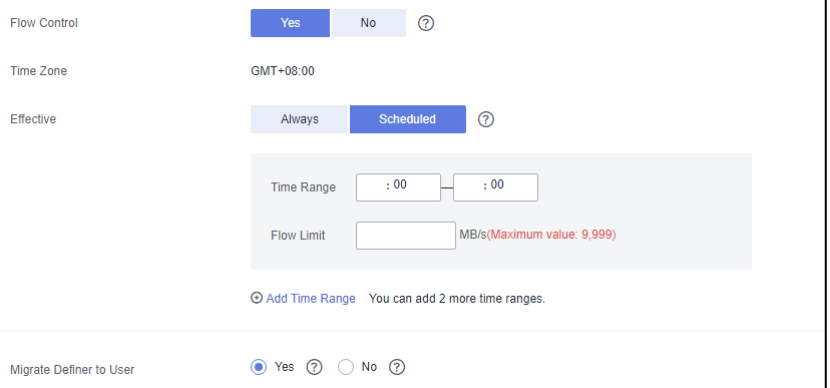
NOTE

The IP address, domain name, username, and password of the DR database are encrypted and stored in DRS and will be cleared after the task is deleted.

Step 4 On the **Configure DR** page, specify flow control and click **Next**.

Figure 2-45 DR settings

Table 2-49 DR settings

Parameter	Description
Flow Control	You can choose whether to control the flow. • **Yes** You can customize the maximum DR speed. In addition, you can set the time range based on your service requirements. The traffic rate setting usually includes setting of a rate limiting time period and a traffic rate value. Flow can be controlled all day or during specific time ranges. The default value is **All day**. A maximum of three time ranges can be set, and they cannot overlap. The flow rate must be set based on the service scenario and cannot exceed 9,999 MB/s. **Figure 2-46** Flow control  • **No** The DR speed is not limited and the outbound bandwidth of the source database is maximally used, which causes read consumption on the source database accordingly. For example, if the outbound bandwidth of the source database is 100 MB/s and 80% bandwidth is used, the I/O consumption on the source database is 80 MB/s. **NOTE** – Flow control mode takes effect only in the DR initialization phase. – You can also change the flow control mode when the task is in the **Configuration** state. For details, see **Modifying the Flow Control Mode**.

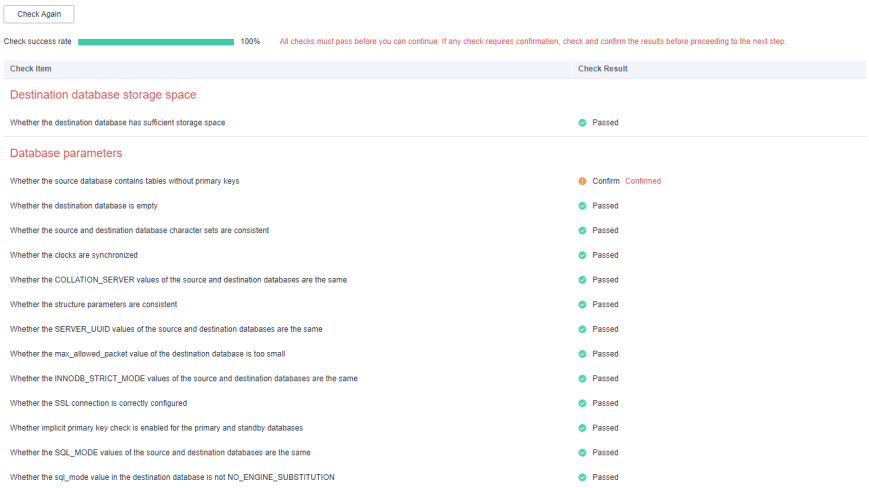
Parameter	Description
Migrate Definer to User	Indicates whether to migrate the Definers of all source database objects to the destination database user entered during the connection test. • Yes The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see **How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?** For example, if the view is CREATE ALGORITHM=UNDEFINED DEFINER=`username`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` before migration, it is converted to CREATE ALGORITHM=UNDEFINED DEFINER=`drsUser`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` after the migration. **drsUser** indicates the destination database user used for testing the connection. • **No** The Definers of all source database objects will not be changed. You need to migrate all accounts and permissions of the source database in the next step. Note that if the Definer account is not found in the destination database, unavailable objects will be created. For details about Definer, see the **MySQL official document**.

Step 5 On the **Check Task** page, check the DR task.

- If any check fails, review the failure cause and rectify the fault. After the fault is rectified, click **Check Again**.

  For details about how to handle check failures, see **Solutions to Failed Check Items** in *Data Replication Service User Guide*.

Figure 2-47 Pre-check



- If the check is complete and the check success rate is 100%, click **Next**.

  NOTE

  You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

Step 6 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO Synchronization Delay Threshold**, **Stop Abnormal Tasks After** and DR instance details. Then, click **Submit**.

Figure 2-48 Task startup settings

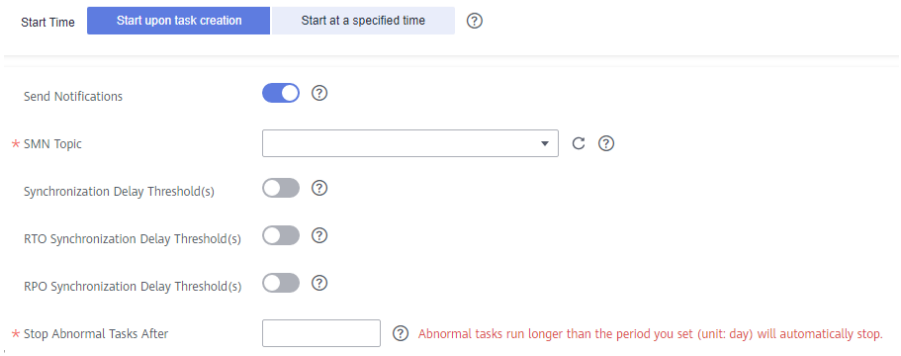


Table 2-50 Task and recipient description

Parameter	Description
Start Time	Set **Start Time** to **Start upon task creation** or **Start at a specified time** based on site requirements. **NOTE** Starting a DR task may slightly affect the performance of the service and DR databases. You are advised to start a DR task during off-peak hours.

Parameter	Description
Send Notifications	SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.
SMN Topic	This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber. For details, see **Simple Message Notification User Guide**.
Synchronization Delay Threshold	During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RTO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the DR database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the RTO delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RPO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the service database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient. • In the early stages of an incremental disaster recovery, the synchronization delay is long because a large quantity of data is awaiting synchronization. In this case, no notifications will be sent.

Parameter	Description
Stop Abnormal Tasks After	Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is **14**. **NOTE** • You can set this parameter only for pay-per-use tasks. • Tasks in the abnormal state are still charged. If tasks remain in the abnormal state for a long time, they cannot be resumed. Abnormal tasks run longer than the period you set (unit: day) will automatically stop to avoid unnecessary fees.

Step 7 After the task is submitted, view and **manage it** on the **Disaster Recovery Management** page.

- You can view the task status. For more information about task status, see **Task Statuses**.
- You can click in the upper-right corner to view the latest task status.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.

----End

2.5 From MySQL to MySQL (Dual-Active DR)

Supported Source and Destination Databases

Table 2-51 Supported databases

Service database	DR Database
• On-premises MySQL databases • MySQL databases on an ECS • MySQL databases on other clouds • RDS for MySQL	• RDS for MySQL

Database Account Permission Requirements

To start a DR task, the service and DR database users must meet the requirements in the following table. Different types of DR tasks require different permissions. For details, see **Table 2-52**. DRS automatically checks the database account permissions in the pre-check phase and provides handling suggestions.

Table 2-52 Database account permission

Type	Permission Required
Service database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION. The user **root** of the RDS for MySQL instance has the preceding permissions by default. If the service database version is 8.0.14 to 8.0.18, the SESSION_VARIABLES_ADMIN permission is required.
DR database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION. The user **root** of the RDS for MySQL instance has the preceding permissions by default. If the DR database version is 8.0.14 to 8.0.18, the SESSION_VARIABLES_ADMIN permission is required.

NOTE

- You are advised to create an independent database account for DRS task connection to prevent task failures caused by database account password modification.
- After changing the account passwords for the service and DR databases, **modify the connection information** in the DRS task as soon as possible to prevent automatic retry after a task failure. Automatic retry will lock the database accounts.
- **Table 2-52** lists the minimum permissions required by a DRS task. If you need to migrate the grant permission through a DRS task, ensure that the connection account of the DRS task has the corresponding permission. Otherwise, the destination database user may not be authorized due to grant execution failure. For example, if the connection account of the DRS task does not require the process permission, but you need to migrate the process permission through a DRS task, ensure that the connection account of the DRS task has the process permission.

Prerequisites

- **You have logged in to the DRS console.**
- Your account balance is greater than or equal to $0 USD.
- For details about the supported DB types and versions, see **Supported Databases**.
- If a subaccount is used to create a DRS task, ensure that an agency has been added. For details about how to create an agency, see **Agency Management**.

Suggestions

CAUTION

- During the DR initialization, do not perform DDL operations on the service database. Otherwise, the task may be abnormal.
- During DR initialization, ensure that no data is written to the DR database to ensure data consistency before and after DR.

- The success of DR depends on environment and manual operations. To ensure a smooth DR, perform a DR trial before you start the DR task to help you detect and resolve problems in advance.
- It is recommended that you start your DR task during off-peak hours to minimize the impact on your services.
  - If the bandwidth is not limited, initialization of DR will increase query workload of the source database by 50 MB/s and occupy 2 to 4 vCPUs.
  - To ensure data consistency, tables without a primary key may be locked for 3s during disaster recovery.
  - The data in the DR process may be locked by other transactions for a long period of time, resulting in read timeout.
  - If DRS concurrently reads data from a database, it will use about 6 to 10 sessions. The impact of the connections on services must be considered.
  - If you read a table, especially a large table, during DR, the exclusive lock on that table may be blocked.
  - For more information about the impact of DRS on databases, see **What Is the Impact of DRS on Source and Destination Databases?**
- Data-Level Comparison

  To obtain accurate comparison results, start data comparison at a specified time point during off-peak hours. If it is needed, select **Start at a specified time** for **Comparison Time**. Due to slight time difference and continuous operations on data, data inconsistency may occur, reducing the reliability and validity of the comparison results.

Precautions

Before creating a DR task, read the following precautions:

Table 2-53 Precautions

Type	Restrictions
Disaster recovery objects	• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery. • System tables are not supported. • Triggers and events do not support disaster recovery. • Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery. • DDL operations cannot be executed on the active database 2.
Service database configuration	• The binlog of the MySQL service database must be enabled and use the row-based format. • If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days. – For self-built MySQL databases, you can set the **expire_logs_days** parameter to specify the binlog retention period. – If the source database is an RDS for MySQL instance, set the binlog retention period by following the instructions provided in **RDS User Guide**. • The service database username or password cannot be empty. • **server_id** in the MySQL service database must be set. If the service database version is MySQL 5.6 or earlier, the **server_id** value ranges from **2** to **4294967296**. If the service database is MySQL 5.7 or later, the **server_id** value ranges from **1** to **4294967296**. • During disaster recovery, if the session variable **character_set_client** is set to **binary**, some data may include garbled characters. • GTID must be enabled for the database. • The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_). • The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '<>/\ • If the **expire_logs_days** value of the service database is set to **0**, the disaster recovery may fail. • If tables that have no primary key contain hidden primary keys in the service database, the DR task may fail or data may be inconsistent.

Type	Restrictions
DR database configuration	• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal. • The DR DB instance must have sufficient storage space. • The major version of the active database 1 must be the same as that of the active database 2. • The binlog of the DR database must be enabled and use the row-based format. • GTID must be enabled for the DR database. • In addition to the MySQL system database, the active database 2 must be an empty instance. After the forward task is started, active database 2 is set to read-only. After the backward task is started and DR is performed, the active database 2 is restored to read-write.

Type	Restrictions
Precautions	• Only whitelisted users can use this function. To use this function, submit a service ticket. • Dual-active DR supports backup in backward and forward directions. Due to certain uncontrollable factors, data may be inconsistent between the two sides. For example, if the load of active database 1 is too heavy and the load of active database 2 is light, data updates on the active database 1 synchronized to the active database 2 will be delayed due to the heave load, as a result, the operation sequence is changed and data becomes inconsistency. Therefore, divide data by unit (database, table, or row) and ensure the unit on one database is responsible for data read and write while on the other is read-only. In essence, in dual-active DR, both the databases play the active role but work differently. For details about common scenarios, see **Common Exceptions in Real-Time Disaster Recovery**. • Before creating a DRS task, if concurrency control rules of SQL statements are configured for the service or DR database, the DRS task may fail. • During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal. • During disaster recovery initialization, a lot of binlogs are generated in the DR database, occupying too much storage space. Therefore, during disaster recovery initialization, only the latest five binlogs are retained in the DR database by default. After the disaster recovery initialization is complete, the retention period of binlogs in the DR database is restored to the value you configure. If you want to keep the binlog retention period of the DR database to be the value you specify due to service requirements, you need to submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket. • During disaster recovery, you can create accounts for the service database. • If the same data on both databases is updated simultaneously, data conflicts may occur. DRS resolves the conflict by overwriting the previous settings with the last settings. – When the deletion operation is performed, data is deleted and DRS does not perform any operation. – When the insert operation is performed, DRS updates data with the latest inserted data. – When the update operation is performed, the original data has been updated and DRS directly insert the new data. • Primary key conflicts between the two sides need to be avoided. For example, you can use a UUID or the primary key rule of region+auto-increment ID to avoid conflicts.

Type	Restrictions
	• If the synchronization delay takes a long time due to connection interruption or network issues, you need to determine whether your services can tolerant the long-term delay. • Cascade operations cannot be performed on tables with foreign keys. If the foreign key index of a table is a common index, the table structure may fail to be created. You are advised to use a unique index. • If a physically generated column in a table is generated based on a time type, the data in the column may be inconsistent. • The dual-active DR is different from the single-active DR. Therefore, no active/standby switchover is required. • The DR latency is uncontrollable. Therefore, DDL operations must be performed when no service is running, and both RPO and RTO are zero and latency is kept within 30 seconds on active database 1. Do not perform DDL operations on active database 2. (DRS synchronizes only the DDL operations on active database 1 to active database 2.) • Ensure that the tables, columns, and rows are consistent in both the databases. (The table structures of both the active databases are consistent.) • A backward task can be started only when the forward task is in the DR process and both RPO and RTO are less than 60s. • After the dual-active DR task is in the DR process, perform tests on the active database 2 first. If the test results meet the requirements, switch certain service traffic to the active database 2.

Procedure

Step 1 On the **Disaster Recovery Management** page, click **Create Disaster Recovery Task**.

Step 2 On the **Create Disaster Recovery Instance** page, select a region and project, specify the task name, description, and the DR instance details, and click **Create Now**.

- Task information description

Figure 2-49 DR task information

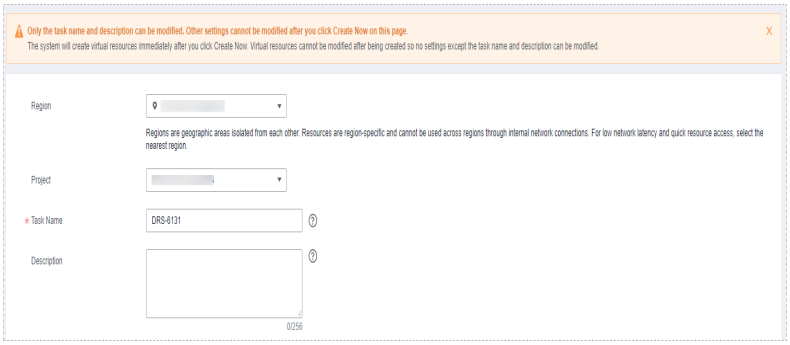


Table 2-54 Task and recipient description

Parameter	Description
Region	The region where your service is running. You can change the region.
Project	The project corresponds to the current region and can be changed.
Task Name	The task name must start with a letter and consist of 4 to 50 characters. It can contain only letters, digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters !=<>'&"\

- DR instance information

Figure 2-50 DR instance information

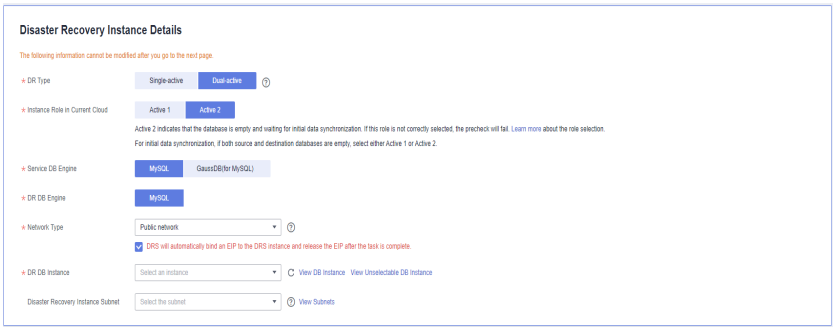


Table 2-55 DR instance settings

Parameter	Description
DR Type	Select **Dual-active**. The DR type can be single-active or dual-active. If **Dual-active** is selected, two subtasks are created by default, a forward DR task and a backward DR task. **NOTE** Only whitelisted users can use dual-active DR. To use this function, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket.
Current Cloud RDS Instance Role	Select **Active 1** or **Active 2**. This parameter specifies the role of the current RDS DB instance in the DR relationship and is available when **DR Type** is set to **Dual-active**. For details, see **How Do I Select Active Database 1 and 2 for Dual-Active DR?** – Active 1: Initial data is available on the current cloud RDS when a task is created. – Active 2: The RDS DB instance on the current cloud is empty when a task is created. Active 2 is used as an example.
Service DB Engine	Select **MySQL**.
DR DB Engine	Select **MySQL**.
Network Type	The public network is used as an example. Available options: **VPN or Direct Connect** and **Public network**. By default, the value is **Public network**.
DR DB Instance	The RDS for MySQL instance you created.
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click **View Subnet** to go to the network console to view the subnet where the instance resides. By default, the DRS instance and the destination DB instance are in the same subnet. You need to select the subnet where the DRS instance resides and ensure that there are available IP addresses. To ensure that the DR instance can be successfully created, only subnets with DHCP enabled are displayed.

- Specifications

Figure 2-51 Specifications

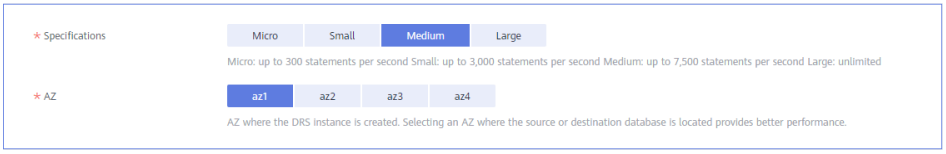


Table 2-56 Specifications

Parameter	Description
Specifications	DRS instance specifications. Different specifications have different performance upper limits. For details, see **Real-Time DR**. **NOTE** DRS allows you to upgrade specifications only for real-time DR tasks from MySQL to MySQL, from MySQL to GaussDB(for MySQL), and from GaussDB(for MySQL) to GaussDB(for MySQL). Task specifications cannot be downgraded. For details, see **Changing Specifications**.
AZ	Select the AZ where you want to create the DRS task. Selecting the one housing the source or destination database can provide better performance.

- Enterprise Project and Tags

Figure 2-52 Enterprise projects and tags

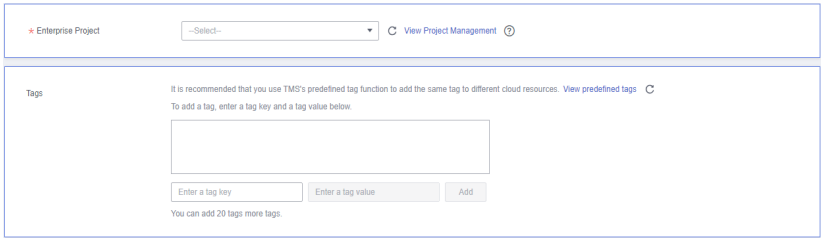


Table 2-57 Enterprise Project and Tags

Parameter	Description
Enterprise Project	An enterprise project you would like to use to centrally manage your cloud resources and members. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise projects, see ***Enterprise Management User Guide***. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Project Management Service** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.

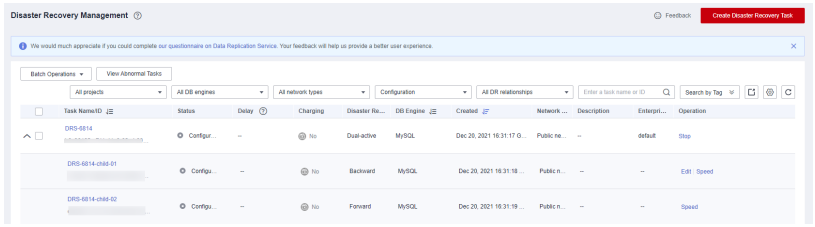
Parameter	Description
Tags	– Tags a task. This configuration is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 20 tags. – After a task is created, you can view its tag details on the **Tags** tab. For details, see **Tag Management**.

NOTE

If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.

Step 3 On the **Disaster Recovery Management** page, after the task is created, locate the forward subtask and click **Edit** in the **Operation** column. The **Configure Source and Destination Databases** page is displayed.

Figure 2-53 DR task list



Step 4 On the **Configure Source and Destination Databases** page, wait until the DR instance is created. Then, specify source and destination database information and click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, select the check box before the agreement and click **Next**.

Figure 2-54 Service database information

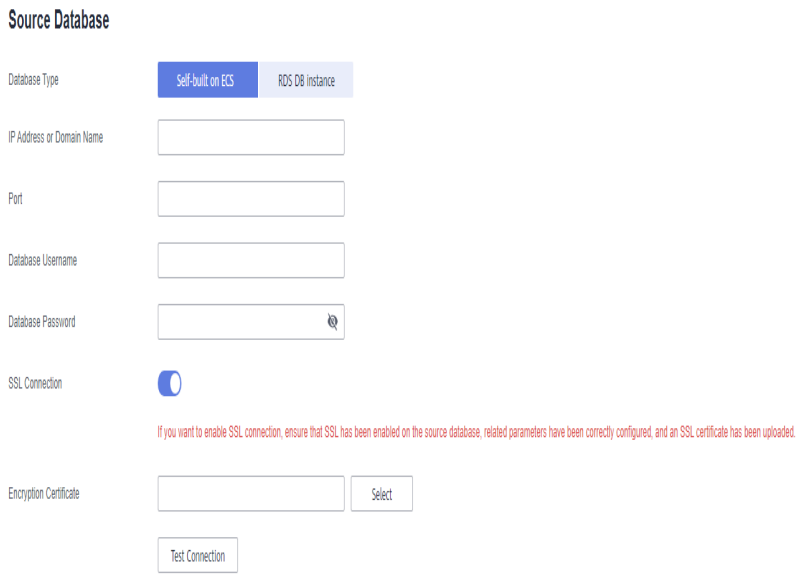


Table 2-58 Service database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The source database can be a **Self-built on ECS** or an **RDS DB instance**. After selecting **RDS DB instance**, select the region where the source database resides and the region cannot be the same as the region where the destination database resides. The region where the destination database is located is the region where you log in to the management console. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the service database.
Port	The port of the service database. Range: 1 – 65535
Database Username	The username for accessing the service database.
Database Password	The password for the service database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **Connection Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password.
SSL Connection	SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate. **NOTE** • The maximum size of a single certificate file that can be uploaded is 500 KB. • If SSL is disabled, your data may be at risk.
Region	The region where the service DB instance is located. This parameter is selected by default. This parameter is available only when the source database is an **RDS DB instance**.
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an **RDS DB instance**.
Database Username	The username for accessing the service database.
Database Password	The password for the service database username.

NOTE

The IP address, domain name, username, and password of the service database are encrypted and stored in DRS and will be cleared after the task is deleted.

Figure 2-55 DR database information

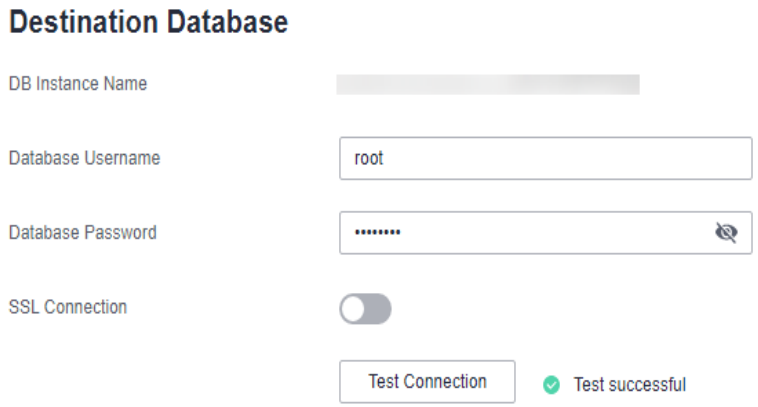


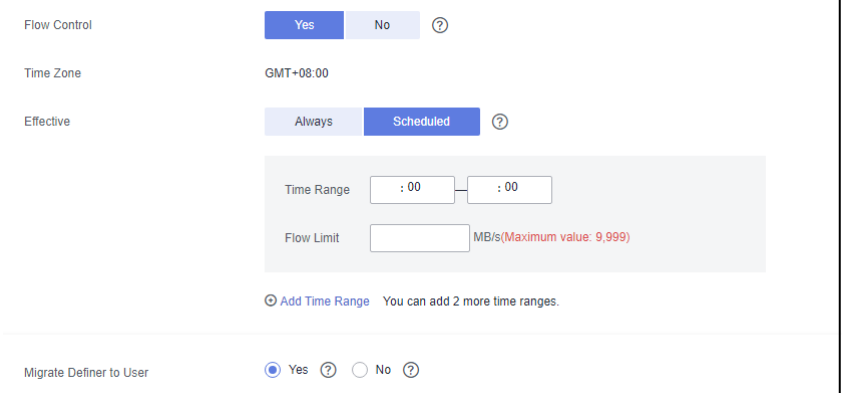
Table 2-59 DR database settings

Parameter	Description
DB Instance Name	The RDS for MySQL instance you selected when you create the DR instance. The instance name cannot be changed.
Database Username	The username for accessing the DR database.
Database Password	The password for the database username. The password can be changed after a task is created. If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **Connection Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.
SSL Connection	If SSL connection is required, enable SSL on the DR database, ensure that related parameters have been correctly configured, and upload an SSL certificate. **NOTE** • The maximum size of a single certificate file that can be uploaded is 500 KB. • If SSL is disabled, your data may be at risk.

Step 5 On the **Configure DR** page, specify flow control and click **Next**.

Figure 2-56 DR settings

Table 2-60 DR settings

Parameter	Description
Flow Control	You can choose whether to control the flow. • **Yes** You can customize the maximum DR speed. In addition, you can set the time range based on your service requirements. The traffic rate setting usually includes setting of a rate limiting time period and a traffic rate value. Flow can be controlled all day or during specific time ranges. The default value is **All day**. A maximum of three time ranges can be set, and they cannot overlap. The flow rate must be set based on the service scenario and cannot exceed 9,999 MB/s. **Figure 2-57** Flow control  • **No** The DR speed is not limited and the outbound bandwidth of the source database is maximally used, which causes read consumption on the source database accordingly. For example, if the outbound bandwidth of the source database is 100 MB/s and 80% bandwidth is used, the I/O consumption on the source database is 80 MB/s. **NOTE** – Flow control mode takes effect only in the DR initialization phase. – You can also change the flow control mode when the task is in the **Configuration** state. For details, see **Modifying the Flow Control Mode**.

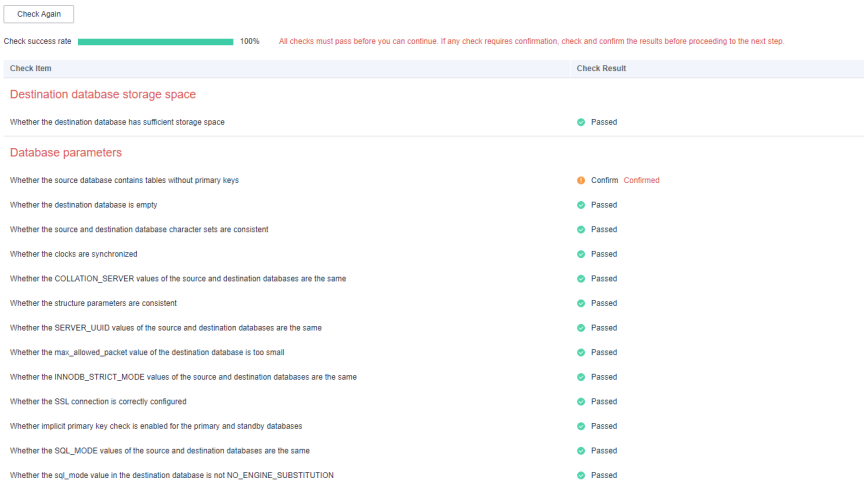
Parameter	Description
Migrate Definer to User	Indicates whether to migrate the Definers of all source database objects to the destination database user entered during the connection test. • Yes The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see **How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?** For example, if the view is CREATE ALGORITHM=UNDEFINED DEFINER=`username`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` before migration, it is converted to CREATE ALGORITHM=UNDEFINED DEFINER=`drsUser`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` after the migration. **drsUser** indicates the destination database user used for testing the connection. • **No** The Definers of all source database objects will not be changed. You need to migrate all accounts and permissions of the source database in the next step. Note that if the Definer account is not found in the destination database, unavailable objects will be created. For details about Definer, see the **MySQL official document**.

Step 6 On the **Check Task** page, check the DR task.

- If any check fails, review the failure cause and rectify the fault. After the fault is rectified, click **Check Again**.

  For details about how to handle check failures, see **Solutions to Failed Check Items** in *Data Replication Service User Guide*.

Figure 2-58 Pre-check



- If the check is complete and the check success rate is 100%, click **Next**.

  NOTE

  You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

Step 7 Compare the parameters.

The parameter comparison function helps you check the consistency of common parameters and performance parameters between service and DR databases and show inconsistent values. You can determine whether to use this function based on service requirements. It mainly ensures that services are not affected after the DR task is completed.

- This process is optional, so you can click **Next** to skip the comparison.
- Compare common parameters:
  - For common parameters, if the parameters in the service database are different from those in the DR database, click **Save Change** to make the parameters of the DR database be the same as those in the service database.

    Figure 2-59 Modifying common parameters

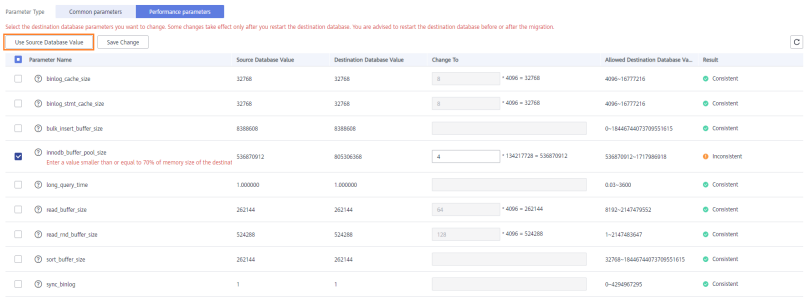
  - Performance parameter values in both the service and DR databases can be the same or different.
    - If you need to adjust the performance parameters, enter the value in the **Change to** column and click **Save Change**.

- If you want to make the performance parameter values of the source and destination database be the same:

  1) Click **Use Source Database Value**.

     DRS automatically makes the DR database values the same as those of the service database.

     Figure 2-60 One-click modification

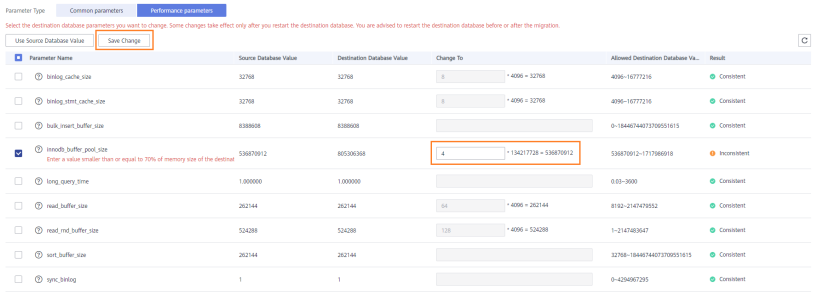
     NOTE

     You can also manually enter the value as required.

  2) Click **Save Change**.

     DRS changes the DR database parameter values based on your settings. After the modification, the comparison results are automatically updated.

     Figure 2-61 One-click modification

     Some parameters in the DR database cannot take effect immediately, so the comparison result is temporarily inconsistent. Restart the DR database before the DR task is started or after the DR task is completed. To minimize the impact of database restart on your services, restart the DR database at the scheduled time after the disaster recovery is complete.

     For details about parameter comparison, see **Parameters for Comparison** in the *Data Replication Service User Guide*.

  3) Click **Next**.

Step 8 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO**

Synchronization Delay Threshold, and **Stop Abnormal Tasks After** for the forward subtask. After confirming that the configured information is correct, click **Submit** to submit the forward DR task.

Figure 2-62 Task startup settings

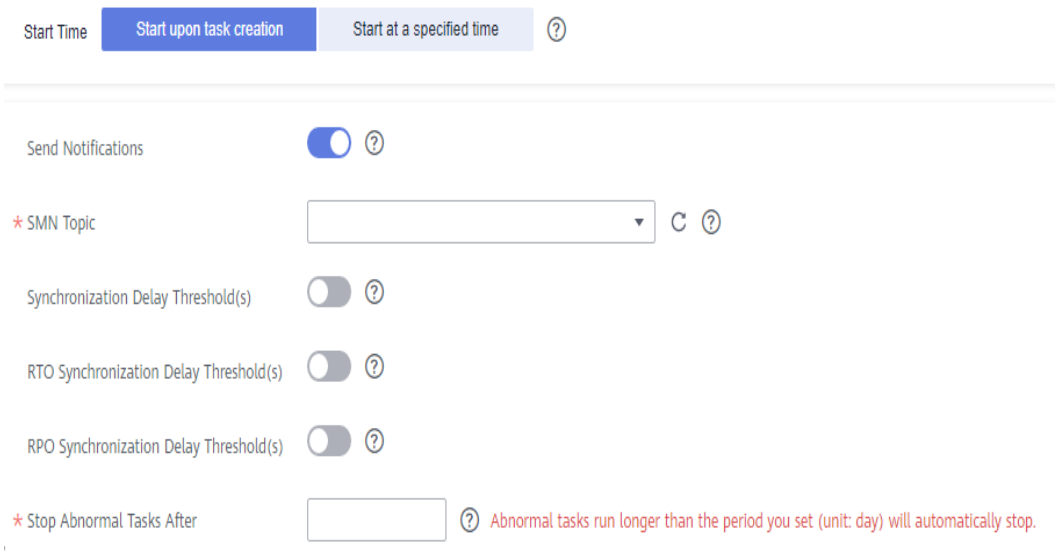


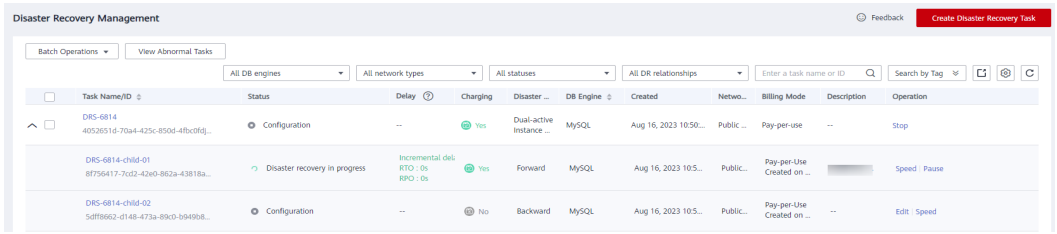
Table 2-61 Task and recipient description

Parameter	Description
Start Time	Set **Start Time** to **Start upon task creation** or **Start at a specified time** based on site requirements. **NOTE** After a DR task is started, the performance of the service and DR databases may be affected. You are advised to start a DR task during off-peak hours.
Send Notifications	SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.
SMN Topic	This parameter is available only after you enable **Send Notifications** and create a topic on the SMN console and add a subscriber. For details, see ***Simple Message Notification User Guide***.

Parameter	Description
Synchronization Delay Threshold	During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RTO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the DR database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the RTO delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RPO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the service database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient. • In the early stages of an incremental disaster recovery, the synchronization delay is long because a large quantity of data is awaiting synchronization. In this case, no notifications will be sent.
Stop Abnormal Tasks After	Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is **14**. **NOTE** • You can set this parameter only for pay-per-use tasks. • Tasks in the abnormal state are still charged. If tasks remain in the abnormal state for a long time, they cannot be resumed. Abnormal tasks run longer than the period you set (unit: day) will automatically stop to avoid unnecessary fees.

Step 9 Return to the **Disaster Recovery Management** page. After the forward subtask enters the **Disaster recovery in progress** state, locate the backward subtask and click **Edit** in the **Operation** column. The **Configure Source and Destination Databases** page of the backward subtask is displayed.

Figure 2-63 DR task list



Step 10 On the **Configure Source and Destination Databases** page, click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, click **Next**.

Step 11 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO Synchronization Delay Threshold**, and **Stop Abnormal Tasks After** for the backward subtask. After confirming that the configured information is correct, click **Submit** to submit the backward DR task.

Step 12 After the task is submitted, view and **manage it** on the **Disaster Recovery Management** page.

- You can view the task status. For more information about task status, see **Task Statuses**.
- You can click in the upper-right corner to view the latest task status.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.

----End

2.6 From GaussDB(for MySQL) to GaussDB(for MySQL) (Dual-Active DR)

Supported Source and Destination Databases

Table 2-62 Supported databases

Service database	DR Database
GaussDB(for MySQL)	GaussDB(for MySQL)

Database Account Permission Requirements

To start a DR task, the service and DR database users must meet the requirements in the following table. Different types of DR tasks require different permissions. For details, see **Table 2-63**. DRS automatically checks the database account permissions in the pre-check phase and provides handling suggestions.

Table 2-63 Database account permission

Type	Permission Required
Service database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION The **root** account of the GaussDB(for MySQL) instance has the preceding permissions by default.
DR database user	The user must have the following permissions: SELECT, CREATE, ALTER, DROP, DELETE, INSERT, UPDATE, TRIGGER, REFERENCES, SHOW VIEW, EVENT, INDEX, LOCK TABLES, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, RELOAD, REPLICATION SLAVE, REPLICATION CLIENT, and WITH GRANT OPTION The **root** account of the GaussDB(for MySQL) instance has the preceding permissions by default.

NOTE

- You are advised to create an independent database account for DRS task connection to prevent task failures caused by database account password modification.
- After changing the account passwords for the service and DR databases, **modify the connection information** in the DRS task as soon as possible to prevent automatic retry after a task failure. Automatic retry will lock the database accounts.
- **Table 2-63** lists the minimum permissions required by a DRS task. If you need to migrate the grant permission through a DRS task, ensure that the connection account of the DRS task has the corresponding permission. Otherwise, the destination database user may not be authorized due to grant execution failure. For example, if the connection account of the DRS task does not require the process permission, but you need to migrate the process permission through a DRS task, ensure that the connection account of the DRS task has the process permission.

Prerequisites

- **You have logged in to the DRS console.**
- Your account balance is greater than or equal to $0 USD.
- For details about the supported DB types and versions, see **Supported Databases**.

- If a subaccount is used to create a DRS task, ensure that an agency has been added. For details about how to create an agency, see **Agency Management**.

Suggestions

CAUTION

- During the DR initialization, do not perform DDL operations on the service database. Otherwise, the task may be abnormal.
- During DR initialization, ensure that no data is written to the DR database to ensure data consistency before and after DR.

- The success of DR depends on environment and manual operations. To ensure a smooth DR, perform a DR trial before you start the DR task to help you detect and resolve problems in advance.
- It is recommended that you start your DR task during off-peak hours to minimize the impact on your services.
  - If the bandwidth is not limited, initialization of DR will increase query workload of the source database by 50 MB/s and occupy 2 to 4 vCPUs.
  - To ensure data consistency, tables without a primary key may be locked for 3s during disaster recovery.
  - The data in the DR process may be locked by other transactions for a long period of time, resulting in read timeout.
  - If DRS concurrently reads data from a database, it will use about 6 to 10 sessions. The impact of the connections on services must be considered.
  - If you read a table, especially a large table, during DR, the exclusive lock on that table may be blocked.
  - For more information about the impact of DRS on databases, see **What Is the Impact of DRS on Source and Destination Databases?**
- Data-Level Comparison

  To obtain accurate comparison results, start data comparison at a specified time point during off-peak hours. If it is needed, select **Start at a specified time** for **Comparison Time**. Due to slight time difference and continuous operations on data, data inconsistency may occur, reducing the reliability and validity of the comparison results.

Precautions

Before creating a DR task, read the following precautions:

Table 2-64 Precautions

Type	Restrictions
Disaster recovery objects	• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery. • System tables are not supported. • Triggers and events do not support disaster recovery. • Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery. • DDL operations cannot be executed on the active database 2.
Service database configuration	• The service database must be the primary node of the GaussDB(for MySQL) instance. • The binlog of the service database must be enabled and use the row-based format. • If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days. • The service database username or password cannot be empty. • GTID must be enabled for the database. • The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_). • The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '<>/\ • If the **expire_logs_days** value of the database is set to **0**, the disaster recovery may fail.
DR database configuration	• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal. • The DR DB instance must have sufficient storage space. • The binlog of the DR database must be enabled and use the row-based format. • GTID must be enabled for the DR database. • The major version of the active database 1 must be the same as that of the active database 2. • Active database 2 must be an empty instance. After the forward task is started, active database 2 is set to read-only. After the backward task is started and DR is performed, active database 2 is restored to read/write.

Type	Restrictions
Precautions	• Dual-active DR supports backup in backward and forward directions. Due to certain uncontrollable factors, data may be inconsistent between the two sides. For example, if the load of active database 1 is too heavy and the load of active database 2 is light, data updates on the active database 1 synchronized to the active database 2 will be delayed due to the heave load, as a result, the operation sequence is changed and data becomes inconsistency. Therefore, divide data by unit (database, table, or row) and ensure the unit on one database is responsible for data read and write while on the other is read-only. In essence, in dual-active DR, both the databases play the active role but work differently. For details about common scenarios, see **Common Exceptions in Real-Time Disaster Recovery**. • Before creating a DRS task, if concurrency control rules of SQL statements are configured for the service or DR database, the DRS task may fail. • During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal. • During disaster recovery, you can create accounts for the service database. • If the same data on both databases is updated simultaneously, data conflicts may occur. DRS resolves the conflict by overwriting the previous settings with the last settings. – When the deletion operation is performed, data is deleted and DRS does not perform any operation. – When the insert operation is performed, DRS updates data with the latest inserted data. – When the update operation is performed, the original data has been updated and DRS directly insert the new data. • Primary key conflicts between the two sides need to be avoided. For example, you can use a UUID or the primary key rule of region+auto-increment ID to avoid conflicts. • If the synchronization delay takes a long time due to connection interruption or network issues, you need to determine whether your services can tolerant the long-term delay. • Cascade operations cannot be performed on tables with foreign keys. If the foreign key index of a table is a common index, the table structure may fail to be created. You are advised to use a unique index. • If a physically generated column in a table is generated based on a time type, the data in the column may be inconsistent. • The dual-active DR is different from the single-active DR. Therefore, no active/standby switchover is required.

Type	Restrictions
	• The DR latency is uncontrollable. Therefore, DDL operations must be performed when no service is running, and both RPO and RTO are zero and latency is kept within 30 seconds on active database 1. Do not perform DDL operations on active database 2. (DRS synchronizes only the DDL operations on active database 1 to active database 2.) • Ensure that the tables, columns, and rows are consistent in both the databases. (The table structures of both the active databases are consistent.) • A backward task can be started only when the forward task is in the DR process and both RPO and RTO are less than 60s. • After the dual-active DR task is in the DR process, perform tests on the active database 2 first. If the test results meet the requirements, switch certain service traffic to the active database 2.

Procedure

Step 1 On the **Disaster Recovery Management** page, click **Create Disaster Recovery Task**.

Step 2 On the **Create Disaster Recovery Instance** page, select a region and project, specify the task name, description, and the DR instance details, and click **Create Now**.

- Task information description

Figure 2-64 DR task information

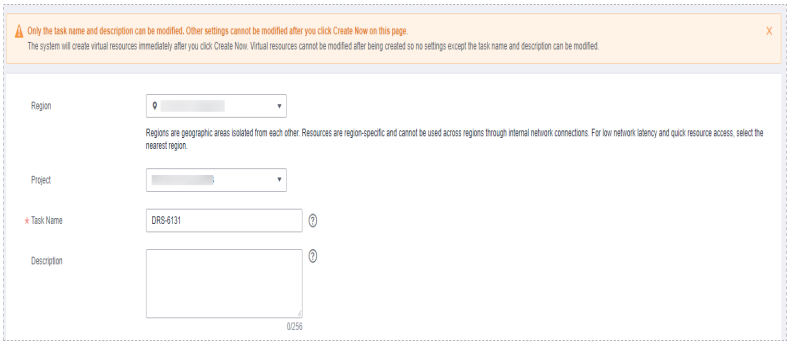


Table 2-65 Task and recipient description

Parameter	Description
Region	The region where your service is running. You can change the region.
Project	The project corresponds to the current region and can be changed.

Parameter	Description
Task Name	The task name must start with a letter and consist of 4 to 50 characters. It can contain only letters, digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters !=<>'&"\

- DR instance information

Figure 2-65 DR instance information

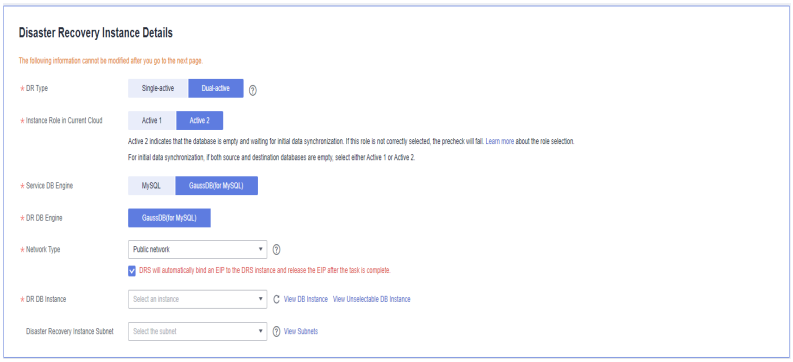


Table 2-66 DR instance settings

Parameter	Description
DR Type	Select **Dual-active**. The DR type can be single-active or dual-active. If **Dual-active** is selected, two subtasks are created by default, a forward DR task and a backward DR task. **NOTE** Only whitelisted users can use dual-active DR. To use this function, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket.
Current Cloud RDS Instance Role	Select **Active 1** or **Active 2**. This parameter specifies the role of the current RDS DB instance in the DR relationship and is available when **DR Type** is set to **Dual-active**. For details about how to choose active 1 and 2, see **How Do I Select Active Database 1 and 2 for Dual-Active DR?** – Active 1: Initial data is available on the current cloud database when a task is created. – Active 2: The instance on the current cloud is empty when a task is created. Active 2 is used as an example.

Parameter	Description
Service DB Engine	Select **GaussDB(for MySQL)**.
DR DB Engine	Select **GaussDB(for MySQL)**.
Network Type	The public network is used as an example. Available options: **VPN or Direct Connect** and **Public network**. By default, the value is **Public network**.
DR DB Instance	The GaussDB(for MySQL) instance you created.
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click **View Subnet** to go to the network console to view the subnet where the instance resides. By default, the DRS instance and the destination DB instance are in the same subnet. You need to select the subnet where the DRS instance resides and ensure that there are available IP addresses. To ensure that the disaster recovery instance is successfully created, only subnets with DHCP enabled are displayed.

- Specifications

Figure 2-66 Specifications

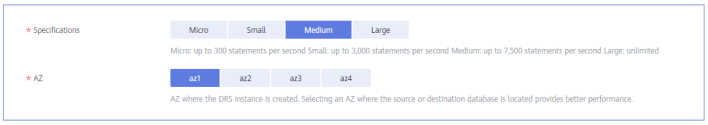


Table 2-67 Specifications

Parameter	Description
Specifications	DRS instance specifications. Different specifications have different performance upper limits. For details, see **Real-Time DR**. **NOTE** DRS allows you to upgrade specifications only for real-time DR tasks from MySQL to MySQL, from MySQL to GaussDB(for MySQL), and from GaussDB(for MySQL) to GaussDB(for MySQL). Task specifications cannot be downgraded. For details, see **Changing Specifications**.
AZ	Select the AZ where you want to create the DRS task. Selecting the one housing the source or destination database can provide better performance.

- Enterprise Project and Tags

Figure 2-67 Enterprise projects and tags

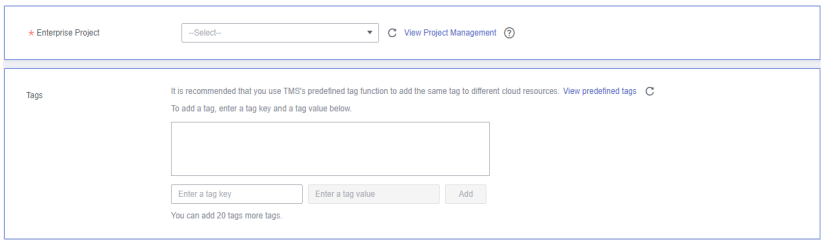


Table 2-68 Enterprise Project and Tags

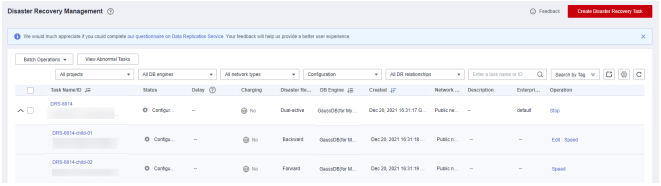
Parameter	Description
Enterprise Project	An enterprise project you would like to use to centrally manage your cloud resources and members. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise projects, see ***Enterprise Management User Guide***. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Project Management Service** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.
Tags	– Tags a task. This configuration is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 20 tags. – After a task is created, you can view its tag details on the **Tags** tab. For details, see **Tag Management**.

NOTE

If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.

Step 3 On the **Disaster Recovery Management** page, after the task is created, locate the forward subtask and click **Edit** in the **Operation** column. The **Configure Source and Destination Databases** page is displayed.

Figure 2-68 DR task list



Step 4 On the **Configure Source and Destination Databases** page, wait until the DR instance is created. Then, specify source and destination database information and click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, select the check box before the agreement and click **Next**.

Figure 2-69 Service database information

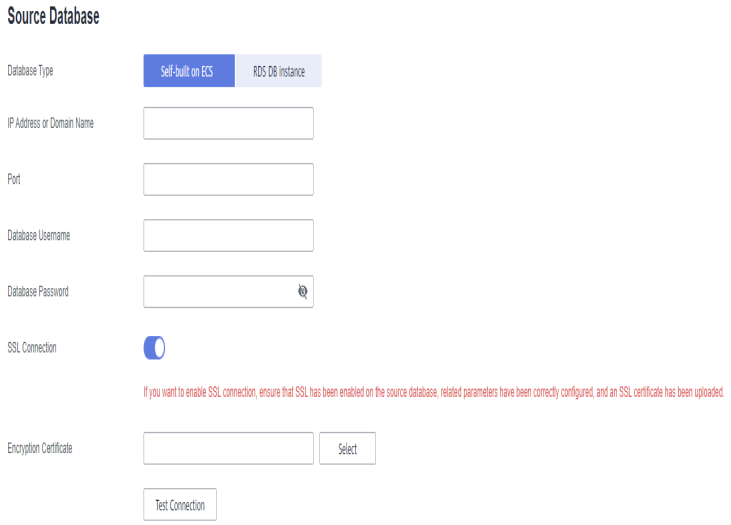


Table 2-69 Service database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The source database can be a **Self-built on ECS** or an **RDS DB instance**. After selecting **RDS DB instance**, select the region where the source database resides and the region cannot be the same as the region where the destination database resides. The region where the destination database is located is the region where you log in to the management console. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the service database.
Port	The port of the service database. Range: 1 – 65535
Database Username	The username for accessing the service database.
Database Password	The password for the service database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **Connection Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password.

Parameter	Description
SSL Connection	SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate. **NOTE** • The maximum size of a single certificate file that can be uploaded is 500 KB. • If SSL is disabled, your data may be at risk.
Region	The region where the service DB instance is located. This parameter is selected by default. This parameter is available only when the source database is an **RDS DB instance**.
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an **RDS DB instance**.
Database Username	The username for accessing the service database.
Database Password	The password for the service database username.

NOTE

The IP address, domain name, username, and password of the service database are encrypted and stored in DRS and will be cleared after the task is deleted.

Figure 2-70 DR database information

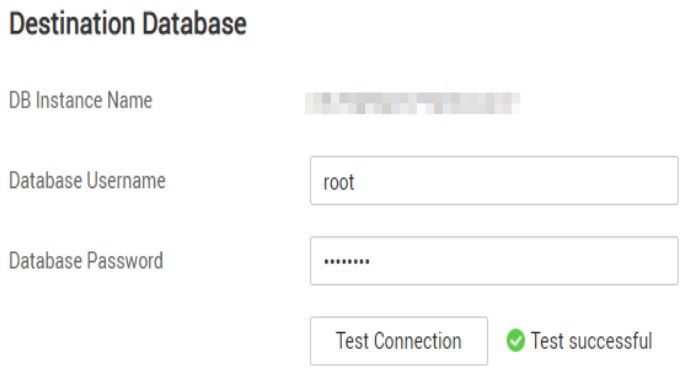


Table 2-70 DR database settings

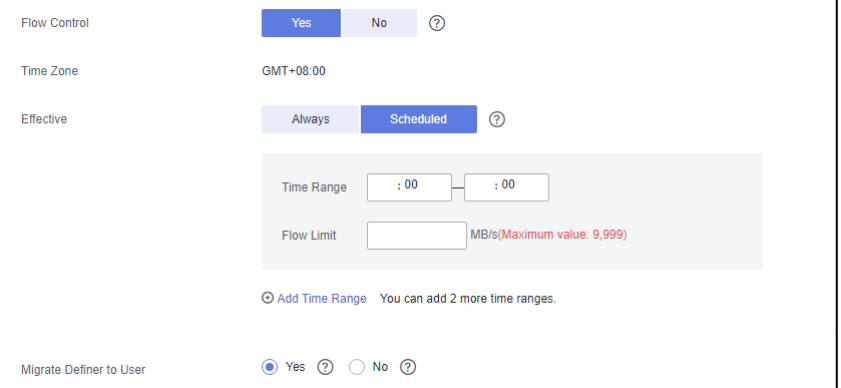
Parameter	Description
DB Instance Name	The GaussDB(for MySQL) instance you selected when creating the DR task. This parameter cannot be changed.
Database Username	The username for accessing the DR database.

Parameter	Description
Database Password	The password for the database username. The password can be changed after a task is created. If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **Connection Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.

Step 5 On the **Configure DR** page, specify flow control and click **Next**.

Figure 2-71 DR settings

Table 2-71 DR settings

Parameter	Description
Flow Control	You can choose whether to control the flow. • **Yes** You can customize the maximum DR speed. In addition, you can set the time range based on your service requirements. The traffic rate setting usually includes setting of a rate limiting time period and a traffic rate value. Flow can be controlled all day or during specific time ranges. The default value is **All day**. A maximum of three time ranges can be set, and they cannot overlap. The flow rate must be set based on the service scenario and cannot exceed 9,999 MB/s. **Figure 2-72** Flow control  • **No** The DR speed is not limited and the outbound bandwidth of the source database is maximally used, which causes read consumption on the source database accordingly. For example, if the outbound bandwidth of the source database is 100 MB/s and 80% bandwidth is used, the I/O consumption on the source database is 80 MB/s. **NOTE** – Flow control mode takes effect only in the DR initialization phase. – You can also change the flow control mode when the task is in the **Configuration** state. For details, see **Modifying the Flow Control Mode**.

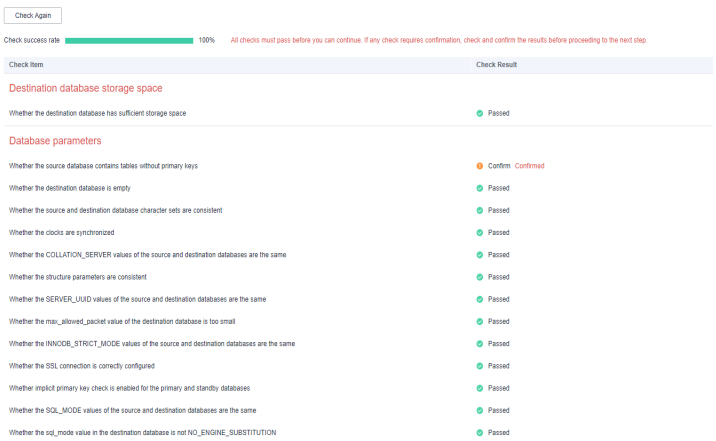
Parameter	Description
Migrate Definer to User	Indicates whether to migrate the Definers of all source database objects to the destination database user entered during the connection test. • Yes The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see **How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?** For example, if the view is CREATE ALGORITHM=UNDEFINED DEFINER=`username`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` before migration, it is converted to CREATE ALGORITHM=UNDEFINED DEFINER=`drsUser`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` after the migration. **drsUser** indicates the destination database user used for testing the connection. • **No** The Definers of all source database objects will not be changed. You need to migrate all accounts and permissions of the source database in the next step. Note that if the Definer account is not found in the destination database, unavailable objects will be created. For details about Definer, see the **MySQL official document**.

Step 6 On the **Check Task** page, check the DR task.

- If any check fails, review the failure cause and rectify the fault. After the fault is rectified, click **Check Again**.

  For details about how to handle check failures, see **Solutions to Failed Check Items** in *Data Replication Service User Guide*.

Figure 2-73 Pre-check



- If the check is complete and the check success rate is 100%, click **Next**.

  NOTE

  You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

Step 7 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO Synchronization Delay Threshold**, and **Stop Abnormal Tasks After** for the forward subtask. After confirming that the configured information is correct, click **Submit** to submit the forward DR task.

Figure 2-74 Task startup settings

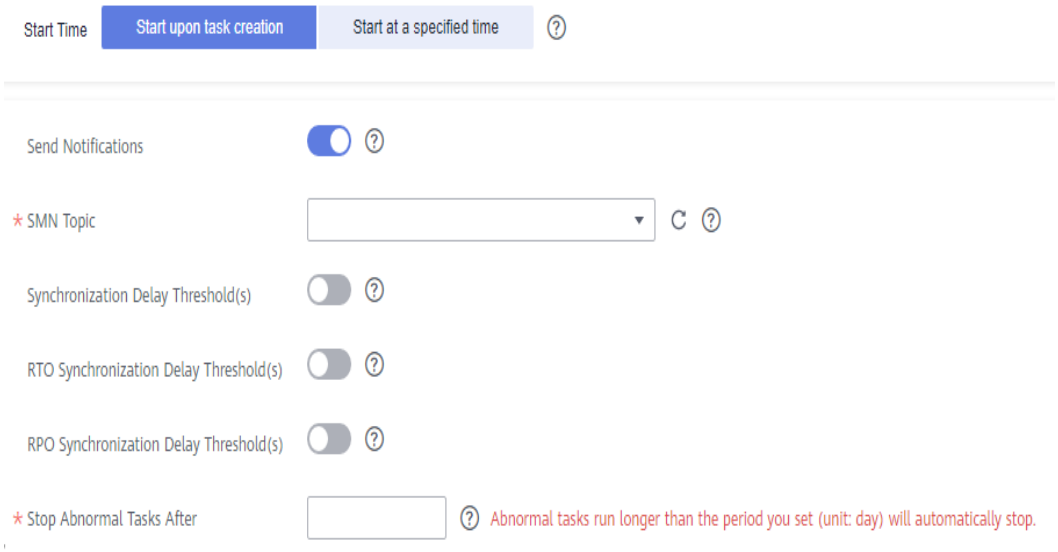


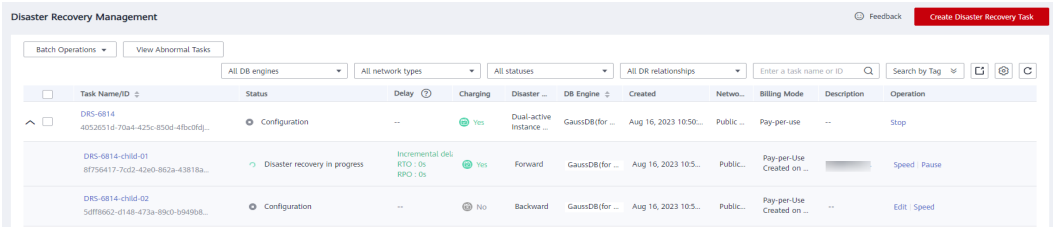
Table 2-72 Task and recipient description

Parameter	Description
Start Time	Set **Start Time** to **Start upon task creation** or **Start at a specified time** based on site requirements. **NOTE** After a DR task is started, the performance of the service and DR databases may be affected. You are advised to start a DR task during off-peak hours.
Send Notifications	SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.
SMN Topic	This parameter is available only after you enable **Send Notifications** and create a topic on the SMN console and add a subscriber. For details, see ***Simple Message Notification User Guide***.

Parameter	Description
Synchronization Delay Threshold	During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RTO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the DR database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the RTO delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RPO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the service database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient. • In the early stages of an incremental disaster recovery, the synchronization delay is long because a large quantity of data is awaiting synchronization. In this case, no notifications will be sent.
Stop Abnormal Tasks After	Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is **14**. **NOTE** • You can set this parameter only for pay-per-use tasks. • Tasks in the abnormal state are still charged. If tasks remain in the abnormal state for a long time, they cannot be resumed. Abnormal tasks run longer than the period you set (unit: day) will automatically stop to avoid unnecessary fees.

Step 8 Return to the **Disaster Recovery Management** page. After the forward subtask enters the **Disaster recovery in progress** state, locate the backward subtask and click **Edit** in the **Operation** column. The **Configure Source and Destination Databases** page of the backward subtask is displayed.

Figure 2-75 DR task list



Step 9 On the **Configure Source and Destination Databases** page, click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, click **Next**.

Step 10 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO Synchronization Delay Threshold**, and **Stop Abnormal Tasks After** for the backward subtask. After confirming that the configured information is correct, click **Submit** to submit the backward DR task.

Step 11 After the task is submitted, view and **manage it** on the **Disaster Recovery Management** page.

- You can view the task status. For more information about task status, see **Task Statuses**.
- You can click in the upper-right corner to view the latest task status.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.

----End

3 Task Management

3.1 Creating a DR Task

Scenario

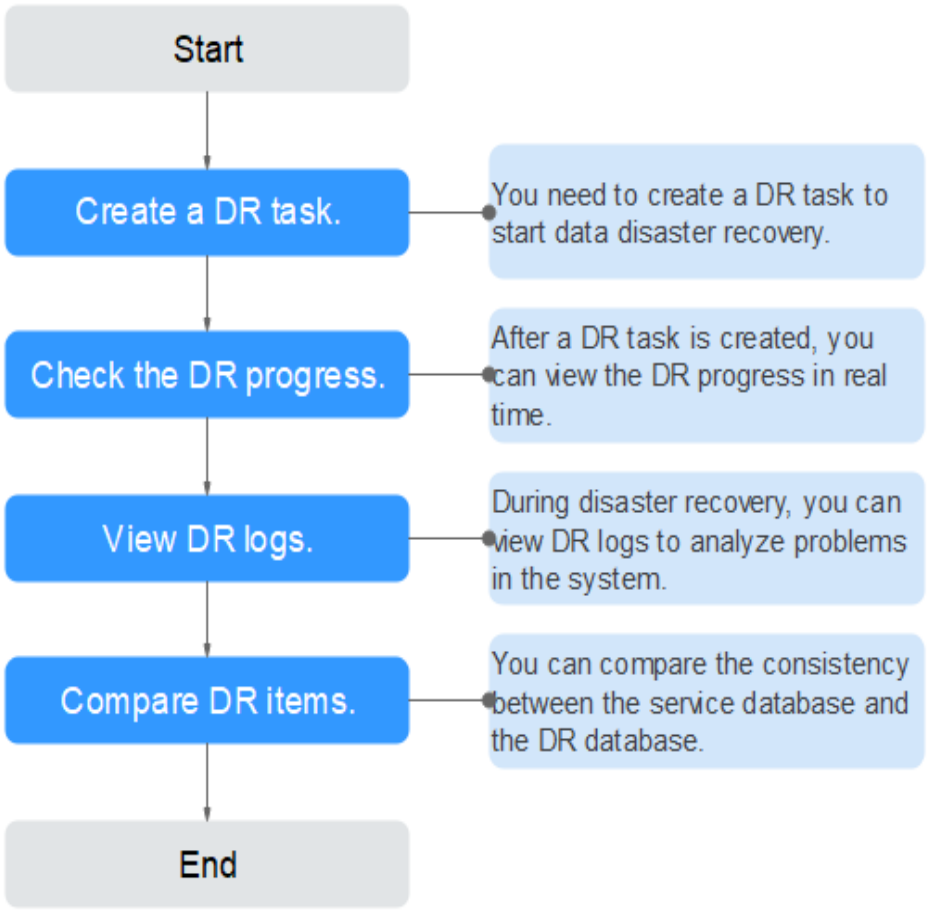
To prevent service unavailability caused by regional faults, DRS provides disaster recovery to ensure service continuity. If the region where the primary instance is located encounters a natural disaster and cannot be connected, you can switch the remote instance to the primary instance. To reconnect to the primary instance, you only need to change the connection address on the application side. DRS allows you to perform cross-region real-time synchronization between a primary instance and a DR instance during disaster recovery

A complete online disaster recovery consists of creating a DR task, tracking task progress, analyzing DR logs, and comparing data consistency. By comparing multiple items and data, you can synchronize data between different service systems.

Process

The following flowchart shows the basic processes for disaster recovery.

Figure 3-1 Disaster recovery process



- **Step 1: Create a DR task.** Select the service and DR databases as required and create a DR task.
- **Step 2: Query the DR progress.** During the disaster recovery, you can view the DR progress.
- **Step 3: View DR logs.** Disaster recovery logs contain alarms, errors, and prompt information. You can analyze system problems based on such information.
- **Step 4: Compare DR items.** The DR system supports object-level, data-level comparison to ensure data consistency.

This section uses disaster recovery from a MySQL instance to an RDS for MySQL instance as an example describes how to configure a DR task on the DRS console over a public network.

You can create a DR task that will walk you through each step of the process. After a DR task is created, you can manage it on the DRS console.

Prerequisites

- **You have logged in to the DRS console.**
- Your account balance is greater than or equal to $0 USD.
- For details about the supported DB types and versions, see **Supported Databases**.

- If a subaccount is used to create a DRS task, ensure that an agency has been added. For details about how to create an agency, see **Agency Management**.

Procedure

Step 1 On the **Disaster Recovery Management** page, click **Create Disaster Recovery Task**.

Step 2 On the **Create Disaster Recovery Instance** page, select a region and project, specify the task name, description, and the DR instance details, and click **Create Now**.

- Task information description

Figure 3-2 DR task information

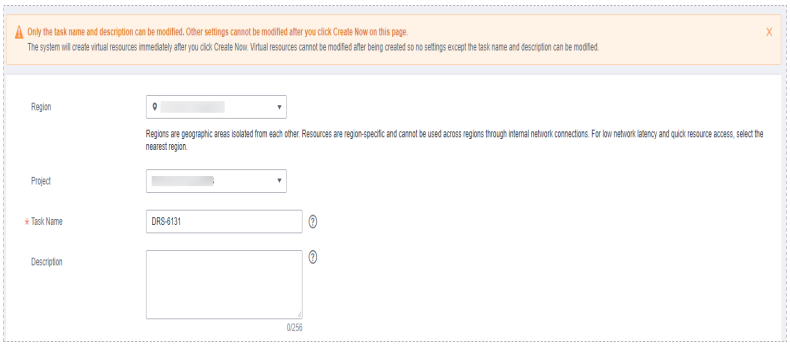


Table 3-1 Task and recipient description

Parameter	Description
Region	The region where your service is running. You can change the region.
Project	The project corresponds to the current region and can be changed.
Task Name	The task name must start with a letter and consist of 4 to 50 characters. It can contain only letters, digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters !=<>'&"\

- DR instance information

Figure 3-3 DR instance information

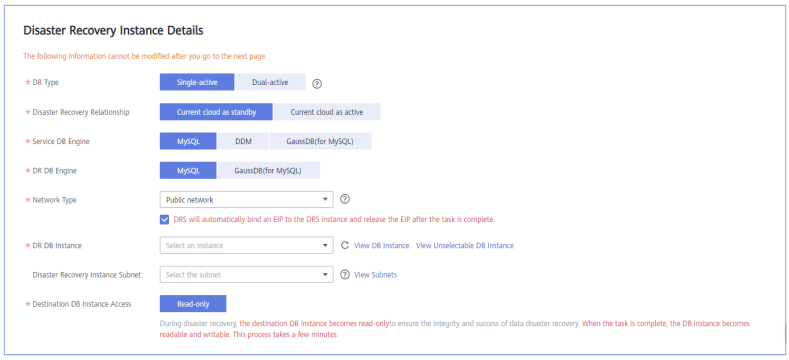


Table 3-2 DR instance settings

Parameter	Description
DR Type	Select **Single-active**. The DR type can be single-active or dual-active. If **Dual-active** is selected, two subtasks are created by default, a forward DR task and a backward DR task. **NOTE** Only whitelisted users can use dual-active DR. To use this function, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** to submit a service ticket.
Disaster Recovery Relationship	Select **Current cloud as standby**. This parameter is available only when you select **Single-active**. By default, **Current cloud as standby** is selected. You can also select **Current cloud as active**. – **Current cloud as standby**: The DR database is on the current cloud. – **Current cloud as active**: The service database is on the current cloud.
Service DB Engine	Select **MySQL**.
DR DB Engine	Select **MySQL**.
Network Type	The public network is used as an example. Available options: **VPN or Direct Connect** and **Public network**. By default, the value is **Public network**.
DR DB Instance	RDS DB instance you have created as the destination database of the DR task.

Parameter	Description
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click **View Subnet** to go to the network console to view the subnet where the instance resides. By default, the DRS instance and the destination DB instance are in the same subnet. You need to select the subnet where the DRS instance resides and ensure that there are available IP addresses. To ensure that the disaster recovery instance is successfully created, only subnets with DHCP enabled are displayed.
Destination Database Access	Select **Read-only**. This parameter is available only when you select **Single-active**. – During disaster recovery, the entire DR database instance becomes read-only. To change the DR database to **Read/Write**, you can change the DR database (or destination database) to a service database by clicking **Promote Current Cloud** on the **Disaster Recovery Monitoring** tab. – After the DR task is complete, the DR database changes to **Read/Write**. – When the external database functions as the DR database, the user with the superuser permission can set the database to read-only. – If a DRS instance node is rebuilt due to a fault, to ensure data consistency during the DRS task restoration, the current cloud standby database is set to read-only before the task is restored. After the task is restored, the synchronization relationship recovers.

- Specifications

Figure 3-4 Specifications

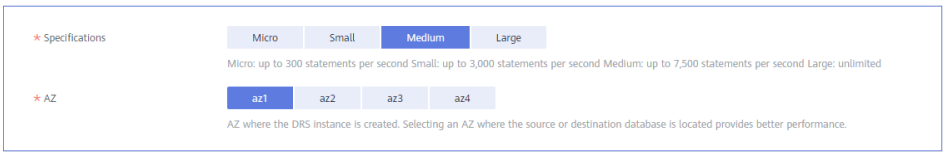


Table 3-3 Specifications

Parameter	Description
Specifications	DRS instance specifications. Different specifications have different performance upper limits. For details, see **Real-Time DR**. **NOTE** DRS allows you to upgrade specifications only for real-time DR tasks from MySQL to MySQL, from MySQL to GaussDB(for MySQL), and from GaussDB(for MySQL) to GaussDB(for MySQL). Task specifications cannot be downgraded. For details, see **Changing Specifications**.
AZ	Select the AZ where you want to create the DRS task. Selecting the one housing the source or destination database can provide better performance.

- Enterprise Project and Tags

Figure 3-5 Enterprise projects and tags

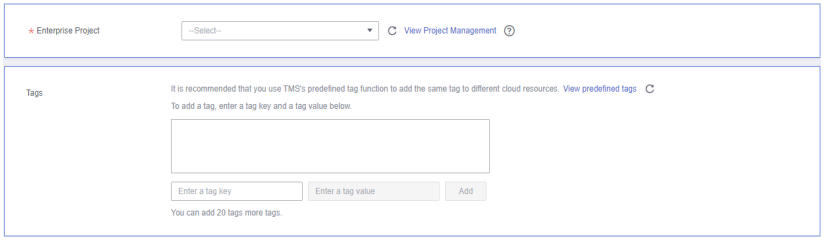


Table 3-4 Enterprise Project and Tags

Parameter	Description
Enterprise Project	An enterprise project you would like to use to centrally manage your cloud resources and members. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise projects, see ***Enterprise Management User Guide***. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Project Management Service** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.
Tags	– Tags a task. This configuration is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 20 tags. – After a task is created, you can view its tag details on the **Tags** tab. For details, see **Tag Management**.

NOTE

If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.

Step 3 On the **Configure Source and Destination Databases** page, wait until the DR instance is created. Then, specify source and destination database information and click **Test Connection** for both the source and destination databases to check whether they have been connected to the DR instance. After the connection tests are successful, select the check box before the agreement and click **Next**.

- Select **Current cloud as standby** for **Disaster Recovery Relationship** in **Step 2**.

Figure 3-6 Service database information

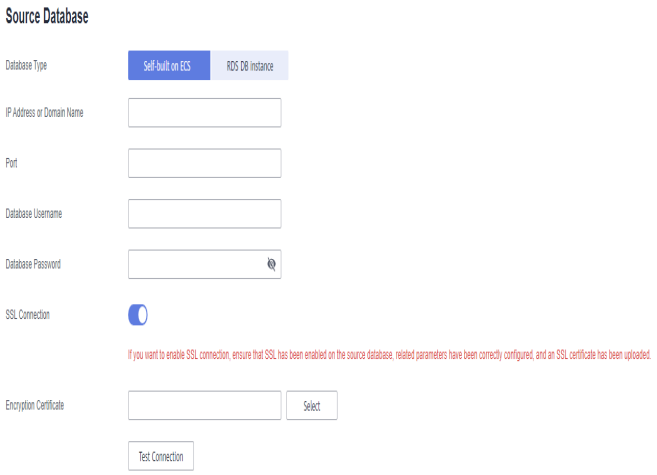


Table 3-5 Service database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The source database can be a **Self-built on ECS** or an **RDS DB instance**. After selecting **RDS DB instance**, select the region where the source database resides and the region cannot be the same as the region where the destination database resides. The region where the destination database is located is the region where you log in to the management console. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the service database.
Port	The port of the service database. Range: 1 – 65535
Database Username	The username for accessing the service database.

Parameter	Description
Database Password	The password for the service database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **Connection Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password.
SSL Connection	SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.
Region	The region where the service DB instance is located. This parameter is selected by default. This parameter is available only when the source database is an **RDS DB instance**.
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an **RDS DB instance**.
Database Username	The username for accessing the service database.
Database Password	The password for the service database username.

NOTE

The IP address, domain name, username, and password of the service database are encrypted and stored in DRS and will be cleared after the task is deleted.

Figure 3-7 DR database information

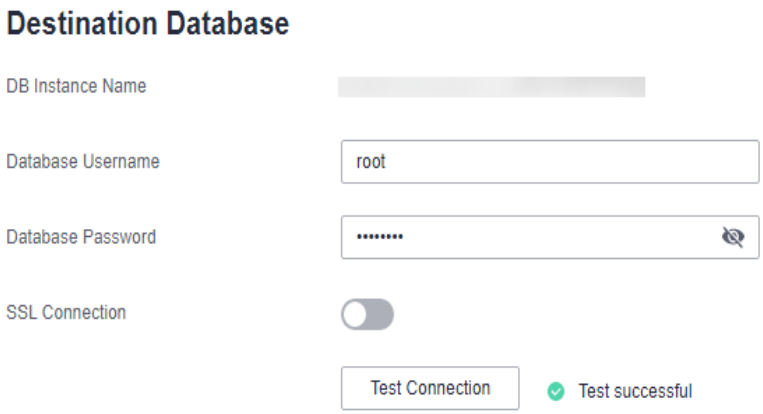


Table 3-6 DR database settings

Parameter	Description
DB Instance Name	The DB instance you selected when creating the DR task and cannot be changed.
Database Username	The username for accessing the DR database.
Database Password	The password for the database username. The password can be changed after a task is created. If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.
SSL Connection	If SSL connection is required, enable SSL on the DR database, ensure that related parameters have been correctly configured, and upload an SSL certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.

- Select **Current cloud as active** for **Disaster Recovery Relationship** in **Step 2**.

Figure 3-8 Service database information

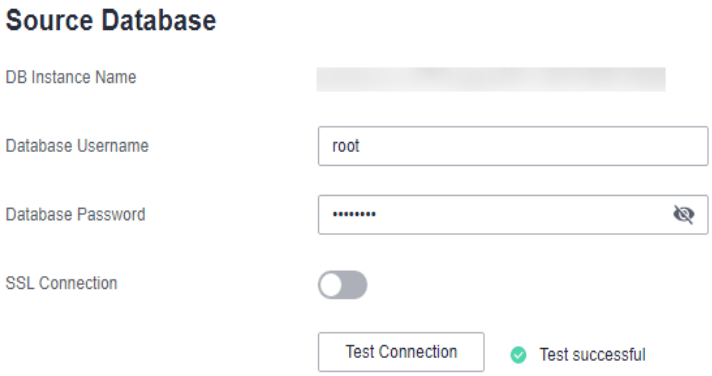


Table 3-7 Service database settings

Parameter	Description
DB Instance Name	The RDS instance selected when you created the DR task. This parameter cannot be changed.
Database Username	The username for accessing the service database.
Database Password	The password for the database username. You can change the password if necessary. To change the password, perform the following operation after the task is created: If the task is in the **Starting**, **Initializing**, **Disaster recovery in progress**, or **Disaster recovery failed** status, in the **DR Information** area on the **Basic Information** tab, click **Modify Connection Details**. In the displayed dialog box, change the password. The database username and password are encrypted and stored in the system and will be cleared after the task is deleted.
SSL Connection	If SSL connection is required, enable SSL on the service database, ensure that related parameters have been correctly configured, and upload an SSL certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.

Figure 3-9 DR database information

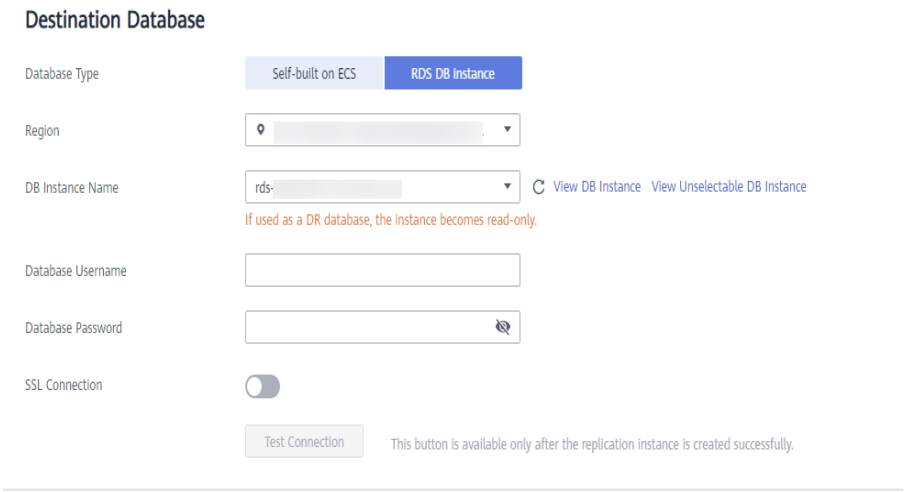


Table 3-8 DR database settings

Parameter	Description
Database Type	By default, **Self-built on ECS** is selected. The destination database can be a **Self-built on ECS** or an **RDS DB instance**. If you select **RDS DB instance**, you need to select the region where the destination database is located. To use the **RDS DB instance** option, submit a service ticket.
IP Address or Domain Name	The IP address or domain name of the DR database.
Port	The port of the DR database. Range: 1 – 65535
Region	The region where the RDS DB instance is located. This parameter is available only when the destination database is an RDS DB instance.
DB Instance Name	DR instance name. This parameter is available only when the destination database is an RDS DB instance. **NOTE** When the DB instance is used as the DR database, it is set to read-only. After the task is complete, the DB instance can be readable and writable.
Database Username	Username for logging in to the DR database.
Database Password	Password for the database username.

Parameter	Description
SSL Connection	If SSL connection is required, enable SSL on the DR database, ensure that related parameters have been correctly configured, and upload an SSL certificate. **NOTE** – The maximum size of a single certificate file that can be uploaded is 500 KB. – If SSL is disabled, your data may be at risk.

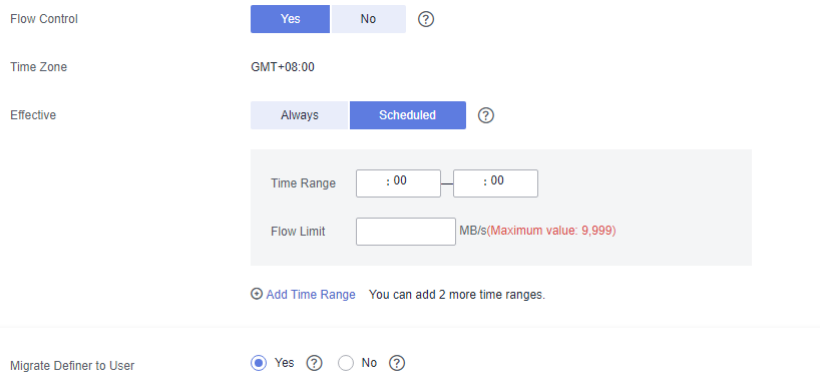
NOTE

The IP address, domain name, username, and password of the DR database are encrypted and stored in DRS and will be cleared after the task is deleted.

Step 4 On the **Configure DR** page, specify flow control and click **Next**.

Figure 3-10 DR settings

Table 3-9 DR settings

Parameter	Description
Flow Control	You can choose whether to control the flow. • **Yes** You can customize the maximum DR speed. In addition, you can set the time range based on your service requirements. The traffic rate setting usually includes setting of a rate limiting time period and a traffic rate value. Flow can be controlled all day or during specific time ranges. The default value is **All day**. A maximum of three time ranges can be set, and they cannot overlap. The flow rate must be set based on the service scenario and cannot exceed 9,999 MB/s. **Figure 3-11** Flow control  • **No** The DR speed is not limited and the outbound bandwidth of the source database is maximally used, which causes read consumption on the source database accordingly. For example, if the outbound bandwidth of the source database is 100 MB/s and 80% bandwidth is used, the I/O consumption on the source database is 80 MB/s. **NOTE** – Flow control mode takes effect only in the DR initialization phase. – You can also change the flow control mode when the task is in the **Configuration** state. For details, see **Modifying the Flow Control Mode**.

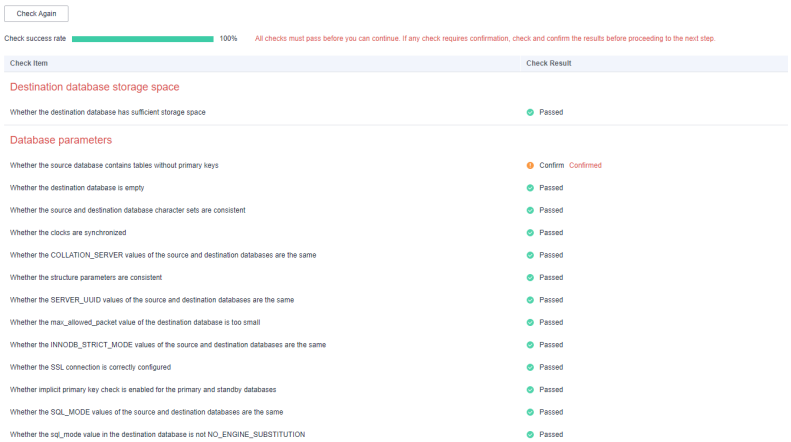
Parameter	Description
Migrate Definer to User	Indicates whether to migrate the Definers of all source database objects to the destination database user entered during the connection test. • Yes The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see **How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?** For example, if the view is CREATE ALGORITHM=UNDEFINED DEFINER=`username`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` before migration, it is converted to CREATE ALGORITHM=UNDEFINED DEFINER=`drsUser`@`%` SQL SECURITY DEFINER VIEW `test_db`.`view5` AS select 1 AS `1` after the migration. **drsUser** indicates the destination database user used for testing the connection. • **No** The Definers of all source database objects will not be changed. You need to migrate all accounts and permissions of the source database in the next step. Note that if the Definer account is not found in the destination database, unavailable objects will be created. For details about Definer, see the **MySQL official document**.

Step 5 On the **Check Task** page, check the DR task.

- If any check fails, review the failure cause and rectify the fault. After the fault is rectified, click **Check Again**.

  For details about how to handle check failures, see **Solutions to Failed Check Items** in *Data Replication Service User Guide*.

Figure 3-12 Pre-check



- If the check is complete and the check success rate is 100%, go to the **Compare Parameter** page.

  NOTE

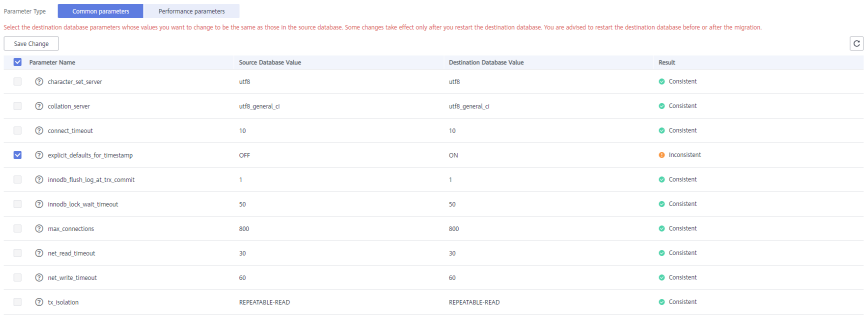
  You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

Step 6 Compare the parameters.

The parameter comparison function helps you check the consistency of common parameters and performance parameters between service and DR databases and show inconsistent values. You can determine whether to use this function based on service requirements. It mainly ensures that services are not affected after the DR task is completed.

- This process is optional, so you can click **Next** to skip the comparison.
- Compare common parameters:
  - For common parameters, if the parameters in the service database are different from those in the DR database, click **Save Change** to make the parameters of the DR database be the same as those in the service database.

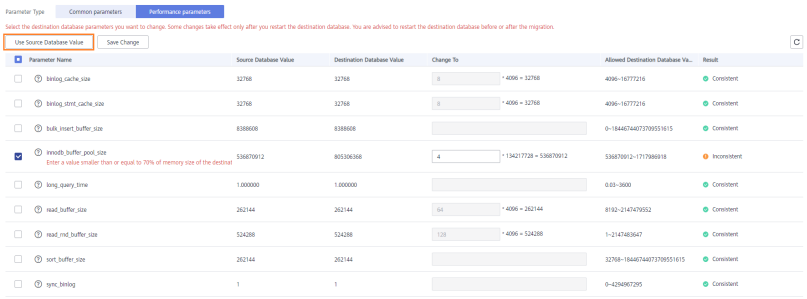
    Figure 3-13 Modifying common parameters

  - Performance parameter values in both the service and DR databases can be the same or different.
    - If you need to adjust the performance parameters, enter the value in the **Change to** column and click **Save Change**.
    - If you want to make the performance parameter values of the source and destination database be the same:
      1) Click **Use Source Database Value**.

         DRS automatically makes the DR database values the same as those of the service database.

Figure 3-14 One-click modification



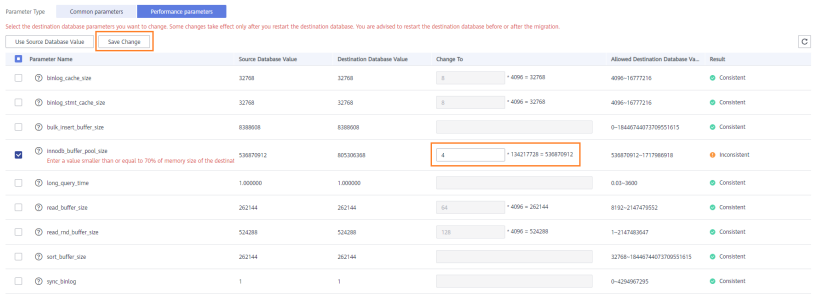
NOTE

You can also manually enter the value as required.

2) Click **Save Change**.

DRS changes the DR database parameter values based on your settings. After the modification, the comparison results are automatically updated.

Figure 3-15 One-click modification



Some parameters in the DR database cannot take effect immediately, so the comparison result is temporarily inconsistent. Restart the DR database before the DR task is started or after the DR task is completed. To minimize the impact of database restart on your services, restart the DR database at the scheduled time after the disaster recovery is complete.

For details about parameter comparison, see **Parameters for Comparison** in the *Data Replication Service User Guide*.

3) Click **Next**.

Step 7 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO Synchronization Delay Threshold**, **Stop Abnormal Tasks After** and DR instance details. Then, click **Submit**.

Figure 3-16 Task startup settings

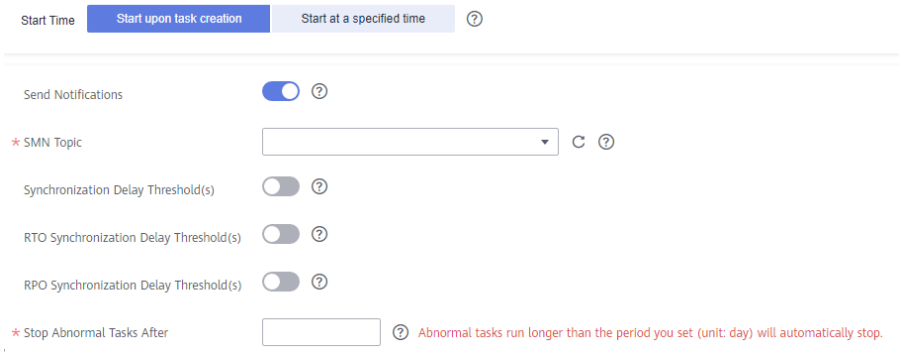


Table 3-10 Task and recipient description

Parameter	Description
Start Time	Set **Start Time** to **Start upon task creation** or **Start at a specified time** based on site requirements. **NOTE** Starting a DR task may slightly affect the performance of the service and DR databases. You are advised to start a DR task during off-peak hours.
Send Notifications	SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.
SMN Topic	This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber. For details, see **Simple Message Notification User Guide**.
Synchronization Delay Threshold	During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.

Parameter	Description
RTO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the DR database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the RTO delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RPO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the service database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient. • In the early stages of an incremental disaster recovery, the synchronization delay is long because a large quantity of data is awaiting synchronization. In this case, no notifications will be sent.
Stop Abnormal Tasks After	Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is **14**. **NOTE** • You can set this parameter only for pay-per-use tasks. • Tasks in the abnormal state are still charged. If tasks remain in the abnormal state for a long time, they cannot be resumed. Abnormal tasks run longer than the period you set (unit: day) will automatically stop to avoid unnecessary fees.

Step 8 After the task is submitted, view and **manage it** on the **Disaster Recovery Management** page.

- You can view the task status. For more information about task status, see **Task Statuses**.
- You can click in the upper-right corner to view the latest task status.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.

----End

Helpful Links

- **Supported Databases**
- **Preparations**
- **DR Overview**

3.2 Querying the DR Progress

After a DR task starts, you can check the DR progress.

Prerequisites

- You have logged in to the DRS console.
- A DR task has been created and started.

Procedure

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the displayed page, click the **Disaster Recovery Progress** tab to view the DR progress. When the data initialization is complete, the initialization progress is displayed as 100%.

- On the **Disaster Recovery Progress** tab, you can view the DR synchronization delay.
- You can also view the DR synchronization delay on the **Disaster Recovery Management** page. When the synchronization delay exceeds the preset or default threshold, the value of the synchronization delay is displayed in red in the task list.
- When the delay is 0, data is synchronized from the service database to the DR database in real-time. You can view more metrics, such as RPO and RTO, on the **Disaster Recovery Monitoring** tab.

NOTE

"Delay" refers to the delay from when the transaction was submitted to the source database to when it is synchronized to the destination database and executed.

Transactions are synchronized as follows:

1. Data is extracted from the source database.
2. The data is transmitted over the network.
3. DRS parses the source logs.
4. The transaction is executed on the destination database.

If the delay is 0, the source database is consistent with the destination database, and no new transactions need to be synchronized.

> **CAUTION**
>
> Frequent DDL operations, ultra-large transactions, and network problems may result in excessive synchronization delay.

----End

3.3 Viewing DR Logs

DR logs refer to the warning-, error-, and info-level logs generated during the DR process. This section describes how to view DR logs to locate and analyze database problems.

Prerequisites

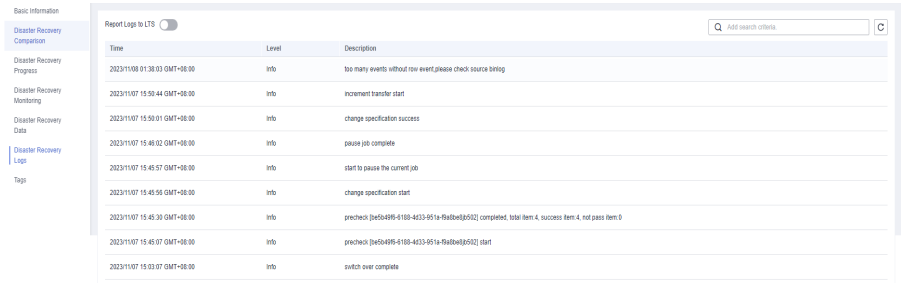
You have logged in to the DRS console.

Procedure

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the displayed page, click **Disaster Recovery Logs** to view the logs generated during DR.

Figure 3-17 Viewing DR Logs



In addition, DRS can interconnect with Log Tank Service (LTS). After you enable log reporting to LTS, all logs generated by DRS instances will be uploaded to LTS for management. For details, see **Log Reporting**.

----End

3.4 Comparing DR Items

Comparison Scenarios

DR item comparison: You can compare DR items to check data consistency between the service database and DR database. Currently, you can compare the following items during DR:

- Object-level comparison: compares databases, events, indexes, tables, views, stored procedures, functions, and triggers.
- Data-level comparison is classified into row comparison and value comparison.
  - Row comparison: It helps you compare the number of rows in the tables to be synchronized. This comparison method is recommended because it is fast.
  - Value comparison: It helps you check whether data in the synchronized table is consistent. The comparison process is relatively slow.

  To ensure that the comparison results are valid, compare data during off-peak hours by select **Start at a specified time** or compare cold data that is infrequently modified.
- Account comparison: It compares usernames and permissions of the source and destination databases.

When you check data consistency, compare the number of rows first. If the number of rows are inconsistent, you can then compare the data in the table to determine the inconsistent data.

Table 3-11 Supported comparison methods

DR Direction	Data Flow	Object-level Comparison	Row Comparison	Value Comparison	Dynamic Comparison	Account-level Comparison
Current cloud as standby	MySQL->MySQL	Supported	Supported	Supported	Supported	Supported
Current cloud as active	MySQL->MySQL	Supported	Supported	Supported	Supported	Supported
Current cloud as standby	MySQL->GaussDB(for MySQL)	Supported	Supported	Supported	Supported	Supported

DR Direction	Data Flow	Object-level Comparison	Row Comparison	Value Comparison	Dynamic Comparison	Account-level Comparison
Current cloud as standby	DDM -> DDM	Supported	Supported	Not supported	Not supported	Not supported
Current cloud as active	DDM -> DDM	Supported	Supported	Not supported	Not supported	Not supported
Current cloud as standby	GaussDB(for MySQL)->GaussDB(for MySQL)	Supported	Supported	Supported	Supported	Supported
Current cloud as active	GaussDB(for MySQL)->GaussDB(for MySQL)	Supported	Supported	Supported	Supported	Supported
Dual-Active DR	MySQL->MySQL	Supported	Supported	Supported	Not supported	Supported
Dual-Active DR	GaussDB(for MySQL)->GaussDB(for MySQL)	Supported	Supported	Supported	Not supported	Supported

Constraints

- If DDL operations were performed on the service database, you need to compare the objects again to ensure the accuracy of the comparison results.
- If data in the DR database is modified separately, the comparison results may be inconsistent.
- Currently, only tables with primary keys support value comparison. For tables that do not support value comparison, you can compare rows. Therefore, you can compare data by row or value based on scenarios.
- The DRS task cannot be suspended during value comparison. Otherwise, the comparison task may fail.

- Some data types do not support value comparison. For details, see **Which Data Types Does Not Support Content Comparison?**
- To prevent resources from being occupied for a long time, DRS limits the row comparison duration. If the row comparison duration exceeds the threshold, the row comparison task stops automatically. If the service database is a relational database, the row comparison duration is limited within 60 minutes. If the service database is a non-relational database, the row comparison duration is limited within 30 minutes.
- To avoid occupying resources, the comparison results of DRS tasks can be retained for a maximum of 60 days. After 60 days, the comparison results are automatically cleared.
- If you want to compare values and the DRS task you create supports value comparison, select a large specification for your DRS instance when creating the DRS task.

Impact on Databases

- Object comparison: System tables of the source and destination databases are queried, occupying about 10 sessions. The database is not affected. However, if there are a large number of objects (for example, hundreds of thousands of tables), the database may be overloaded.
- Row comparison: The number of rows in the source and destination databases is queried, which occupies about 10 sessions. The SELECT COUNT statement does not affect the database. However, if a table contains a large amount of data (hundreds of millions of records), the database will be overloaded and the query results will be returned slowly.
- Value comparison: All data in the source and destination databases is queried, and each field is compared. The query pressure on the database leads to high I/O. The query speed is limited by the I/O and network bandwidth of the source and destination databases. Value comparison occupies one or two CPUs, and about 10 sessions.
- Account comparison: The accounts and permissions of the source and destination databases are queried, which does not affect the database.

Estimated Comparison Duration

- Object comparison: Generally, the comparison results are returned within several minutes based on the query performance of the source database. If the amount of data is large, the comparison may take dozens of minutes.
- Row comparison: The SELECT COUNT method is used. The query speed depends on the database performance.
- Value comparison: If the database workload is not heavy and the network is normal, the comparison speed is about 5 MB/s.
- Account comparison: The results are returned with the object-level comparison results. If the number of objects is small, the results are returned in several minutes.

Prerequisites

- You have logged in to the DRS console.

- A DR task has been started.

Procedure

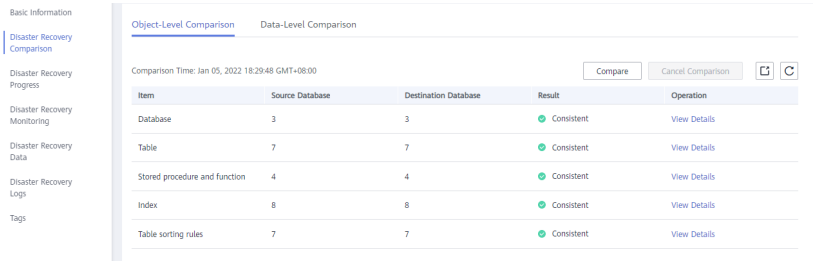
Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the **Disaster Recovery Comparison** tab, compare the service and DR databases.

1. Check the integrity of the database object.

   Click **Validate Objects**. On the **Object-Level Comparison** tab, click **Compare**. Wait for a while and click , and view the comparison result of each comparison item.

   Figure 3-18 Comparing objects

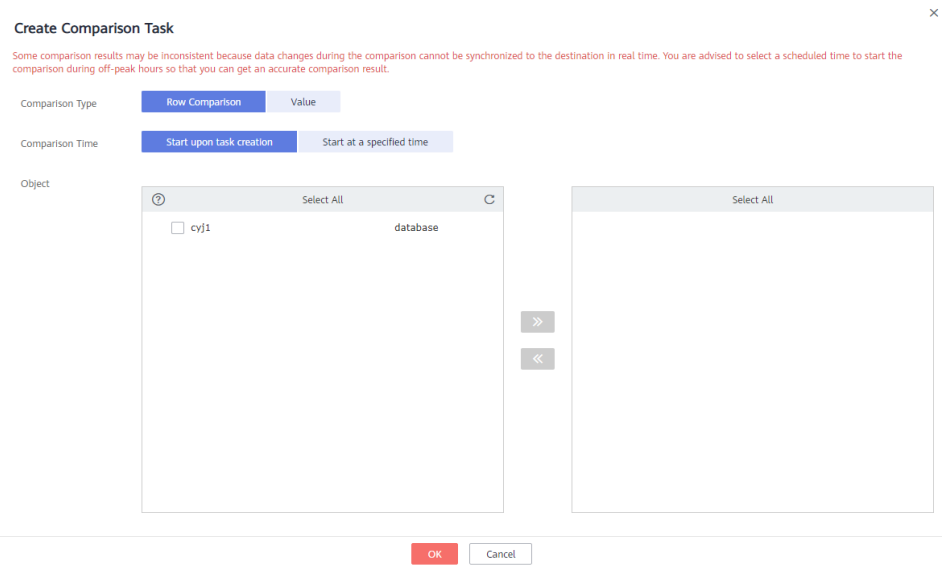


   Locate a comparison item you want to view and click **View Details** in the **Operation** column.

2. After the check is complete, compare the number of rows and values.

   On the **Data-Level Comparison** tab, click **Create Comparison Task**. In the displayed dialog box, specify **Comparison Method**, **Comparison Type**, **Comparison Time**, and **Object**. Then, click **OK**.

   Figure 3-19 Creating a comparison task



- **Comparison Type**: compares rows and values.
- **Comparison Method**: DRS provides static and dynamic comparison methods.
  - **Static**: All data in the source and destination databases is compared. The comparison task ends as the comparison is completed. Static comparison can only be performed when there are no ongoing services.
  - **Dynamic**: All data in the source database is compared with that in the destination database. After the comparison task is complete, incremental data in the source and destination databases is compared in real time. A dynamic comparison can be performed when data is changing.

  NOTE

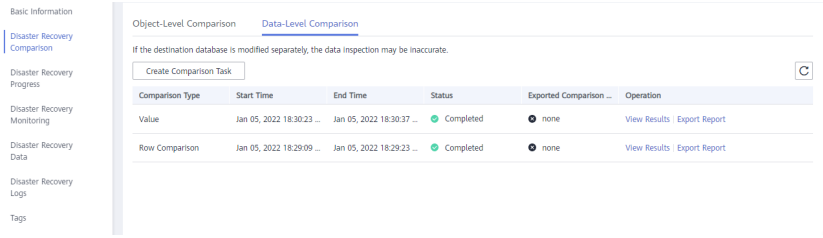
  - Currently, only MySQL and GaussDB(for MySQL) support the comparison mode.
  - New tables cannot be created in the service database during dynamic comparison. If you want to create a table in the service database, cancel the dynamic comparison first. After the new table is created and real-time DR is performed, restart the dynamic comparison.
- **Comparison Time**: You can select **Start upon task creation** or **Start at a specified time**. There is a slight difference in time between the source and destination databases during synchronization. Data inconsistency may occur. You are advised to compare migration items during off-peak hours for more accurate results.
- **Object**: You can select objects to be compared based on the scenarios.

NOTE

- Data-level comparison cannot be performed for tasks in initialization.

3. After the comparison creation task is submitted, the **Data-Level Comparison** tab is displayed. Click to refresh the list and view the comparison result of the specified comparison type.

Figure 3-20 Viewing the data-level comparison result



4. To view the comparison details, locate the target comparison type and click **View Results** in the **Operation** column. On the displayed page, locate a pair of service and DR databases, and click **View Details** in the **Operation** column to view detailed comparison results.

Figure 3-21 Row comparison details

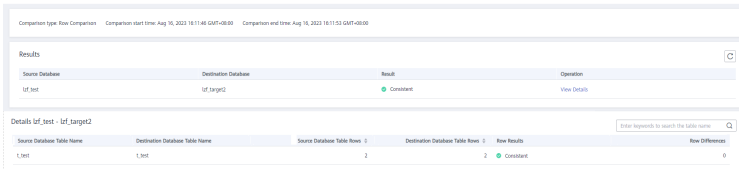
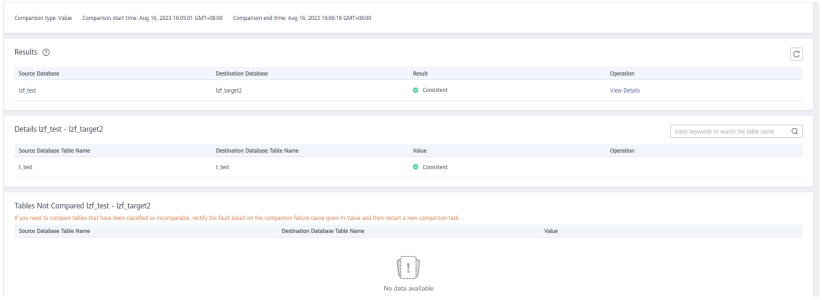


Figure 3-22 Value comparison details

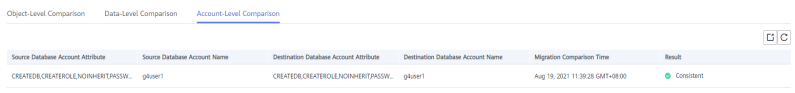


NOTE

- You can also view comparison details of canceled comparison tasks.
- You can sort the row comparison results displayed on the current page in ascending or descending order based on the number of rows in the source database table or the destination database table.
- If a negative number is displayed in the **differences** column, the number of rows in the destination database table is greater than that in the source database table. If a positive number is displayed in the **differences** column, the number of rows in the source database table is greater than that in the destination database table.

5. Check the database accounts and permissions. Click the **Account-Level Comparison** tab to view the comparison results of database accounts and permissions.

Figure 3-23 Account-level comparison



NOTE

- Account comparison cannot be performed for tasks in the initialization phase.

----End

3.5 Task Life Cycle

3.5.1 Viewing DR Data

The data synchronization information is recorded during a disaster recovery. You can check the integrity of DR data after synchronization.

DRS allows you to view the initialization progress and of DR data health report on the management console.

Prerequisites

- You have logged in to the DRS console.
- You have created a DR task.

Procedure

NOTE

In the task list, only tasks created by the current login user are displayed. Tasks created by different users of the same tenant are not displayed.

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the **Basic Information** tab, click the **Disaster Recovery Data** tab.

- Initialization Progress

  Initialization Progress shows the historical data import progress during the disaster recovery environment creation. After the historical data is imported, the initialization is complete, and data on this tab will not be updated anymore.

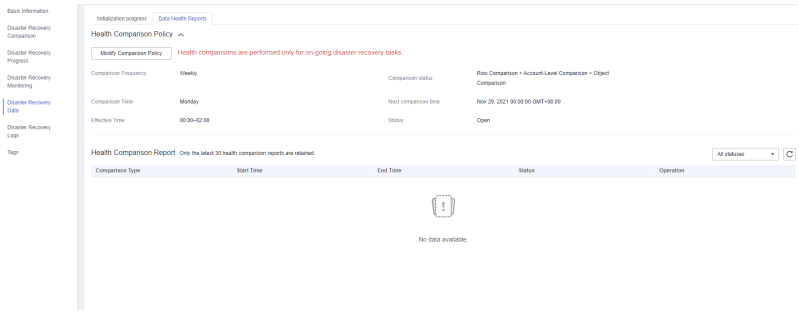
- Data Health Reports

  Data Health Reports periodically shows the data comparison result between the primary and disaster recovery instances, helping you review the data health status in the disaster recovery environment.

  NOTE

  - Data comparison is performed only for disaster recovery tasks.
  - Only the latest 30 health comparison reports are retained.
  - The periodical health report helps you learn the data consistency between the primary and standby instances. To avoid performance loss caused by long-term comparison of the primary instance, you can use **DR comparison** to compare large tables (for example, tables with more than 100 million rows).

  Figure 3-24 Data Health Reports

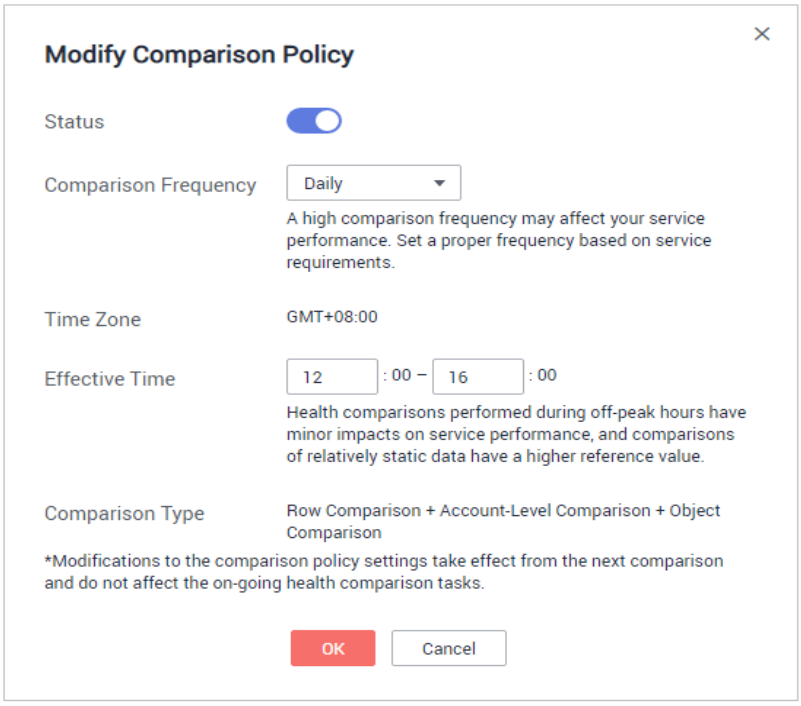
  

  - Modify the comparison policy.

    Modifying the comparison policy does not affect the current health comparison task. The modification takes effect upon the next comparison.

- In the **Health Comparison Policy** area on the **Data Health Reports** tab, click **Modify Comparison Policy**.

  Figure 3-25 Modify Comparison Policy

- On the **Modify Comparison Policy** page, set the required parameters.
  - **Status**: After the health comparison policy is disabled, the health comparison will not be performed, and historical health reports can still be viewed.
  - **Comparison Frequency**: The comparison can be performed weekly or daily.
  - **Comparison Time**: When **Comparison Frequency** is set to **Weekly**, you can set one or more days from Monday to Sunday as the comparison time.
  - **Time Zone**: The default value is the local time zone.
  - **Effective Time**: Specifies the time period during which the comparison policy takes effect. You are advised to perform the comparison in off-peak hours. If the health comparison is not complete within the validity period, the health comparison is automatically interrupted. You can still view the health comparison results of the completed task.
  - **Comparison Type**: Rows, accounts, and objects are compared by default.
- Click **OK**.

  After the modification is successful, the new policy applies to the following comparison tasks. You can cancel the ongoing tasks but

the health reports of the comparison tasks that have been completed can still be viewed.

----End

3.5.2 Modifying Task Information

After a DR task is created, you can modify task information to identify different tasks.

The following task information can be edited:

- Task name
- Description
- SMN Topic
- Synchronization delay threshold
- Number of days when an abnormal task is stopped
- Task start time

Prerequisites

You have logged in to the DRS console.

Procedure

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the **Basic Information** tab, locate the information to be modified in the **Task Information** area.

- You can click  to modify the task name, SMN topic, delay threshold, the time to stop abnormal tasks, and description.
  - To submit the change, click  .
  - To cancel the change, click  .

Table 3-12 Real-time DR task information

Task Information	Description
Task Name	The task name must start with a letter and consist of 4 to 50 characters. It can contain only letters, digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters ! <>&'\"
SMN Topic	You can apply for a topic on the SMN console and add a subscription. For details, see **Simple Message Notification User Guide**.

Task Information	Description
Synchronization delay threshold	The delay ranges from 0s to 3600s. **NOTE** If the delay threshold is set to 0, no notifications will be sent to the recipient.
Stop Abnormal Tasks After	The value must range from 14 to 100. The default value is 14. **NOTE** You can set this parameter only for pay-per-use tasks.

- You can modify the task start time only when the task is in the **Pending start** status.

  In the **Task Information** area, click **Modify** in the **Scheduled Start Time** field. On the displayed page, specify the scheduled start time and click **OK**.

Step 3 View the change result on the **Basic Information** tab.

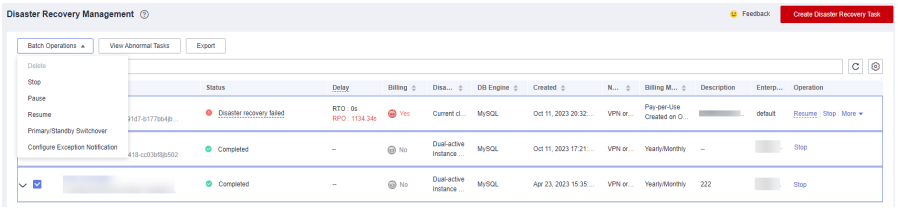
----End

Configuring Exception Notifications

Step 1 On the **Disaster Recovery Management** page, select the task for which you want to modify the exception notification.

Step 2 Click **Batch Operations** in the upper left corner and choose **Configure Exception Notification**.

Figure 3-26 Batch Operations



Step 3 In the displayed dialog box, modify the required parameter and click **Confirm**.

----End

3.5.3 Modifying Connection Information

During the disaster recovery, you may change the password of the service or DR database. As a result, the data DR, data comparison, task pause, resume, primary/standby switchover, and stopping may fail. In this case, you need to change the password on the DRS console and resume the task.

You can modify the following information:

- Database password
- Database IP address
- Database port

- Database username

Constraints

- You can change the IP address, port, and username during the disaster recovery phase only for a single-active DR task with MySQL or GaussDB(for MySQL) serving as the source and IP address entered for the connection test. If the IP address, port number, or username changes due to some operations on the service database, you can use this function to update the information.
- The function of changing an IP address applies to the scenario where the IP address of the service database changes. The IP addresses before and after the change must belong to the same data instance. Otherwise, the task may fail or data may be inconsistent.
- After the connection information is changed, the change takes effect immediately, and the data in the DR database is not cleared.

Procedure

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the **Basic Information** tab, click **Modify Connection Details** in the **DR Information** area.

Step 3 In the displayed dialog box, change the passwords of the source and destination databases and click **OK**.

----End

3.5.4 Modifying the Flow Control Mode

DRS allows you to change the flow control mode for a task. Currently, only the following DR tasks support this function.

- MySQL->MySQL
- MySQL->GaussDB(for MySQL)
- DDM->DDM
- GaussDB(for MySQL)->GaussDB(for MySQL)

Constraints

- The flow control mode limits the maximum traffic speed in seconds. The actual statistical value may be lower than the flow rate because the statistical value may decrease due to network fluctuation.
- The flow control mode takes effect only in the DR initialization phase.

Prerequisites

- You have logged in to the DRS console.
- A disaster recovery task has been created and not started.

Method 1

Step 1 In the **Flow Control Information** area on the **Basic Information** tab, click **Modify**.

Step 2 In the displayed dialog box, modify the settings.

----End

Method 2

Step 1 In the task list on the **Disaster Recover Management** page, locate the target task and choose **More** > **Speed** or **Speed** in the **Operation** column.

Step 2 In the displayed dialog box, modify the settings.

----End

3.5.5 Editing a DR Task

For a DR task that has been created but not started, DRS allows you to edit the configuration information of the task, including the source and destination database details. For DR tasks in the following statuses, you can edit and submit the tasks again.

- Creating
- Configuration

Prerequisites

You have logged in to the DRS console.

Method 1

Step 1 In the task list on the **Disaster Recovery Management** page, locate the target task and click **Edit** in the **Operation** column.

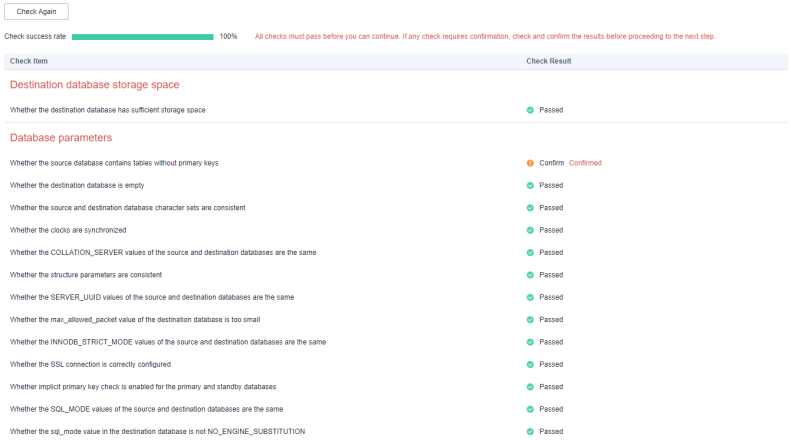
Step 2 On the **Configure Source and Destination Databases** page, enter information about the service and DR databases and click **Next**.

Step 3 On the **Check Task** page, check the DR task.

- If any check fails, review the failure cause and rectify the fault. After the fault is rectified, click **Check Again**.

  For details about how to handle check failures, see **Solutions to Failed Check Items** in *Data Replication Service User Guide*.

Figure 3-27 Pre-check



- If the check is complete and the check success rate is 100%, go to the **Compare Parameter** page.

  NOTE

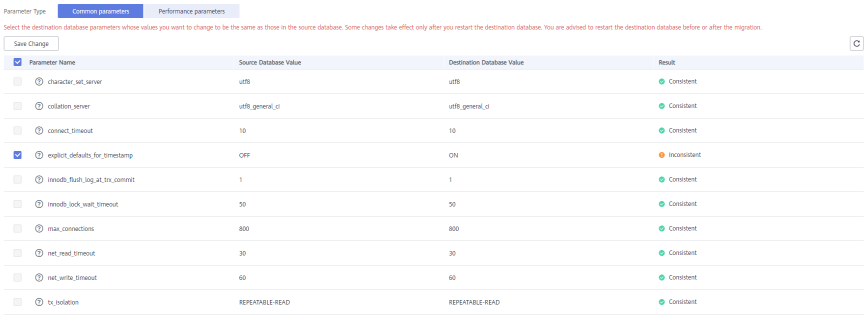
  You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

Step 4 Compare the parameters.

The parameter comparison function helps you check the consistency of common parameters and performance parameters between service and DR databases and show inconsistent values. You can determine whether to use this function based on service requirements. It mainly ensures that services are not affected after the DR task is completed.

- This process is optional, so you can click **Next** to skip the comparison.
- Compare common parameters:
  - For common parameters, if the parameters in the service database are different from those in the DR database, click **Save Change** to make the parameters of the DR database be the same as those in the service database.

    Figure 3-28 Modifying common parameters

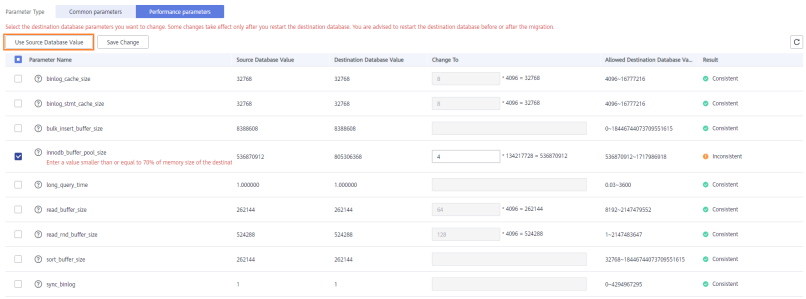
  - Performance parameter values in both the service and DR databases can be the same or different.
    - If you need to adjust the performance parameters, enter the value in the **Change to** column and click **Save Change**.

- If you want to make the performance parameter values of the source and destination database be the same:

  1) Click **Use Source Database Value**.

     DRS automatically makes the DR database values the same as those of the service database.

     Figure 3-29 One-click modification

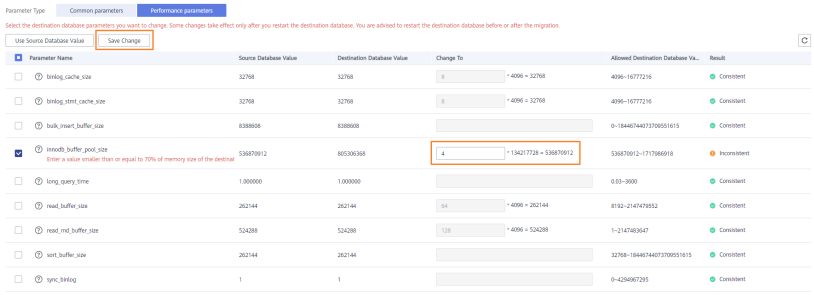
     NOTE

     You can also manually enter the value as required.

  2) Click **Save Change**.

     DRS changes the DR database parameter values based on your settings. After the modification, the comparison results are automatically updated.

     Figure 3-30 One-click modification

     Some parameters in the DR database cannot take effect immediately, so the comparison result is temporarily inconsistent. Restart the DR database before the DR task is started or after the DR task is completed. To minimize the impact of database restart on your services, restart the DR database at the scheduled time after the disaster recovery is complete.

     For details about parameter comparison, see **Parameters for Comparison** in the *Data Replication Service User Guide*.

  3) Click **Next**.

Step 5 On the displayed page, specify **Start Time**, **Send Notification**, **SMN Topic**, **Synchronization Delay Threshold**, **RPO Synchronization Delay Threshold**, **RTO**

Synchronization Delay Threshold, **Stop Abnormal Tasks After** and DR instance details. Then, click **Submit**.

Figure 3-31 Task startup settings

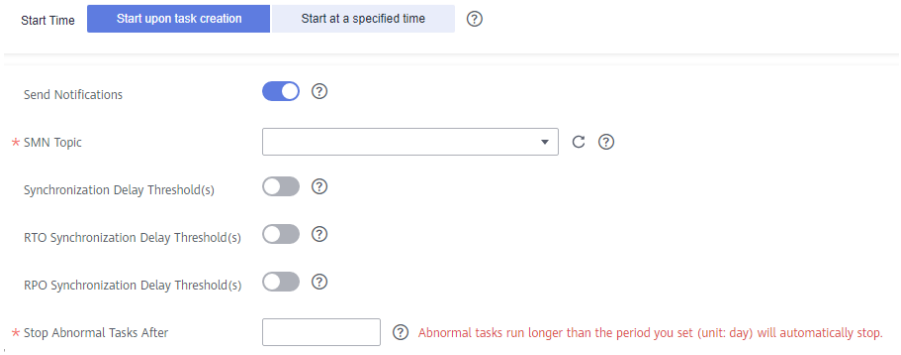


Table 3-13 Task and recipient description

Parameter	Description
Start Time	Set **Start Time** to **Start upon task creation** or **Start at a specified time** based on site requirements. **NOTE** Starting a DR task may slightly affect the performance of the service and DR databases. You are advised to start a DR task during off-peak hours.
Send Notifications	SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.
SMN Topic	This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber. For details, see **Simple Message Notification User Guide**.
Synchronization Delay Threshold	During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.

Parameter	Description
RTO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the DR database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the RTO delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient.
RPO Synchronization Delay Threshold	If the synchronization delay from the DRS instance to the service database exceeds the threshold you specify, DRS will notify specified recipients. The value ranges from 0 to 3,600. To avoid repeated alarms caused by the fluctuation of delay, an alarm is sent only after the delay has exceeded the threshold for six minutes. **NOTE** • Before setting the delay threshold, enable **Send Notification**. • If the delay threshold is set to 0, no notifications will be sent to the recipient. • In the early stages of an incremental disaster recovery, the synchronization delay is long because a large quantity of data is awaiting synchronization. In this case, no notifications will be sent.
Stop Abnormal Tasks After	Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is **14**. **NOTE** • You can set this parameter only for pay-per-use tasks. • Tasks in the abnormal state are still charged. If tasks remain in the abnormal state for a long time, they cannot be resumed. Abnormal tasks run longer than the period you set (unit: day) will automatically stop to avoid unnecessary fees.

Step 6 After the task is submitted, view and **manage it** on the **Disaster Recovery Management** page.

- You can view the task status. For more information about task status, see **Task Statuses**.
- You can click in the upper-right corner to view the latest task status.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.

----End

Method 2

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the displayed page, click **edit this task** to go to the **Configure Source and Destination Databases** page.

Step 3 Perform **Step 2** through **Step 6** in method 1.

----End

3.5.6 Resuming a DR Task

A fault may occur during DR due to external factors, such as insufficient storage space.

NOTE

- If a DR task fails due to non-network problems, the system will automatically resume the task three times by default. If the failure persists, you can resume the task manually.
- If the DR task fails due to network problems, the system will automatically resume the task until the task is restored.

Prerequisites

- You have logged in to the DRS console.
- A DR task has been created.

Method 1

In the task list on the **Disaster Recovery Management** page, locate the target task and click **Resume** in the **Operation** column.

Method 2

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the displayed page, click the **Migration Progress** tab, and click **Resume** in the upper right corner.

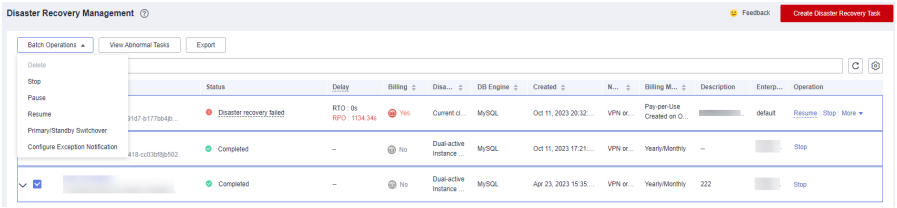
----End

Resume Tasks

Step 1 On the **Disaster Recovery Management** page, select the tasks to be resumed.

Step 2 Click **Batch Operations** in the upper left corner and choose **Resume**.

Figure 3-32 Batch Operations



Step 3 In the displayed dialog box, confirm the task information and click **Yes**.

----End

3.5.7 Pausing a DR Task

You can pause the DR tasks if they may cause buffer overflow or network congestion during peak hours.

You can pause the following DR tasks:

- MySQL->MySQL
- MySQL->GaussDB(for MySQL)
- GaussDB(for MySQL)>GaussDB(for MySQL)

Prerequisites

- You have logged in to the DRS console.
- The DR task is running properly.

Pausing a Task

Step 1 In the task list on the **Disaster Recovery Management** page, locate the target task and click **Pause** in the **Operation** column.

Step 2 In the displayed **Pause Task** dialog box, select **Pause log capturing** and click **Yes**.

NOTE

- After the task is paused, the status of the task becomes **Paused**.
- After you select **Pause log capturing**, the DRS instance will no longer communicate with the source and destination databases. If the pause duration is too long, the task may fail to be resumed because the logs required by the source database expire. You are not advised pausing a task for more than 24 hours. For details, check the corresponding log configuration.
- You can use the resumable transfer function to continue the DR task.

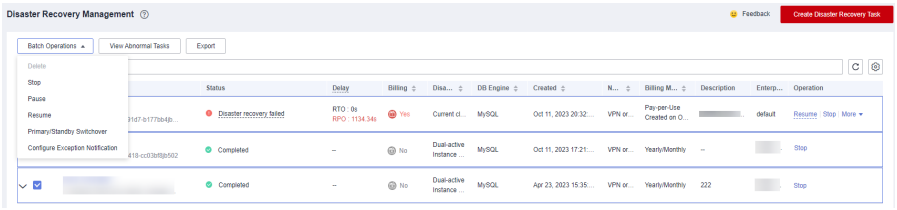
----End

Pausing Tasks

Step 1 On the **Disaster Recovery Management** page, select the tasks to be paused.

Step 2 Click **Batch Operations** in the upper left corner and choose **Pause**.

Figure 3-33 Batch Operations



Step 3 In the displayed dialog box, confirm the task information and click **Yes**.

----End

3.5.8 Viewing DR Metrics

DRS monitors the DB instance performance and the migration progress. With the monitoring information, you can determine the data flow health status, data integrity, and data consistency. If both RPO and RTO are 0, data has been completely migrated to the DR database. Then, you can determine whether to perform a switchover.

Prerequisites

- You have logged in to the DRS console.
- You have created a DR task.

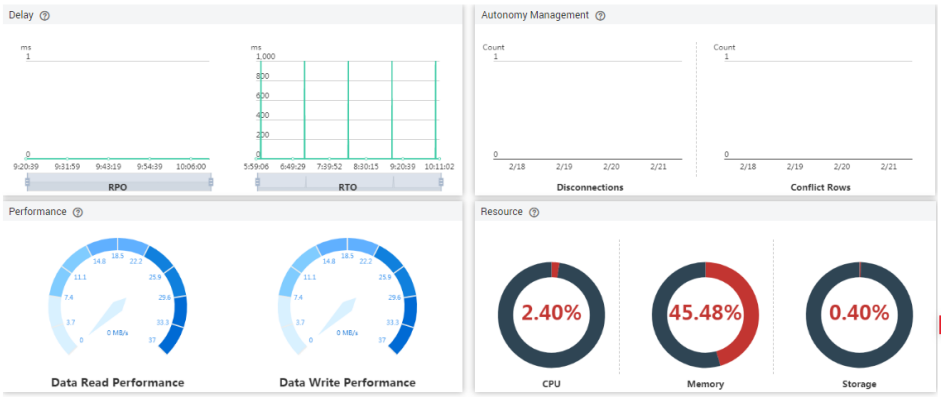
Procedure

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the **Basic Information** tab, click the **Disaster Recovery Monitoring** tab.

- Recovery Point Objective (RPO) measures the consistency between the data in the service database and the data in the DRS instance. When RPO is 0, all the data in the service database has been migrated to the DRS instance.
- Recovery Time Objective (RTO) measures the amount of data being transmitted. When RTO is 0, all transactions on the DRS instance have been completed on the DR database.
- Delay: Monitors the historical RPO and RTO, which helps predict the amount of lost data if a disaster occurs. You can pay attention to the following time ranges during which:
  - The RPO or RTO is high for a long time.
  - The RPO or RTO is consistently high or spiking high on a regular basis.
- Autonomy Management: Monitors the following DRS intelligent autonomy capabilities:
  - Number of times that DRS automatically resumes data transfer after a network is disconnected
  - Number of times that DRS automatically overwrites old data with the latest data when a data conflict occurs
- Performance: You can use performance monitoring to help diagnose the network quality.
- Resource: You can use resource monitoring to help determine whether to scale up the DRS instance specifications.

Figure 3-34 DR monitoring



----End

3.5.9 Performing a Primary/Standby Switchover for DR Tasks

DRS supports primary/standby switchover for DR tasks. If both RPO and RTO are 0, data has been completely migrated to the DR database. Then, you can determine whether to perform a switchover.

- RPO measures the difference between the data in the service database and the data in the DRS instance. When RPO is 0, all the data in the service database has been migrated to the DRS instance.
- RTO measures the amount of data being transmitted. When RTO is 0, all transactions on the DRS instance have been completed on the DR database.

Prerequisites

- You have logged in to the DRS console.
- You have created a DR task.

Primary/Standby Switchover

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

Step 2 On the **Basic Information** tab, click the **Disaster Recovery Monitoring** tab.

Step 3 A primary/secondary switchover can be performed only when the task status is disaster recovery in progress. Click **Promote Current Cloud** to promote the current instance to the service database. Click **Demote Current Cloud** to demote the current instance to the disaster recovery database.

The DR relationship involves only one primary database. During a primary/standby switchover, ensure that there is no data written to the database that will be the standby node, and no data will be written to the standby node in the future. The data of the standby node is synchronized only from the primary node. Any other write operations will pollute the data in the standby database, data conflicts occur in the DR center and cannot be resolved.

NOTE

Data DR from DDM to DDM involves multiple tasks and does not support primary/standby switchover on the **Disaster Recovery Monitoring** tab. You can perform a switchover by referring to **Performing Primary/Standby Switchovers in Batches**.

Figure 3-35 DR monitoring

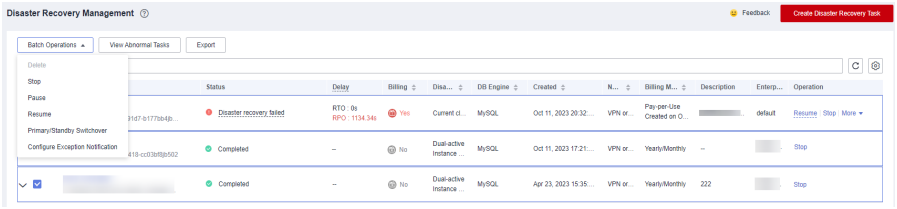
----End

Performing Primary/Standby Switchovers in Batches

Step 1 On the **Disaster Recovery Management** page, select the tasks.

Step 2 Click **Batch Operations** in the upper left corner and choose **Primary/Standby Switchover**.

Figure 3-36 Batch Operations



Step 3 In the displayed dialog box, confirm the task information and click **Yes**.

----End

3.5.10 Exchanging the DR Direction

In dual-active DR, only forward tasks support DDL execution to prevent DDL loopback. DRS allows you to exchange the direction of a DR task. You can use this function to change the task role to enable DDL execution on backward tasks.

Constraints

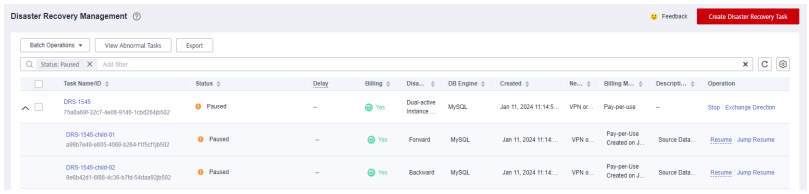
- This function is available only for dual-active DR tasks.
- The direction can be exchanged only when both the forward and backward tasks are paused.
- You need to resume the task to apply the change.

Procedure

Step 1 On the **Disaster Recovery Management** page, locate the paused dual-active DR task.

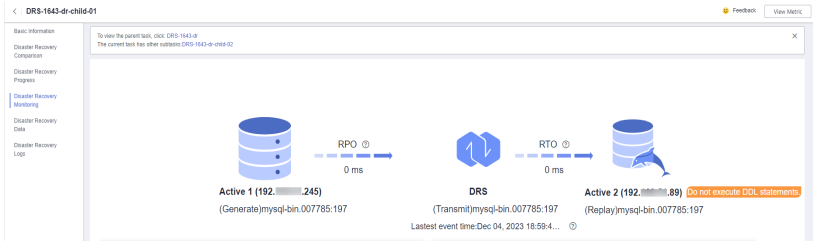
Subtask 1 is a forward task.

Figure 3-37 Before direction exchange



View the DR monitoring of subtask 1. The DDL execution is disabled on active node 2.

Figure 3-38 DR monitoring before direction exchange

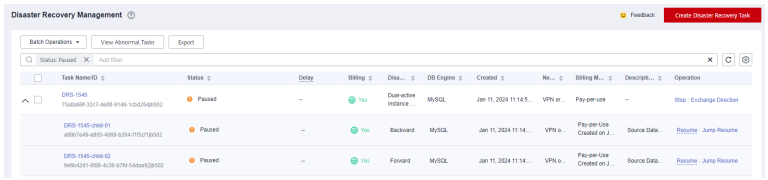


Step 2 Click **Exchange Direction** in the **Operation** column of the task.

Step 3 In the displayed dialog box, click **Yes**.

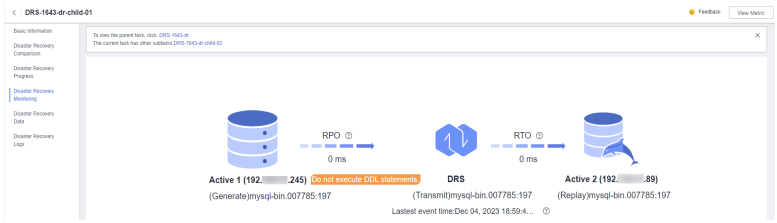
Step 4 After the direction exchange, view that the DR relationship of subtask 1 changes and subtask 1 becomes a backward task.

Figure 3-39 After direction exchange



View the DR monitoring of subtask 1. The DDL execution is disabled on active node 1.

Figure 3-40 DR monitoring after direction exchange



Step 5 Click **Resume** in the **Operation** column of the subtask.

----End

3.5.11 Changing Specifications

You can change the DRS task specifications based on your service requirements. After the specification change starts, the task enters the **Changing specifications** state and data disaster recovery is suspended. After the specification change is complete, the task is automatically resumed. Only whitelisted users can use this function. You need to submit a service ticket to apply for this function.

Constraints

- You can change the task specifications only when your account balance is more than $0 USD.
- DRS allows you to upgrade specifications only for real-time DR tasks from MySQL to MySQL, from MySQL to GaussDB(for MySQL), and from GaussDB(for MySQL) to GaussDB(for MySQL). Task specifications cannot be downgraded.
- DRS allows you to change the specifications of only tasks in the **Initializing** or **Disaster recovery in progress** state.
- You are advised to change the task specifications during off-peak hours.
- After the specification change starts, the task is suspended. The task is automatically resumed after the change is complete.
- It takes about 5 to 10 minutes to change the task specifications.

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 Choose **Databases** > **Data Replication Service**. The **Data Replication Service** page is displayed.

Step 4 On the **Disaster Recovery Management** page, select the target task and choose **More** > **Change Specifications** in the **Operation** column.

Step 5 On the displayed page, select the desired specifications, perform a pre-check, and click **Next**.

Step 6 Confirm specifications.

- If you need to modify your settings, click **Previous**.
- For pay-per-use instances, click **Change**.

  To view the cost incurred by the specifications change, choose **Billing Center** > **Cost Bills** in the upper right corner.
- For yearly/monthly DB instances, click **Change**. On the displayed page, click **Pay**. You can change the specifications only after the payment is successful.

Step 7 View the task specification change result.

After the application is submitted, click **Back to Task List**. On the **Disaster Recovery Management** page, the instance status is **Changing specifications**.

After the task status changes from **Changing specifications** to another status, you can view the instance specifications on the **Basic Information** page to check

whether the change is successful. Alternatively, you can view the change logs on the **Synchronization Logs** page to whether the change is successful.

- **change specification start**: indicates that the specification change starts.
- **change specification success**: indicates that the specifications are changed.
- **change specification failed**: indicates that the specifications fail to be changed.

----End

3.5.12 Unsubscribing from a Yearly/Monthly Task

To delete a DRS task billed on the yearly/monthly basis, you need to unsubscribe the order.

Prerequisites

- You have logged in to the DRS console.
- The billing mode of the current DRS instance is yearly/monthly.

Method 1

Unsubscribe from a yearly/monthly task on the **Disaster Recovery Management** page.

Step 1 Log in to the management console.

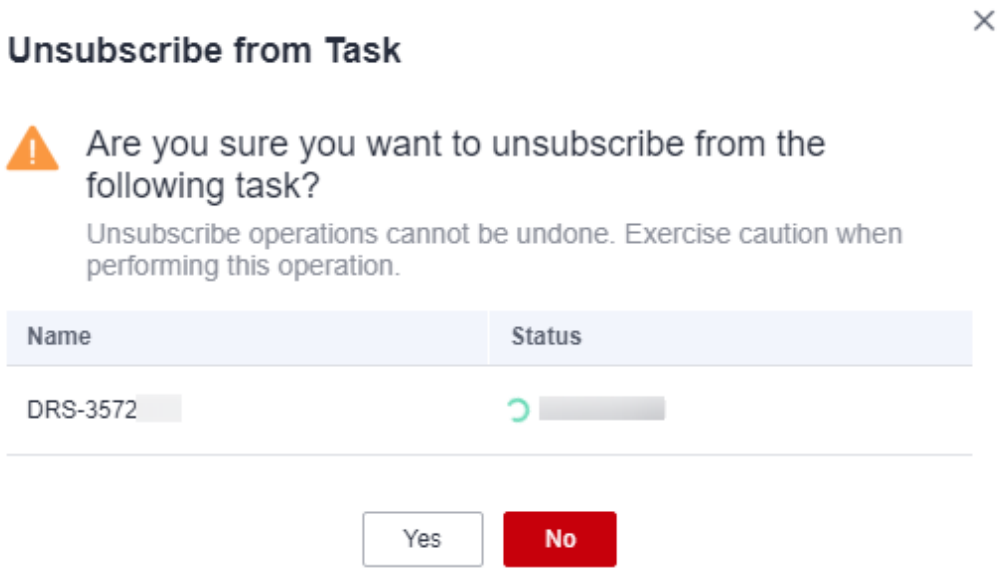
Step 2 Click  in the upper left corner and select a region and project.

Choose **Databases** > **Data Replication Service**. The **Data Replication Service** page is displayed.

Step 3 On the **Disaster Recovery Management** page, select the target task and choose **More** > **Unsubscribe** in the **Operation** column.

Step 4 In the displayed dialog box, click **Yes**. The **Unsubscribe from Resource** page is displayed.

Figure 3-41 Unsubscribing from a task



Step 5 On the **Unsubscribe from Resource** page, verify the information about the instance to be unsubscribed, specify a reason, select the ckeck box, and click **Confirm**.

NOTE

After a DRS instance is unsubscribed, the DRS task ends immediately. Ensure that data DR is complete or the DRS instance is no longer used.

Step 6 In the displayed dialog box, click **Yes**.

----End

Method 2

Unsubscribe from a yearly/monthly task on the **Billing Center** page.

Step 1 Log in to the management console.

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

Step 3 Choose **Databases** > **Data Replication Service**. The **Data Replication Service** page is displayed.

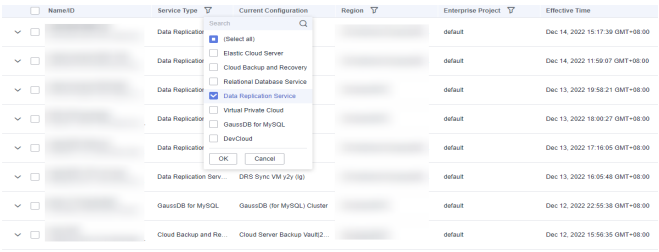
Step 4 Click **Billing & Costs** from the top menu bar. The **Billing Center** page is displayed.

Step 5 In the navigation pane, choose **Orders** > **Unsubscriptions**.

Step 6 On the displayed page, select the order to be unsubscribed and click **Unsubscribe** in the **Operation** column.

- You can select DRS in the **Service Type** to filter all DRS orders.

Figure 3-42 Filtering all orders



- Alternatively, search for target orders by name, order No., or ID in the search box.

Step 7 On the displayed page, confirm the order to be unsubscribed from and select a reason. Then, click **Confirm**.

For unsubscription details, see **Unsubscription Rules**.

Step 8 In the displayed dialog box, click **Yes**.

NOTE

After a DRS instance is unsubscribed, the DRS task ends immediately. Ensure that data synchronization is complete or the DRS instance is no longer used.

----End

3.5.13 Stopping a DR Task

When the DR task is complete or no longer needed, you can stop the DR task. You can stop a task in any of the following statuses:

- Creating
- Configuration
- Initializing
- Disaster recovery in progress
- Paused
- Disaster recovery failed

NOTICE

- For a task in the **Configuration** state, it cannot be stopped if it fails to be configured.
- After a task is stopped, it cannot be resumed.

Procedure

Step 1 In the task list on the **Disaster Recovery Management** page, locate the target task and click **Stop** in the **Operation** column.

Step 2 In the displayed dialog box, click **OK**.

NOTE

- If the task status is abnormal (for example, the task fails or the network is abnormal), DRS will select **Forcibly stop task** to preferentially stop the task to reduce the waiting time.
- Forcibly stopping a task will release DRS resources. Check whether the synchronization is affected.
- To stop the task properly, restore the DRS task first. After the task status becomes normal, click **Stop**.

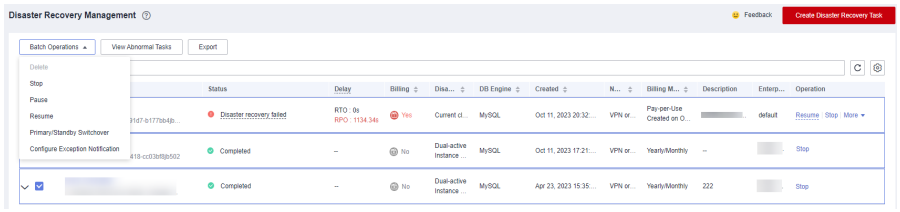
----End

Stopping Tasks

Step 1 On the **Disaster Recovery Management** page, select tasks you wan to stop.

Step 2 Click **Batch Operations** in the upper left corner and choose **Stop**.

Figure 3-43 Batch Operations



Step 3 In the displayed dialog box, confirm the task information and click **Yes**.

----End

3.5.14 Deleting a DR Task

You can delete a DR task, when it is no longer needed Deleted tasks will no longer be displayed in the task list. Exercise caution when performing this operation.

Prerequisites

You have logged in to the DRS console.

Deleting a Task

Step 1 In the task list on the **Disaster Recovery Management** page, locate the target task and click **Delete** in the **Operation** column.

Step 2 Click **Yes** to submit the deletion task.

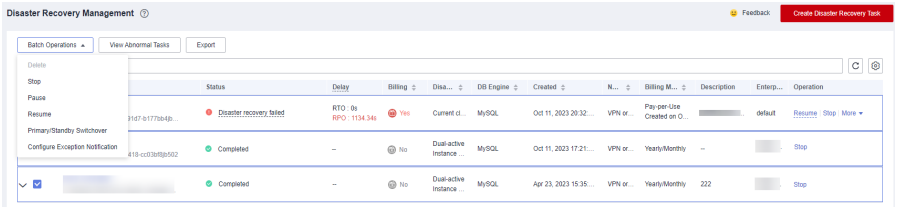
----End

Deleting Tasks

Step 1 On the **Disaster Recovery Management** page, select the tasks to be deleted.

Step 2 Click **Batch Operations** in the upper left corner and choose **Delete**.

Figure 3-44 Batch Operations



Step 3 In the displayed dialog box, confirm the task information and click **Yes**.

----End

3.5.15 Task Statuses

DR statuses indicate different DR phases.

Table 3-14 lists DR task statuses and descriptions.

Table 3-14 Task status and description

Status	Description
Creating	A DR instance is being created for DRS.
Configuration	A DR instance is created, but the DR task is not started. You can continue to configure the task.
Frozen	Instances are frozen when the account balance is less than or equal to $0.
Pending start	A scheduled DR task is created for the DR instance, waiting to be started.
Starting	A DR task is starting.
Start failed	A real-time DR task fails to be started.
Initialization	Full data from the service database to the DR database is being initialized.
Initialization completed	The DR task has been initialized.
Disaster recovery in progress	Incremental data from the service database is being synchronized to the DR database.
Switching over	The primary/standby switchover of a DR task is being performed.
Paused	The real-time DR synchronization task is paused.
Disaster recovery failed	A DR task fails during the disaster recovery.
Task stopping	A DR instance and resources are being released.

Status	Description
Completing	A DR instance and resources are being released.
Stopping task failed	Instances and resources used by the DR task fail to be released.
Completed	The DR instance used by a DR task is released successfully.

NOTE

- If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.
- By default, DRS retains a task in the **Configuration** state for three days. After three days, DRS automatically deletes background resources, but the task status remains unchanged. When you reconfigure the task, DRS applies for resources again.
- Deleted DR tasks are not displayed in the status list.

4 Tag Management

Scenarios

Tag Management Service (TMS) enables you to use tags on the management console to manage resources. TMS works with other cloud services to manage tags. TMS manages tags globally, and other cloud services manage their own tags. If you have to manage a large number of tasks, you can use different tags to identify and search for tasks.

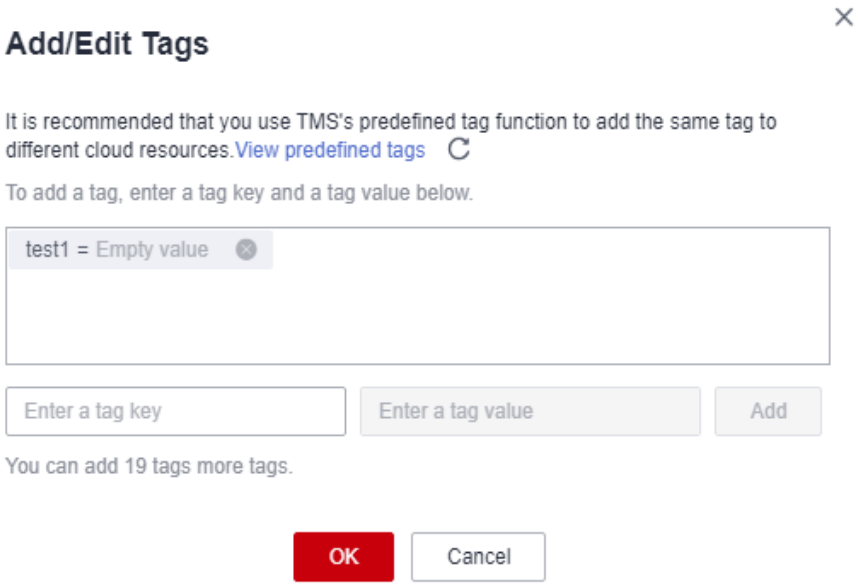
- You are advised to set predefined tags on the TMS console.
- A tag consists of a key and value. You can add only one value for each key.
- Each DB instance can have up to 20 tags.

Adding a Tag

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

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

Step 3 On the **Tags** tab, click **Add/Edit Tags**. In the displayed dialog box, enter a tag key and value, click **Add**, and click **OK**.



- When you enter a tag key and value, the system automatically displays all tags (including predefined tags and resource tags) associated with all DB instances except the current one.
- The tag key must be unique. It must consist of 1 to 128 characters and can include letters, digits, spaces, and the following characters: _**.**:=+-@. It cannot start or end with a space, or start with _**sys**_.
- The tag value can be empty. It cannot start or end with a space and can contain 0 to 255 characters, including letters, digits, spaces, and special characters _:=+.-@

Step 4 View and manage the tag on the **Tags** page.

----End

Editing a Tag

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

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

Step 3 On the **Tags** page, click **Add/Edit Tags**. In the displayed dialog box, modify the tag and click **OK**.

----End

Delete a Tag

Step 1 On the **Disaster Recovery Management** page, click the target DR task in the **Task Name/ID** column.

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

Step 3 On the **Tags** page, locate the tag to be deleted and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

Step 4 After the tag is deleted, it will no longer be displayed on the **Tags** page.

----End

5 Connection Diagnosis

If a DRS instance fails to be connected to the source or destination database during connection testing, DRS provides the quick diagnosis function and returns the diagnosis result.

- You can perform connection diagnosis only on the task node whose database information is obtained by entering an IP address or selecting a task node on the GUI. DN diagnosis of GaussDB is not supported.
- In cluster or multi-AZ task scenarios, diagnosis can be performed only on the node of the primary task.

Prerequisites

- You have logged in to the DRS console.
- A task has been created.

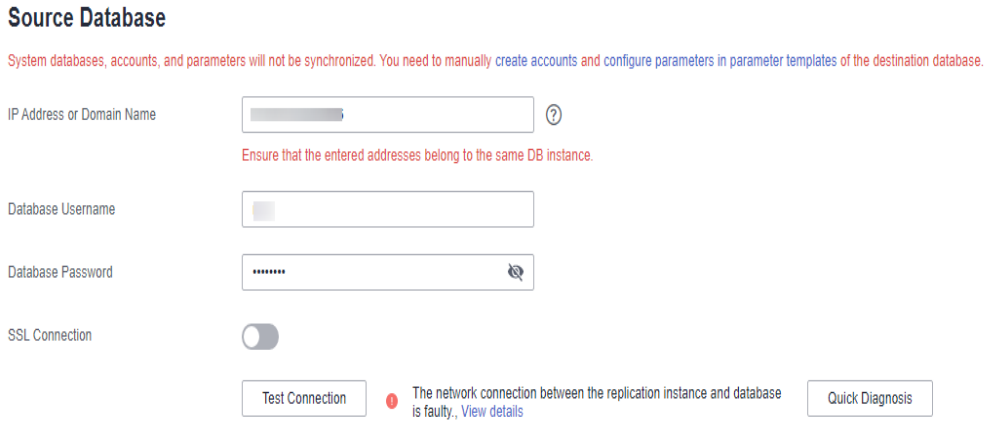
Procedure

Step 1 On the task management page, click the target task name in the **Task Name/ID** column.

Step 2 On the **Configure Source and Destination Databases** page, specify source and destination database information and click **Test Connection** for both the source and destination databases to check whether they have been connected to the DRS instance.

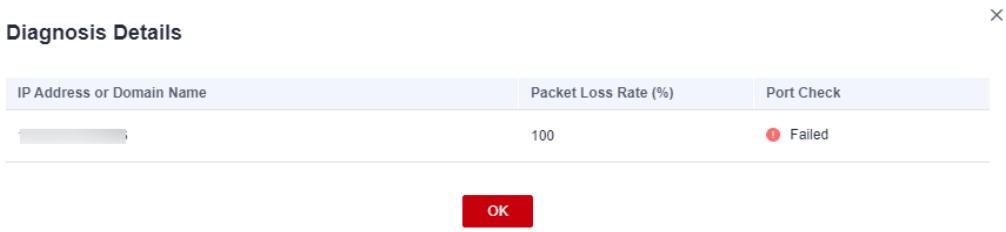
If the connection testing fails, click **Quick Diagnosis** on the right of the failure information to diagnose the fault.

Figure 5-1 Quick Diagnosis



Step 3 View the diagnosis result on the displayed **Diagnosis Details** dialog box. The result includes the packet loss rate and port check result.

Figure 5-2 Diagnosis Details



----End

6 Interconnecting with CTS

6.1 Key Operations Recorded by CTS

Cloud Trace Service (CTS) provides records of operations on cloud service resources, enabling you to query, audit, and backtrack operations.

Table 6-1 DRS operations recorded by CTS

Operation	Resource Type	Trace Name
Creating a task	job	createJob
Editing a task	job	modifyJob
Deleting a task	job	deleteJob
Starting a task	job	startJob
Resuming a task	job	retryJob

6.2 Viewing Traces

After CTS is enabled, CTS starts recording operations on cloud resources. The CTS management console stores the last seven days of operation records.

This section describes how to query the operation records of the last seven days on the CTS console.

Prerequisites

The CTS service has been enabled.

Procedure

Step 1 Log in to the management console.

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

Step 3 Click **Service List**. Under **Management & Governance**, choose **Cloud Trace Service**.

Step 4 Choose **Trace List** in the navigation pane on the left.

Step 5 Specify the search criteria as needed.

- Search time range: In the upper right corner, choose **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.

  If you select **Resource ID** for **Search By**, specify a resource ID.

  If you select **Data** for **Trace Type**, you can only filter traces by tracker.
- **Operator**: Select a specific operator (a user rather than a tenant).
- **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.

Step 6 Click **Query**.

Step 7 Click to the left of the target record to extend its details.

Step 8 Click **View Trace** in the **Operation** column. A dialog box is displayed, on which the trace structure details are displayed.

----End

7 Interconnecting with Cloud Eye

7.1 Supported Metrics

Description

This section describes metrics reported by the Data Replication Service (DRS) to Cloud Eye as well as their namespaces and dimensions. You can use APIs provided by Cloud Eye to query the metrics of the monitored object and alarms generated for DRS.

Namespace

SYS.DRS

DB Instance Monitoring Metrics

Table 7-1 lists the DRS performance metrics.

Table 7-1 DRS metrics

Metric ID	Metrics Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
cpu_util	CPU Usage	CPU usage of the monitored object	0-100 %	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
mem_util	Memory Usage	Memory usage of the monitored object	0-100 %	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
network_incoming_bytes_rate	Network Input Throughput	Incoming traffic in bytes per second	≥ 0 bytes/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
network_outgoing_bytes_rate	Network Output Throughput	Outgoing traffic in bytes per second	≥ 0 bytes/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
disk_read_bytes_rate	Disk Read Throughput	Number of bytes read from the disk per second (bytes/second).	≥ 0 bytes/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute

Metric ID	Metrics Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_write_bytes_rate	Disk Write Throughput	Number of bytes written to the disk per second (bytes/second).	≥ 0 bytes/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
disk_util	Storage Space Usage	Storage space usage of the monitored object	0-100 %	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
extract_bytes_rate	Source Database Read Throughput	Table data or WAL bytes read from the source database per second	≥ 0 bytes/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
extract_rows_rate	Rows Read from Source Database per Second	Number of table data rows or WAL rows read from the source database per second Unit: rows/s.	≥ 0 row/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
extract_latency	Source Database WAL Extract Lag	Latency of extracting WAL from the source database Unit: ms.	≥ms	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute

Metric ID	Metrics Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
apply_bytes_rate	Destination Database Write Throughput	Number of bytes written to the destination database per second.	≥ 0 bytes/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
apply_rows_rate	Rows Written into Destination Database per Second	Number of rows that are written to the destination database per second Unit: rows/s.	≥ 0 row/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
apply_transactions_rate	DML TPS	Number of DML transactions written to the destination database per second.	≥ 0 transaction/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
apply_ddls_numberor apply_ddls_rate **NOTE** apply_ddls_rate is replaced by apply_ddls_number after December 2022.	DDL TPS	Total number of DDL transactions written into the destination database.	≥ 0 transaction	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute

Metric ID	Metrics Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
apply_latency	Replication Delay	Delay (in milliseconds) of data replay.	≥ 0 ms	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
apply_average_execute_time	Average Transaction Execution Time	Average execution time (RT = Execution time + Commit time) of a transaction in the destination database. The unit is millisecond.	≥ 0 ms	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
apply_average_commit_time	Average Transaction Commit Time	Average commit time (RT = Execution time + Commit time) of a transaction in the destination database. The unit is ms.	≥ 0 ms	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
apply_current_state	Synchronization Status	This metric is the synchronization status of the current kernel data (10: abnormal; 1: idle; 2: DML; 3: DDL), instead of the task status.	10: abnormal 1: idle 2: DML is executed. 3: DDL is executed.	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute

Metric ID	Metrics Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
apply_thread_workers	Synchronization Threads	Number of working threads for data synchronization	≥ 0	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
apply_job_status	Task Status	Status of the current task. (**0**: normal; **1**: abnormal; **2**: paused)	**0**: normal **1**: abnormal **2**: paused	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute

Dimensions

Key	Value
instance_id	DRS instance ID

7.2 Configuring Alarm Rules

Scenarios

You can configure DRS alarm rules to customize the monitored objects and notification policies and learn the DRS running status in a timely manner.

This section describes how to set DRS alarm rules, including the alarm rule name, service, dimension, monitoring scope, template, and whether to send a notification.

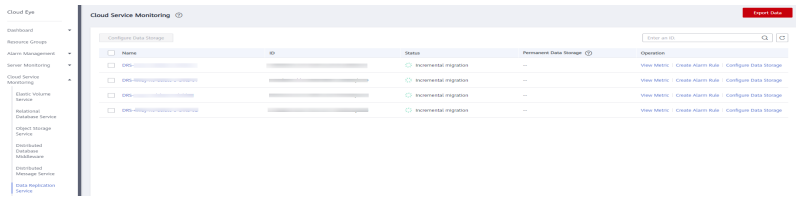
Procedure

Step 1 Log in to the management console.

Step 2 Under **Management & Governance**, click **Cloud Eye**.

Step 3 In the navigation pane on the left, choose **Cloud Eye** > **Data Replication Service**.

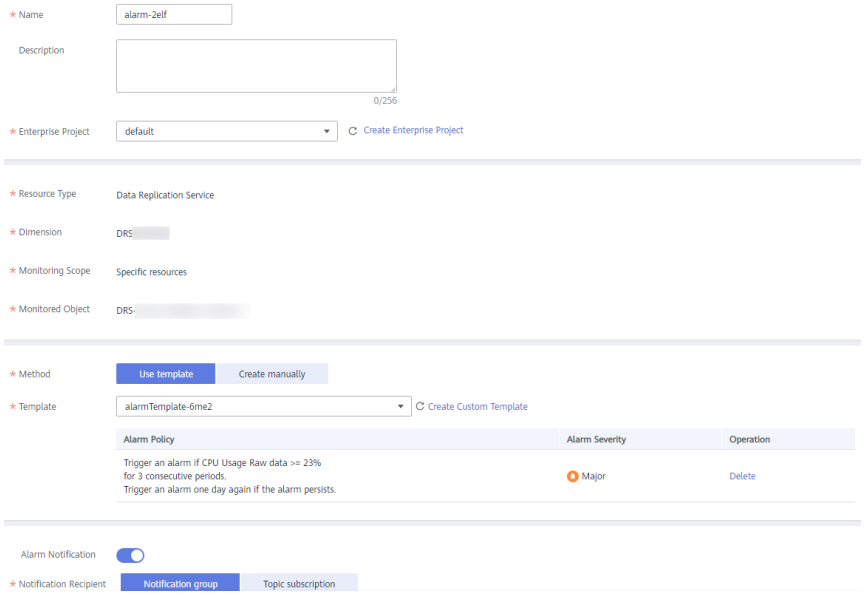
Figure 7-1 Choosing a monitored object



Step 4 Select the DB instance which you want to create an alarm rule for and click **Create Alarm Rule** in the **Operation** column.

Step 5 On the displayed page, set parameters as required.

Figure 7-2 Configuring alarm information



- Specify **Name** and **Description**.
- Select **Use template** for **Method**. The template contains the following common metrics: CPU usage, memory usage, and storage space usage.
- Click  to enable alarm notification. The validity period is 24 hours by default. If the topics you required are not displayed in the drop-down list, click **Create an SMN topic**. Then, select **Generated alarm** and **Cleared alarm** for **Trigger Condition**.

  NOTE

  Cloud Eye sends notifications only within the validity period specified in the alarm rule.

Step 6 Click **Create**. The alarm rule is created.

For details about how to create alarm rules, see **Creating an Alarm Rule** in the *Cloud Eye User Guide*.

----End

7.3 Viewing Monitoring Metrics

Scenarios

Cloud Eye monitors the running statuses of replication, synchronization, and DR instances. You can obtain the monitoring metrics on the management console. Monitored data requires a period of time for transmission and display. The status of the monitored object displayed on the Cloud Eye page is the status obtained 5 to 10 minutes before. You can view the monitored data of a newly created DB instance 5 to 10 minutes later.

Prerequisites

An instance is running properly when in the following statuses:

- Real-time migration: Full migration and Incremental migration
- Real-time synchronization: Full synchronization and Incremental synchronization
- Real-time disaster recovery: Disaster recovery in progress

Viewing Metrics

Step 1 Log in to the management console.

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

Step 3 Choose **Database** > **Data Replication Service**. The **Data Replication Service** page is displayed.

Step 4 Take real-time migration as an example. On the **Online Migration Management** page, click the target migration task name in the **Task Name/ID** column.

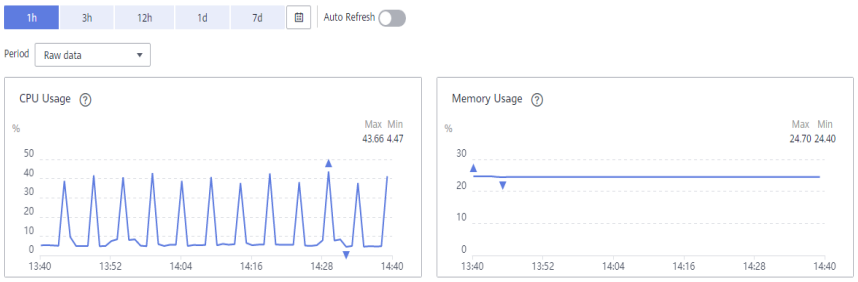
Step 5 On the displayed page, click **View Metric** in the upper right corner of the page to go to the Cloud Eye console.

By default, the monitoring information about the DRS instance is displayed on this page.

Step 6 View monitoring metrics of the instance.

- On the Cloud Eye console, click the target DB instance name and click **Select Metric** in the upper right corner. In the displayed dialog box, you can select the metrics to be displayed and sort them by dragging them at desired locations.
- You can sort graphs by dragging them based on service requirements.
- Cloud Eye can monitor performance metrics from the last 1 hour, 3 hours, 12 hours, 1 day, 7 days, and 6 months.

Figure 7-3 Viewing monitoring metrics



----End

8 Interconnecting with LTS

8.1 Log Reporting

Scenarios

If you enable log reporting, all logs generated by DRS instances (including real-time migration, backup migration, real-time synchronization, real-time disaster recovery, and traffic replay instances) are uploaded to Log Tank Service (LTS) for management.

Precautions

- After this function is enabled, all logs of the task are reported by default.
- This request does not take effect immediately. There is a delay of about 10 minutes.
- You will be billed for this function. For details, see **LTS Pricing Details**.
- Ensure that there are available LTS log groups and log streams in the same region as your instance.

  For more information about log groups and log streams, see **Log Management**.
- After this function is disabled, you will not be billed anymore.

Enabling or Disabling Log Reporting

Step 1 Log in to the management console.

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

Step 3 Choose **Database** > **Data Replication Service**. The **Data Replication Service** page is displayed.

Step 4 Take real-time migration as an example. On the **Online Migration Management** page, click the target migration task name in the **Task Name/ID** column.

Step 5 On the **Basic Information** page, click **Migration Logs** on the left.

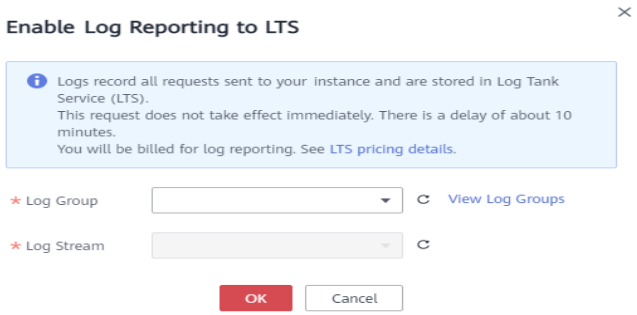
Step 6 Click  next to **Report Logs to LTS** in the upper part of the page.

Step 7 Select an LTS log group and log stream and click **OK**.

NOTE

This request does not take effect immediately. There is a delay of about 10 minutes.

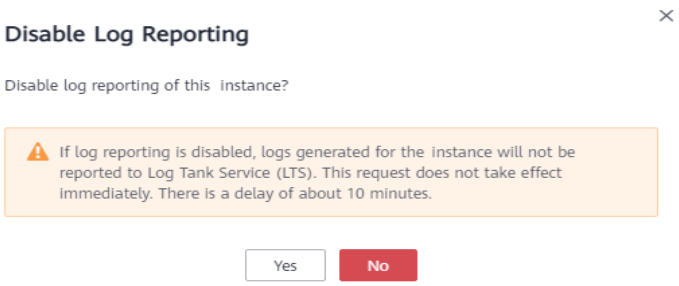
Figure 8-1 Enabling audit log reporting to LTS



Step 8 To disable or modify log reporting, click the toggle switch next to **Report Logs to LTS** or click **Edit** next to the **Report Logs to LTS** toggle switch.

- Modifying log reporting: Click **Edit** next to the **Report Logs to LTS** toggle switch. In the displayed dialog box, select the LTS log group and log stream again and click **OK**.
- Disabling log reporting: Click the toggle switch next to **Report Logs to LTS**. In the displayed dialog box, click **OK**.

Figure 8-2 Disabling log reporting to LTS



----End

8.2 Viewing and Downloading Logs

Scenarios

If you have enabled log reporting to LTS for a DRS task in **Log Reporting**, you can analyze logs, search for logs, visualize logs, download logs, and view real-time logs on the LTS console.

Viewing Logs Reported to LTS

Step 1 Log in to the management console.

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

Step 3 Under **Management & Governance**, click **Log Tank Service**.

Step 4 In the **Log Groups** area, locate a target log group and click its name. For details about LTS, see **Log Tank Service User Guide**.

Figure 8-3 Viewing log details

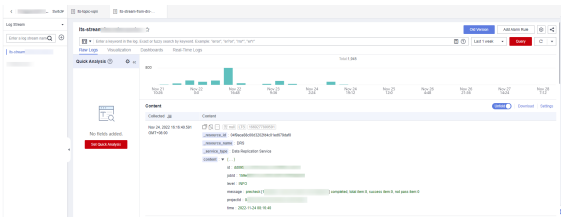


Table 8-1 Log field description

Name	Type	Description
_resource_id	String	Resource ID. The value is fixed to **projectId** for DRS.
_resource_name	String	Resource name. The value is fixed to **DRS**.
_service_type	String	Service type. The value is fixed to **Data Replication Service**.

----End

Downloading Logs Reported to LTS

Step 1 Log in to the management console.

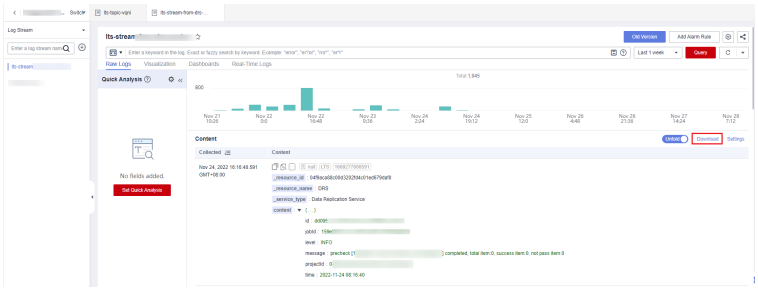
Step 2 Click in the upper left corner and select a region and project.

Step 3 Under **Management & Governance**, click **Log Tank Service**.

Step 4 In the **Log Groups** area, locate a target log group and click its name.

Step 5 Click **Download** on the right to download logs. For details about LTS, see **Log Tank Service User Guide**.

Figure 8-4 Downloading logs



----End

A Change History

Released On	Description
2023-11-30	This issue is the twenty-ninth official release, which incorporates the following change: ● Supported direction exchange for dual-active DR.
2023-10-30	This issue is the twenty-eighth official release, which incorporates the following change: ● Added support for upgrading task specifications in a DRS multi-specification task.
2023-08-30	This issue is the twenty-seventeenth official release, which incorporates the following change: ● Supported DRS task filtering by DB instance ID or database IP address.
2023-07-30	This issue is the twenty-sixth official release, which incorporates the following change: ● Supported AZ selection for DRS DR tasks.
2023-04-30	This issue is the twenty-fifth official release, which incorporates the following changes: ● Supported quick diagnosis if a DRS connection test fails.
2023-03-30	This issue is the twenty-fourth official release, which incorporates the following changes: ● Supported specification upgrade for real-time DR from MySQL to MySQL. Changed the following content: ● On the DRS task creation page, changed **Single** and **Primary/Standby** to **Single-AZ** and **Dual-AZ** in the **DRS Task Type** area.

Released On	Description
2023-02-28	This issue is the twenty-third official release, which incorporates the following changes: ● Supported the sorting of row comparison results in ascending or descending order by **Source Database Table Rows** or **Destination Database Table Rows**.
2022-11-30	This issue is the twenty-second official release, which incorporates the following changes: ● After DRS interconnects with LTS and log reporting to LTS is enabled, all logs generated by DRS instances will be uploaded to LTS for management.
2022-07-30	This issue is the twenty-first official release, which incorporates the following changes: ● If a task fails to be created, DRS retains the task for three days by default. After three days, the task automatically stops.
2022-04-30	This issue is the twentieth official release, which incorporates the following changes: ● Supported dual-active DR tasks that are billed on the yearly/monthly basis. Changed the following content: ● Adjusted the length and character range of tag keys and tag values.
2022-03-30	This issue is the nineteenth official release, which incorporates the following changes: ● Supported account-level comparison for MySQL and GaussDB(for MySQL) databases during real-time DR. ● Supported multiple specifications for some real-time DR tasks. ● Supported yearly/monthly billing for some DR tasks. Changed the following content: ● Supported disable task delay notification.
2022-02-28	This issue is the eighteenth official release, which incorporates the following changes: ● Supported one-click modification of performance parameters during MySQL DR parameter comparison. ● Supported stopping tasks in batches.
2021-12-31	This issue is the seventeenth official release, which incorporates the following changes: ● Added the description about the impact of DRS on databases. Changed the following content: ● Moved the Send Notifications option to the task confirmation page.

Released On	Description
2021-11-30	This issue is the sixteenth official release, which incorporates the following changes: Changed the following content: ● The following scenarios are in the open beta test phase. – Real-time DR from MySQL to GaussDB(for MySQL) – Real-time DR from DDM-to-DDM.
2021-09-30	This issue is the fifteenth official release, which incorporates the following changes: ● Added the description of the product architecture and principles. ● Added account progress statistics in the real-time DR scenario. Changed the following content: ● The following scenarios meet the commercial user standard. – Single-active disaster recovery from GaussDB(for MySQL) to GaussDB(for MySQL)
2021-07-05	This issue is the fourteenth official release, which incorporates the following changes: ● Added permissions, allowing users to perform all operations except deleting DB instances.
2021-04-30	This issue is the thirteenth official release, which incorporates the following changes: ● Supported real-time DR from DDM to DDM.
2021-01-30	This issue is the twelfth official release, which incorporates the following changes: ● Supported the real-time disaster recovery (DR) of GaussDB(for MySQL). ● Supported exporting task information on the real-time disaster recovery page.
2020-11-30	This issue is the eleventh official release, which incorporates the following changes: ● Supported searching objects when the user selects objects. ● Supported setting the number of days after which an abnormal task can be automatically stopped.
2020-10-31	This issue is the tenth official release, which incorporates the following changes: ● Added the description of latency in all DR scenarios to DRS.

Released On	Description
2020-09-30	This issue is the ninth official release, which incorporates the following changes: ● Added the description on the DR monitoring page, and the connection needs to be reset after the RDS DB instance is promoted to the primary DB instance.
2020-08-31	This issue is the eighth official release, which incorporates the following changes: ● Supported configuration of the subnet for the DR instance.
2020-07-31	This issue is the seventh official release, which incorporates the following change: ● Allowed different users under the same tenant to manage their own DRS tasks, and the tasks are invisible to each other.
2020-03-31	This issue is the sixth official release, which incorporates the following changes: ● Supported MySQL to GaussDB(for MySQL) DR for the first time. ● Provided the task pausing function.
2020-02-29	This issue is the fifth official release, which incorporates the following changes: ● Added the flow control mode for disaster recovery. ● Supported forward and backward DR in multi-active DR. ● Supported the change of the flow control mode after the task is started. ● Supported resetting passwords.
2020-01-30	This issue is the fourth official release, which incorporates the following changes: ● Supported alarm reporting for DR tasks. ● Supported forcing tasks to stop.
2019-12-30	This issue is the twenty-seventeenth official release, which incorporates the following changes: ● Supported batch primary/standby switchover in disaster recovery scenarios.
2019-11-30	This issue is the third official release, which incorporates the following changes: ● Supported disaster recovery between RDS DB instances or between self-built databases and RDS DB instances. ● Supported selecting the current cloud as the active during disaster recovery.

Released On	Description
2019-10-30	This issue is the second official release, which incorporates the following changes: • Supported online multi-active DR. • Supported tag management.
2018-10-31	This issue is the first official release.