

**Data Replication Service**

# **Real-Time Disaster Recovery**

**Issue**            01  
**Date**             2022-09-30



**Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI 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](mailto:support@huawei.com)

---

# Contents

---

<b>1 DR Overview</b>	<b>1</b>
<b>2 DR Scenarios</b>	<b>3</b>
2.1 From MySQL to MySQL (Single-Active DR)	3
2.2 From MySQL to GaussDB(for MySQL) Primary/Standby (Single-Active DR)	22
2.3 From DDM to DDM Single-Active DR	38
2.4 From GaussDB(for MySQL) Primary/Standby to GaussDB(for MySQL) Primary/Standby (Single-Active DR)	52
2.5 From MySQL to MySQL (Dual-Active DR)	70
2.6 From GaussDB(for MySQL) Primary/Standby to GaussDB(for MySQL) Primary/Standby (Dual-Active DR)	84
<b>3 Task Management</b>	<b>98</b>
3.1 Creating a DR Task	98
3.2 Querying the DR Progress	114
3.3 Viewing DR Logs	115
3.4 Comparing DR Items	116
3.5 Task Life Cycle	120
3.5.1 Viewing DR Data	120
3.5.2 Editing Subscription Task Information	122
3.5.3 Editing a DR Task	124
3.5.4 Resuming a DR Task	129
3.5.5 Pausing a DR Task	130
3.5.6 Stopping a DR Task	131
3.5.7 Deleting a DR Task	132
3.5.8 Viewing DR Metrics	133
3.5.9 Performing a Primary/Standby Switchover	134
3.5.10 Modifying the Flow Control Mode	135
3.5.11 Task Statuses	136
<b>4 Tag Management</b>	<b>138</b>
<b>5 Interconnecting with CTS</b>	<b>140</b>
5.1 Key Operations Recorded by CTS	140
5.2 Viewing Traces	140
<b>6 Interconnecting with Cloud Eye</b>	<b>142</b>

---

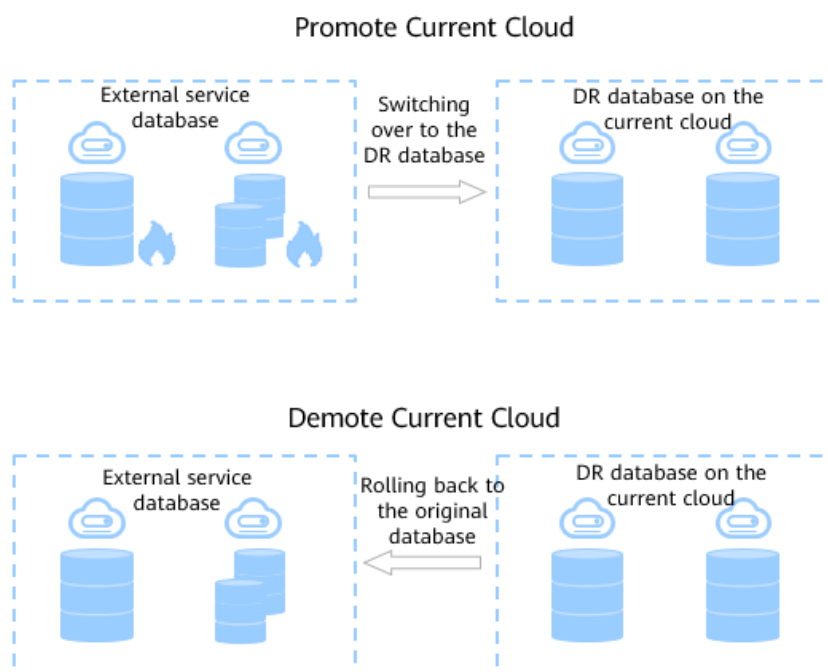
6.1 Supported Metrics.....	142
6.2 Configuring Alarm Rules.....	147
6.3 Viewing Monitoring Metrics.....	148
<b>A Change History.....</b>	<b>150</b>

# 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

**Table 1-1** lists the database types supported by DRS.

**Table 1-1** DR schemes

Service Database	DR Database	Documentation
<ul style="list-style-type: none"> <li>On-premises MySQL databases</li> <li>MySQL databases on an ECS</li> <li>MySQL databases on other clouds</li> <li>RDS for MySQL</li> </ul>	RDS for MySQL	<ul style="list-style-type: none"> <li><a href="#">From MySQL to MySQL (Single-Active DR)</a></li> <li><a href="#">From MySQL to MySQL (Dual-Active DR)</a></li> </ul>
	GaussDB(for MySQL) primary/standby	<ul style="list-style-type: none"> <li><a href="#">From MySQL to GaussDB(for MySQL) Primary/Standby (Single-Active DR)</a></li> </ul>
DDM	DDM	<ul style="list-style-type: none"> <li><a href="#">From DDM to DDM Single-Active DR</a></li> </ul>
GaussDB(for MySQL) primary/standby	GaussDB(for MySQL) primary/standby	<ul style="list-style-type: none"> <li><a href="#">From GaussDB(for MySQL) Primary/Standby to GaussDB(for MySQL) Primary/Standby (Single-Active DR)</a></li> <li><a href="#">From GaussDB(for MySQL) Primary/Standby to GaussDB(for MySQL) Primary/Standby (Dual-Active DR)</a></li> </ul>

## 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
<ul style="list-style-type: none"><li>On-premises MySQL databases</li><li>MySQL databases on an ECS</li><li>MySQL databases on other clouds</li><li>RDS for MySQL</li></ul>	<ul style="list-style-type: none"><li>RDS for MySQL</li></ul>

### 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. 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 2-2** Precautions

Type	Constraint
Database permissions	<ul style="list-style-type: none"> <li>● The service database user must have the following permissions: The user <b>root</b> of the RDS for MySQL instance has the following permissions by default: 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 If the service database version is 8.0.14 to 8.0.18, the SESSION_VARIABLES_ADMIN permission is required.</li> <li>● The DR database user must have the following permissions: The user <b>root</b> of the RDS for MySQL instance has the following permissions by default: 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 If the DR database version is 8.0.14 to 8.0.18, the SESSION_VARIABLES_ADMIN permission is required.</li> </ul>
Disaster recovery objects	<ul style="list-style-type: none"> <li>● Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery.</li> <li>● System tables are not supported.</li> <li>● Triggers and events do not support disaster recovery.</li> <li>● Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery.</li> <li>● Backup and disaster recovery, cross-database DDL, and rename operations cannot be performed on some specified service databases. Otherwise, the disaster recovery fails.</li> </ul>

Type	Constraint
Service database configuration	<ul style="list-style-type: none"> <li>● The binlog of the MySQL service database must be enabled and use the row-based format.</li> <li>● If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days.</li> <li>● The service database username or password cannot be empty.</li> <li>● <b>server_id</b> in the MySQL service database must be set. If the service database version is MySQL 5.6 or earlier, the <b>server_id</b> value ranges from <b>2</b> to <b>4294967296</b>. If the service database is MySQL 5.7 or later, the <b>server_id</b> value ranges from <b>1</b> to <b>4294967296</b>.</li> <li>● GTID must be enabled for the database.</li> <li>● The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_).</li> <li>● The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '&lt;&gt;/\</li> <li>● If the <b>expire_logs_days</b> value of the database is set to <b>0</b>, the disaster recovery may fail.</li> </ul>
DR database configuration	<ul style="list-style-type: none"> <li>● The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal.</li> <li>● The DR DB instance must have sufficient storage space.</li> <li>● The major version of the DR database must be the same as that of the service database.</li> <li>● Except the MySQL system database, the DR database must be empty. After a DR task starts, the DR database is set to read-only.</li> </ul>

Type	Constraint
Precautions	<ul style="list-style-type: none"> <li>● If the DCC does not support instances with 4 vCPUs and 8 GB memory or higher instance specifications, the DR task cannot be created.</li> <li>● Cascade operations cannot be performed on tables with foreign keys.</li> <li>● The service database does not support point-in-time recovery (PITR).</li> <li>● Binlogs cannot be forcibly deleted. Otherwise, the DR task fails.</li> <li>● 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.</li> <li>● Resumable upload is supported, but data may be repeatedly inserted into a table that does not have a primary key.</li> <li>● Migration or synchronization tasks cannot be created when a DR task exists.</li> <li>● 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.</li> <li>● If the service database and DR database are RDS MySQL instances, tables with TDE enabled cannot be created.</li> <li>● If a high-privilege user created in an external database is not supported by RDS MySQL, the user will not be synchronized to the DR database, for example, the super user.</li> <li>● 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.</li> <li>● 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.</li> <li>● 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.</li> <li>● 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.</li> </ul>

Type	Constraint
	<ul style="list-style-type: none"> <li>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.</li> <li>During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal.</li> <li>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.</li> </ul>

## 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, specify the task name, description, and the DR instance details, and click **Next**.

**Figure 2-1** DR task information

The screenshot shows a form with three fields:
 

- Region:** A dropdown menu with a location pin icon.
- \* Task Name:** A text input field containing "DRS-7117" and a help icon (?).
- Description:** A text area with a height of 40 pixels, containing "0/256" characters, and a help icon (?).

**Table 2-3** Task and recipient description

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

**Figure 2-2** DR instance information

**Disaster Recovery Instance Information**

The following information cannot be modified after you go to the next page.

\* DR Type: Single-active Dual-active ⓘ

\* Disaster Recovery Relationship: Current cloud as standby Current cloud as active

\* Service DB Engine: MySQL Cassandra DDM

\* DR DB Engine: MySQL GaussDB(for MySQL) Cassandra DDM

\* Network Type: Public network ⓘ

I acknowledge that an EIP will be automatically bound to the disaster recovery instance and released after the task is completed.

\* DR DB Instance: ... [View DB Instance](#) [View Unselectable DB Instance](#)

\* Disaster Recovery Instance Subnet: ... ⓘ [View Subnets](#)

\* Destination Database Access: Read-only

During the disaster recovery, the destination database becomes read-only to ensure the integrity and success rate of disaster recovery. After the disaster recovery is completed, it becomes readable and writable.

Tags: Tag key Tag value

You can add 10 more tags.

**Table 2-4** DR instance settings

Parameter	Description
DR Type	Select <b>Single-active</b> . The DR type can be single-active or dual-active. If <b>Dual-active</b> is selected, two subtasks are created by default, a forward DR task and a backward DR task. <b>NOTE</b> 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 <b>Service Tickets &gt; Create Service Ticket</b> to submit a service ticket.
Disaster Recovery Relationship	Select <b>Current cloud as standby</b> . This parameter is available only when you select <b>Single-active</b> . By default, <b>Current cloud as standby</b> is selected. You can also select <b>Current cloud as active</b> . <ul style="list-style-type: none"> <li><b>Current cloud as standby</b>: The DR database is on the current cloud.</li> <li><b>Current cloud as active</b>: The service database is on the current cloud.</li> </ul>
Service DB Engine	Select <b>MySQL</b> .
DR DB Engine	Select <b>MySQL</b> .
Network Type	The public network is used as an example. Available options: <b>VPN or Direct Connect</b> and <b>Public network</b> . By default, the value is <b>Public network</b> .

Parameter	Description
DR DB Instance	The RDS instance you created.
Disaster Recovery Instance Subnet	<p>Select the subnet where the disaster recovery instance is located. You can also click <b>View Subnet</b> to go to the network console to view the subnet where the instance resides.</p> <p>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.</p>
Destination Database Access	<p>Select <b>Read-only</b>. This parameter is available only when you select <b>Single-active</b>.</p> <p>During single-active disaster recovery, the DR database becomes read-only. To change the DR database to <b>Read/Write</b>, you can change the DR database (or destination database) to a service database by clicking <b>Promote Current Cloud</b> on the <b>Disaster Recovery Monitoring</b> tab. After the DR task is complete or deleted, you can query and read data to the DR database.</p> <p>When the external database functions as the DR database, the user with the superuser permission can set the database to read-only.</p> <p>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.</p>
Enterprise Project	<ul style="list-style-type: none"> <li>• If the DB instance has been associated with an enterprise project, select the target project from the <b>Enterprise Project</b> drop-down list.</li> <li>• You can also go to the ProjectMan console to create a project. For details about how to create a project, see <i>ProjectMan User Guide</i>.</li> </ul>
Tags	<ul style="list-style-type: none"> <li>• This setting is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 10 tags.</li> <li>• After a task is created, you can view its tag details on the <b>Tags</b> tab. For details, see <a href="#">Tag Management</a>.</li> </ul>

**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 2-3** Service database information

Source Database

Source Database Type  Self-built on ECS  RDS DB Instance

IP Address or Domain Name

Port

Database Username

Database Password

SSL Connection

If you want to enable SSL connection, ensure that SSL has been enabled on the source database, related parameters have been correctly configured, and an SSL certificate has been uploaded.

Encryption Certificate

**Table 2-5** Service database settings

Parameter	Description
Source Database Type	By default, <b>Self-built on ECS</b> is selected. The source database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b> . After selecting <b>RDS DB instance</b> , 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 <b>RDS DB instance</b> 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	<p>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:</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress</b>, or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p>
SSL Connection	<p>SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- The maximum size of a single certificate file that can be uploaded is 500 KB.</li> <li>- If the SSL certificate is not used, your data may be at risk.</li> </ul>
Region	<p>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 <b>RDS DB instance</b>.</p>
DB Instance Name	<p>The name of the service DB instance. This parameter is available only when the source database is an <b>RDS DB instance</b>.</p>
Database Username	<p>The username for accessing the service database.</p>
Database Password	<p>The password for the service database username.</p>

 **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 2-4** DR database information

### Destination Database

DB Instance Name

Database Username

Database Password

✔ Test successful

**Table 2-6** 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	<p>The password for the database username. The password can be changed after a task is created.</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress</b>, or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p> <p>The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.</p>

- Select **Current cloud as active** for **Disaster Recovery Relationship** in [Step 2](#).

**Figure 2-5** Service database information

### Source Database

DB Instance Name

Database Username

Database Password

✔ Test successful

**Table 2-7** 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	<p>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:</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress</b>, or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p> <p>The database username and password are encrypted and stored in the system and will be cleared after the task is deleted.</p>

**Figure 2-6** DR database information

**Destination Database**

Database Type: Self-built on ECS **RDS DB instance**

Region:

DB Instance Name:  [View DB Instance](#) [View Unselectable DB Instance](#)  
If used as a DR database, the instance becomes read-only.

Database Username:

Database Password:

This button is available only after the replication instance is created successfully.

**Table 2-8** DR database settings

Parameter	Description
Database Type	<p>By default, <b>Self-built on ECS</b> is selected.</p> <p>The destination database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b>. If you select <b>RDS DB instance</b>, you need to select the region where the destination database is located.</p>

Parameter	Description
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.
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 <b>Starting, Initializing, Disaster recovery in progress</b> , or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b> . 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.  <b>NOTE</b> The maximum size of a single certificate file that can be uploaded is 500 KB.
Region	The region where the RDS DB instance is located. This parameter is available only when the source database is an RDS DB instance.
DB Instance Name	DR instance name. This parameter is available only when the source database is an RDS DB instance.  <b>NOTE</b> 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.

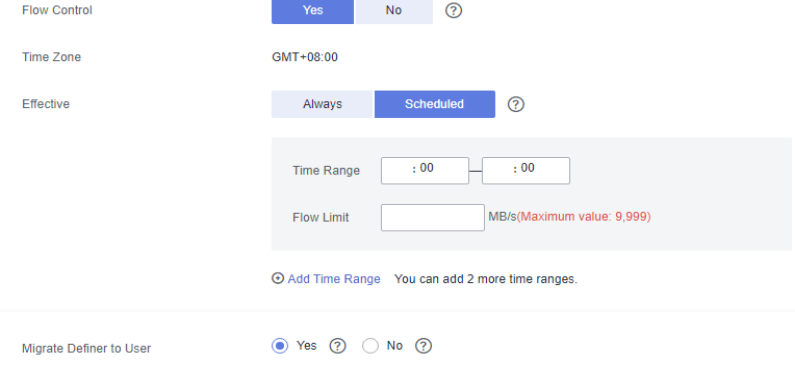
**Step 4** On the **Configure DR** page, specify flow control and click **Next**.

**Figure 2-7** DR settings

The image shows a user interface for configuring DR settings. It contains two rows of settings, each enclosed in a dashed box. The first row is for 'Flow Control', with 'Yes' and 'No' buttons and a help icon. The 'No' button is selected. The second row is for 'Migrate Definer to User', with radio buttons for 'Yes' and 'No', and help icons. The 'Yes' radio button is selected.

Flow Control	<input type="button" value="Yes"/>	<input checked="" type="button" value="No"/>	<input type="button" value="?"/>
Migrate Definer to User	<input checked="" type="radio"/>	<input type="radio"/>	<input type="button" value="?"/> <input type="button" value="?"/>

**Table 2-9** DR settings

Parameter	Description
Flow Control	<p>You can choose whether to control the flow.</p> <ul style="list-style-type: none"> <li> <b>Yes</b>                      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 <b>All day</b>. 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.                 </li> </ul> <p><b>Figure 2-8</b> Flow control</p>  <ul style="list-style-type: none"> <li> <b>No</b>                      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.                 </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- Flow control mode takes effect during the initial DR phase only.</li> <li>- You can also change the flow control mode when the task is in the <b>Configuration</b> state. On the <b>Basic Information</b> tab, in the <b>DR Information</b> area, click <b>Modify</b> next to <b>Flow Control</b>. In the dialog box that is displayed, change the flow control mode. The flow control mode cannot be changed for a task that is in <b>Starting</b> state.</li> </ul>

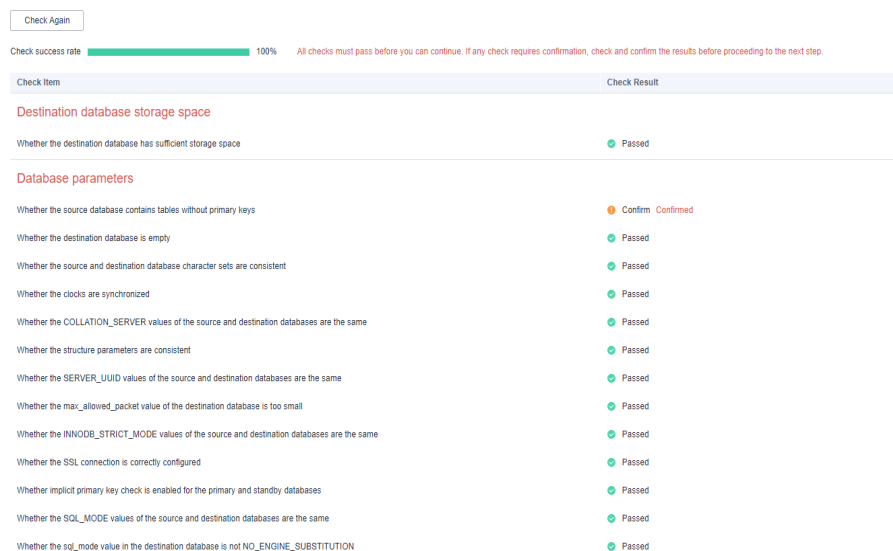
Parameter	Description
Migrate Definer to User	<ul style="list-style-type: none"> <li><b>Yes</b> The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see <a href="#">How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?</a></li> <li><b>No</b> 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.</li> </ul>

**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 [Checking Whether the Source Database Is Connected](#) in *Data Replication Service User Guide*.

**Figure 2-9** 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 2-10** Modifying common parameters

Parameter Name	Source Database Value	Destination Database Value	Result
character_set_server	utf8	utf8	Consistent
collation_server	utf8_general_ci	utf8_general_ci	Consistent
connect_timeout	10	10	Consistent
explicit_defaults_for_timestamp	OFF	ON	Inconsistent
innodb_flush_log_at_trx_commit	1	1	Consistent
innodb_lock_wait_timeout	50	50	Consistent
max_connections	800	800	Consistent
net_read_timeout	30	30	Consistent
net_write_timeout	60	60	Consistent
tx_isolation	REPEATABLE-READ	REPEATABLE-READ	Consistent

- 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 2-11** One-click modification

Parameter Name	Source Database Value	Destination Database Value	Change To	Allowed Destination Database Value	Result
binlog_cache_size	32768	32768	5	4096 - 1677216	Consistent
binlog_stmt_cache_size	32768	32768	8	4096 - 1677216	Consistent
bulk_insert_buffer_size	8388608	8388608		0 - 184467440730551615	Consistent
innodb_buffer_pool_size	536870912	85526368	4	536870912 - 1717388918	Inconsistent
long_query_time	1.000000	1.000000		0.01 - 3000	Consistent
read_buffer_size	262144	262144	64	4096 - 262144	Consistent
read_rnd_buffer_size	524288	524288	128	4096 - 524288	Consistent
sort_buffer_size	262144	262144		32768 - 184467440730551615	Consistent
sync_binlog	1	1		0 - 4294967295	Consistent

**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 2-12 One-click modification

Parameter Name	Source Database Value	Destination Database Value	Change To	Allowed Destination Database Va...	Result	
<input type="checkbox"/> binlog_cache_size	32768	32768	8	+4096 ~ 32768	4096-16777216	Consistent
<input type="checkbox"/> binlog_stmt_cache_size	32768	32768	8	+4096 ~ 32768	4096-16777216	Consistent
<input type="checkbox"/> bulk_insert_buffer_size	8388608	8388608			0-18440744073709551615	Consistent
<input checked="" type="checkbox"/> innodb_buffer_pool_size	536879512	805206384	4	-134317728 ~ 536879512	536879512-117946518	Inconsistent
<input type="checkbox"/> long_query_time	1.000000	1.000000			0.01-3000	Consistent
<input type="checkbox"/> read_buffer_size	262144	262144	64	+4096 ~ 262144	8192-2147483647	Consistent
<input type="checkbox"/> read_rnd_buffer_size	524288	524288	128	+4096 ~ 524288	1-2147483647	Consistent
<input type="checkbox"/> sort_buffer_size	262144	262144			32768-18440744073709551615	Consistent
<input type="checkbox"/> sync_binlog	1	1			0-4250497295	Consistent

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 2-13 Task startup settings

Start Time:  Start upon task creation  Start at a specified time

Send Notifications:

\* SMN Topic:

Synchronization Delay Threshold(s):

RTO Synchronization Delay Threshold(s):

RPO Synchronization Delay Threshold(s):

\* Stop Abnormal Tasks After:  Abnormal tasks run longer than the period you set (unit: day) will automatically stop.




**Table 2-10** Task and recipient description

Parameter	Description
Start Time	<p>Set <b>Start Time</b> to <b>Start upon task creation</b> or <b>Start at a specified time</b> based on site requirements.</p> <p><b>NOTE</b> 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.</p>
Send Notifications	<p>SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.</p>
SMN Topic	<p>This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber.</p> <p>For details, see <a href="#">Simple Message Notification User Guide</a>.</p>
Synchronization Delay Threshold	<p>During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database.</p> <p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RTO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the RTO delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>

Parameter	Description
RPO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> <li>• 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.</li> </ul>
Stop Abnormal Tasks After	<p>Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is <b>14</b>.</p> <p><b>NOTE</b></p> <p>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.</p>

**Step 8** After the DR 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.

----End

## 2.2 From MySQL to GaussDB(for MySQL) Primary/Standby (Single-Active DR)

### Supported Source and Destination Databases

**Table 2-11** Supported databases

Service Database	DR Database
<ul style="list-style-type: none"> <li>• On-premises MySQL databases</li> <li>• MySQL databases on an ECS</li> <li>• MySQL databases on other clouds</li> <li>• RDS for MySQL</li> </ul>	<ul style="list-style-type: none"> <li>• GaussDB(for MySQL) primary/standby</li> </ul>

## 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. 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 2-12** Precautions

Type	Restrictions
Database permissions	<ul style="list-style-type: none"> <li>• The service database 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.</li> <li>• The DR database 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.</li> <li>• The <b>root</b> account of the RDS MySQL DB instance has the preceding permissions by default.</li> </ul>
Disaster recovery objects	<ul style="list-style-type: none"> <li>• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery.</li> <li>• System tables are not supported.</li> <li>• Triggers and events do not support disaster recovery.</li> <li>• Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery.</li> <li>• Backup and disaster recovery, cross-database DDL, and rename operations cannot be performed on some specified service databases. Otherwise, the disaster recovery fails.</li> </ul>
Service database configuration	<ul style="list-style-type: none"> <li>• The binlog of the MySQL service database must be enabled and use the row-based format.</li> <li>• If the storage space is sufficient, you are advised to store the service database binlog for as long as possible. The recommended retention period is seven days.</li> <li>• The service database username or password cannot be empty.</li> <li>• <b>server-id</b> in the MySQL service database must be set. If the service database version is MySQL 5.6 or earlier, the <b>server-id</b> value ranges from <b>2</b> to <b>4294967296</b>. If the service database is MySQL 5.7 or later, the <b>server-id</b> value ranges from <b>1</b> to <b>4294967296</b>.</li> <li>• GTID must be enabled for the database.</li> <li>• The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_).</li> <li>• The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '&lt;&gt;\/\</li> <li>• If the <b>expire_logs_days</b> value of the database is set to <b>0</b>, the disaster recovery may fail.</li> </ul>

Type	Restrictions
DR database configuration	<ul style="list-style-type: none"><li>• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal.</li><li>• The DR DB instance must have sufficient storage space.</li><li>• The DR DB instance cannot contain any service databases except the system database.</li><li>• binlog and GTID must be enabled for the DR database.</li></ul>

Type	Restrictions
Precautions	<ul style="list-style-type: none"> <li>● 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.</li> <li>● If a high-privilege user created in an external database is not supported by RDS MySQL, the user will not be synchronized to the DR database, for example, the super user.</li> <li>● Cascade operations cannot be performed on tables with foreign keys.</li> <li>● The service database does not support point-in-time recovery (PITR).</li> <li>● Binlogs cannot be forcibly deleted. Otherwise, the DR task fails.</li> <li>● 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.</li> <li>● If the DCC does not support instances with 4 vCPUs and 8 GB memory or higher instance specifications, the DR task cannot be created.</li> <li>● Resumable upload is supported, but data may be repeatedly inserted into a table that does not have a primary key.</li> <li>● Migration or synchronization tasks cannot be created when a DR task exists.</li> <li>● 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.</li> <li>● 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.</li> <li>● When DR occurs between an earlier version database and a later version database, service activities must be compatible with both the earlier version and the later version. Otherwise, the DR may fail.</li> <li>● If the service database is an RDS MySQL instance, tables encrypted using Transparent Data Encryption (TDE) cannot be synchronized.</li> <li>● 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</li> </ul>

Type	Restrictions
	<p>console and retry the task to continue disaster recovery. Generally, you are advised not to modify the preceding information during disaster recovery.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal.</li> <li>• During data disaster recovery, accounts cannot be created.</li> <li>• 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.</li> </ul>

## 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, specify the task name, description, and the DR instance details, and click **Next**.

**Figure 2-14** DR task information



The screenshot shows a form with three fields:
 

- Region:** A dropdown menu with a location pin icon.
- Task Name:** A text input field containing "DRS-7117" and a question mark icon.
- Description:** A text area with a question mark icon and a character count "0/256" at the bottom right.

**Table 2-13** Task and recipient description

Parameter	Description
Region	The region where your service is running. You can change the region.

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

Figure 2-15 DR instance information

**Disaster Recovery Instance Details**

The following information cannot be modified after you go to the next page.

- \* DR Type: **Single-active** | Dual-active ⓘ
- \* Disaster Recovery Relationship: **Current cloud as standby** | Current cloud as active
- \* Service DB Engine: **MySQL** | Cassandra | DDM | GaussDB(for MySQL) Primary/Standby Ed...
- \* DR DB Engine: **MySQL** | GaussDB(for MySQL) Primary/Standby Ed...
- \* Network Type: Public network ⓘ  
 I understand that an EIP will be automatically bound to the replication instance and released after the synchronization task is complete.
- \* DR DB Instance: Select an instance ⓘ [View DB Instance](#) [View Unselectable DB Instance](#)
- \* Disaster Recovery Instance Subnet: Select the subnet ⓘ [View Subnets](#) [View occupied IP address](#)
- \* Destination DB Instance Access: **Read-only**  
During the disaster recovery, the destination DB instance becomes read-only to ensure the integrity and success of disaster recovery. When the disaster recovery is complete, it becomes readable and writable.

---

- \* Enterprise Project: --Select-- ⓘ [View Project Management](#) ⓘ

---

Tags: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) ⓘ

Tag key:  Tag value:

You can add 10 more tags.

Table 2-14 DR instance settings

Parameter	Description
DR Type	<p>Select <b>Single-active</b>.</p> <p>The DR type can be single-active or dual-active. If <b>Dual-active</b> is selected, two subtasks are created by default, a forward DR task and a backward DR task.</p> <p><b>NOTE</b></p> <p>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 <b>Service Tickets &gt; Create Service Ticket</b> to submit a service ticket.</p>



Parameter	Description
Disaster Recovery Relationship	<p>Select <b>Current cloud as standby</b>. This parameter is available only when you select <b>Single-active</b>.</p> <p>By default, <b>Current cloud as standby</b> is selected. You can also select <b>Current cloud as active</b>.</p> <ul style="list-style-type: none"> <li>• <b>Current cloud as standby</b>: The DR database is on the current cloud.</li> <li>• <b>Current cloud as active</b>: The service database is on the current cloud.</li> </ul>
Service DB Engine	Select <b>MySQL</b> .
DR DB Engine	Select <b>GaussDB(for MySQL) Primary/Standby Edition</b> .
Network Type	<p>The public network is used as an example.</p> <p>Available options: <b>VPN or Direct Connect</b> and <b>Public network</b>. By default, the value is <b>Public network</b>.</p>
DR DB Instance	The GaussDB(for MySQL) primary/standby instance you created.
Disaster Recovery Instance Subnet	<p>Select the subnet where the disaster recovery instance is located. You can also click <b>View Subnet</b> to go to the network console to view the subnet where the instance resides.</p> <p>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.</p>
Destination Database Access	<p>Select <b>Read-only</b>. This parameter is available only when you select <b>Single-active</b>.</p> <p>During single-active disaster recovery, the DR database becomes read-only. To change the DR database to <b>Read/Write</b>, you can change the DR database (or destination database) to a service database by clicking <b>Promote Current Cloud</b> on the <b>Disaster Recovery Monitoring</b> tab. After the DR task is complete or deleted, you can query and read data to the DR database.</p> <p>When the external database functions as the DR database, the user with the superuser permission can set the database to read-only.</p> <p>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.</p>

Parameter	Description
Enterprise Project	<ul style="list-style-type: none"> <li>If the DB instance has been associated with an enterprise project, select the target project from the <b>Enterprise Project</b> drop-down list.</li> <li>You can also go to the ProjectMan console to create a project. For details about how to create a project, see <i>ProjectMan User Guide</i>.</li> </ul>
Tags	<ul style="list-style-type: none"> <li>This setting is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 10 tags.</li> <li>After a task is created, you can view its tag details on the <b>Tags</b> tab. For details, see <a href="#">Tag Management</a>.</li> </ul>

**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 2-16** Service database information

Source Database

Source Database Type  Self-built on ECS  RDS DB Instance

IP Address or Domain Name

Port

Database Username

Database Password

SSL Connection

If you want to enable SSL connection, ensure that SSL has been enabled on the source database, related parameters have been correctly configured, and an SSL certificate has been uploaded.

Encryption Certificate

**Table 2-15** Service database settings

Parameter	Description
Source Database Type	By default, <b>Self-built on ECS</b> is selected. The source database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b> . After selecting <b>RDS DB instance</b> , 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 <b>RDS DB instance</b> 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 <b>Starting, Initializing, Disaster recovery in progress</b> , or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Update Password</b> next to the <b>Source Database Password</b> field. In the displayed dialog box, change the password. This action only updates DRS with the changed password.
SSL Connection	SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate. <b>NOTE</b> <ul style="list-style-type: none"> <li>The maximum size of a single certificate file that can be uploaded is 500 KB.</li> <li>If the SSL certificate is not used, your data may be at risk.</li> </ul>
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 <b>RDS DB instance</b> .
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an <b>RDS DB instance</b> .
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 2-17** DR database information

### Destination Database

DB Instance Name

Database Username

Database Password

 Test successful

**Table 2-16** DR database settings

Parameter	Description
DB Instance Name	The GaussDB(for MySQL) primary/standby instance you selected when creating the DR. This parameter cannot be changed.
Database Username	The username for accessing the DR database.
Database Password	<p>The password for the database username. The password can be changed after a task is created.</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress, or Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Update Password</b> next to the <b>Destination Database Password</b> field. In the displayed dialog box, change the password. This action only updates DRS with the changed password.</p> <p>The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.</p>

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

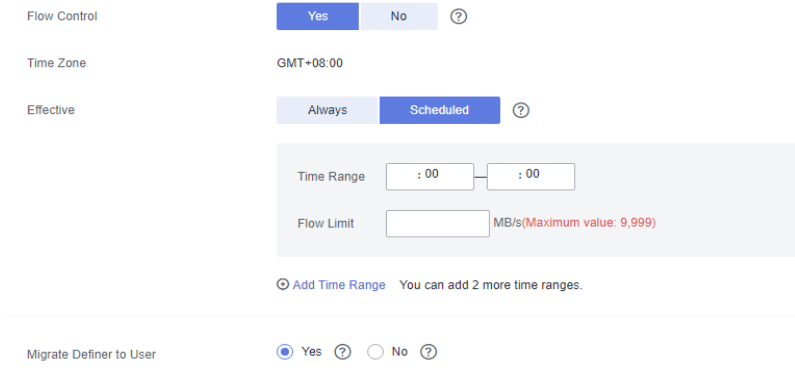
**Figure 2-18** DR settings



The image shows a configuration interface for DR settings. It contains two rows of settings, each enclosed in a dashed border. The first row is for 'Flow Control', with 'Yes' and 'No' buttons and a help icon. The 'No' button is selected. The second row is for 'Migrate Definer to User', with radio buttons for 'Yes' and 'No', and help icons. The 'Yes' radio button is selected.

Flow Control	<input type="button" value="Yes"/>	<input checked="" type="button" value="No"/>	<input type="button" value="?"/>
Migrate Definer to User	<input checked="" type="radio"/>	<input type="radio"/>	<input type="button" value="?"/>

**Table 2-17** DR settings

Parameter	Description
Flow Control	<p>You can choose whether to control the flow.</p> <ul style="list-style-type: none"> <li> <b>Yes</b>                      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 <b>All day</b>. 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.                 </li> </ul> <p><b>Figure 2-19</b> Flow control</p>  <ul style="list-style-type: none"> <li> <b>No</b>                      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.                 </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Flow control mode takes effect during the initial DR phase only.</li> <li>You can also change the flow control mode when the task is in the <b>Configuration</b> state. On the <b>Basic Information</b> tab, in the <b>DR Information</b> area, click <b>Modify</b> next to <b>Flow Control</b>. In the dialog box that is displayed, change the flow control mode. The flow control mode cannot be changed for a task that is in <b>Starting</b> state.</li> </ul>

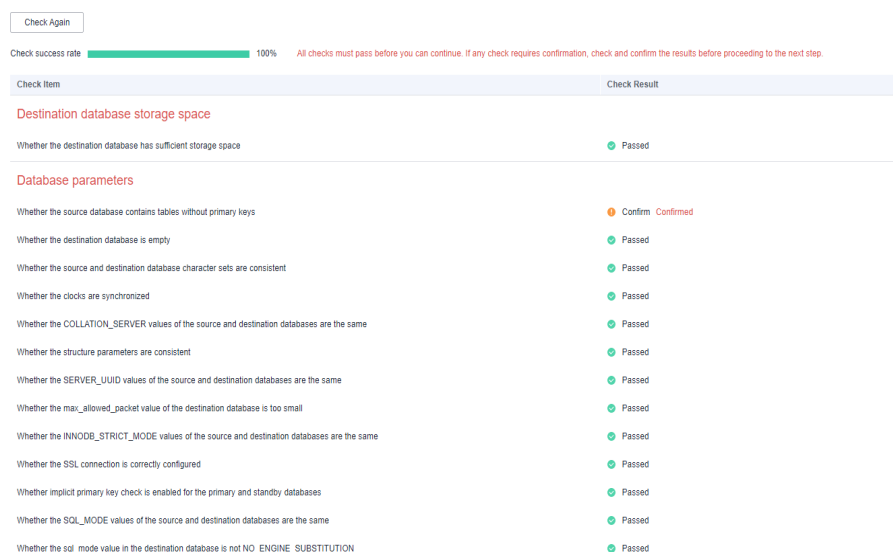
Parameter	Description
Migrate Definer to User	<ul style="list-style-type: none"> <li><b>Yes</b> The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see <a href="#">How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?</a></li> <li><b>No</b> 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.</li> </ul>

**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 [Checking Whether the Source Database Is Connected](#) in *Data Replication Service User Guide*.

**Figure 2-20** 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 2-21** Task startup settings


**Table 2-18** Task and recipient description

Parameter	Description
Start Time	Set <b>Start Time</b> to <b>Start upon task creation</b> or <b>Start at a specified time</b> based on site requirements. <b>NOTE</b> 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 <a href="#">Simple Message Notification User Guide</a> .
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. <b>NOTE</b> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>



Parameter	Description
RTO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the RTO delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RPO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> <li>• 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.</li> </ul>
Stop Abnormal Tasks After	<p>Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is <b>14</b>.</p> <p><b>NOTE</b></p> <p>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.</p>

**Step 7** After the DR 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.

----End

## 2.3 From DDM to DDM Single-Active DR

### Supported Source and Destination Databases

Table 2-19 Supported databases

Service database	DR Database
<ul style="list-style-type: none"><li>• DDM instances</li></ul>	<ul style="list-style-type: none"><li>• DDM instances</li></ul>

### 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. 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 2-20** Environment Constraints

Type	Restrictions
Database permissions	<ul style="list-style-type: none"> <li>• The user of the service database must have at least one permission, for example, SELECT.</li> <li>• The user of the DR database must have at least one permission, for example, SELECT.</li> </ul>
Disaster recovery objects	<ul style="list-style-type: none"> <li>• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery.</li> <li>• Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery.</li> <li>• System tables are not supported.</li> <li>• Triggers and events do not support disaster recovery.</li> <li>• Backup and disaster recovery, cross-database DDL, and rename operations cannot be performed on some specified service databases. Otherwise, the disaster recovery fails.</li> <li>• Disaster recovery of DDM account permissions is not supported.</li> </ul>
Service database configuration	<ul style="list-style-type: none"> <li>• In the public network, EIPs must be bound to each DDM instance and the associated RDS MySQL instance.</li> <li>• The binlog of the RDS MySQL instance associated with the DDM instance must be enabled and uses the ROW format and GTID.</li> <li>• If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days.</li> <li>• The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_).</li> <li>• The table name in the service database cannot contain non-ASCII characters, or the following characters: '&lt;&gt;/\</li> </ul>

Type	Restrictions
DR database configuration	<ul style="list-style-type: none"><li>• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal.</li><li>• The DR DB instance must have sufficient storage space.</li><li>• The binlog and GTID of the RDS instance associated with the DDM instance must be enabled.</li><li>• The minor version of the DR DDM instance must be the same as that of the service DDM instance.</li><li>• The number of DDM disaster recovery instances must be the same as that of the RDS instances associated with the DDM service instance.</li><li>• The sharding rules of the DDM disaster recovery instance must be the same as those of the DDM service instance. You are advised to use the schema import and export functions to ensure sharding rule consistency.</li></ul>

Type	Restrictions
Precautions	<ul style="list-style-type: none"> <li>● 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.</li> <li>● The service database does not support point-in-time recovery (PITR).</li> <li>● Binlogs cannot be forcibly deleted. Otherwise, the DR task fails.</li> <li>● Resumable upload is supported, but data may be repeatedly inserted into a table that does not have a primary key.</li> <li>● Migration or synchronization tasks cannot be created when a DR task exists.</li> <li>● 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.</li> <li>● The DDM DR database cannot create schemas automatically. You need to set the schema rules before disaster recovery.</li> <li>● DDM schemas cannot be added during disaster recovery.</li> <li>● During DR, rebalance and reshard operations cannot be performed on DDM schemas</li> <li>● 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.</li> <li>● 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.</li> <li>● During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal.</li> <li>● 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.</li> </ul>

## 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, specify the task name, description, and the DR instance details, and click **Next**.

**Figure 2-22** DR task information

**Table 2-21** Task and recipient description

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

**Figure 2-23** DR instance information

**Disaster Recovery Instance Details**

The following information cannot be modified after you go to the next page.

- \* DR Type: **Single-active** | Dual-active ?
- \* Disaster Recovery Relationship: **Current cloud as standby** | Current cloud as active
- \* Service DB Engine: MySQL | Cassandra | **DDM** | GaussDB(for MySQL) Primary/Standby Ed...
- \* DR DB Engine: **DDM**
- \* Network Type: **Public network** ?  
 I understand that an EIP will be automatically bound to the replication instance and released after the synchronization task is complete.
- \* DR DB Instance: No DB instance available ? [View DB Instance](#) [View Unselectable DB Instance](#)
- \* Disaster Recovery Instance Subnet: Select the subnet ? [View Subnets](#) [View occupied IP address](#)
- \* Destination DB Instance Access: **Read-only**  
During the disaster recovery, the destination DB instance becomes read-only to ensure the integrity and success of disaster recovery. When the disaster recovery is complete, it becomes readable and writable.

---

- \* Enterprise Project: --Select-- ? [View Project Management](#)

---

Tags: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) ?

Tag key:  Tag value:

You can add 10 more tags.

**Table 2-22** DR instance settings

Parameter	Description
DR Type	<p>Select <b>Single-active</b>.</p> <p>The DR type can be single-active or dual-active. If <b>Dual-active</b> is selected, two subtasks are created by default, a forward DR task and a backward DR task.</p> <p><b>NOTE</b> 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 <b>Service Tickets &gt; Create Service Ticket</b> to submit a service ticket.</p>
Disaster Recovery Relationship	<p>Select <b>Current cloud as standby</b>. This parameter is available only when you select <b>Single-active</b>.</p> <p>By default, <b>Current cloud as standby</b> is selected. You can also select <b>Current cloud as active</b>.</p> <ul style="list-style-type: none"> <li>• <b>Current cloud as standby</b>: The DR database is on the current cloud.</li> <li>• <b>Current cloud as active</b>: The service database is on the current cloud.</li> </ul>
Service DB Engine	Select <b>DDM</b> .
DR DB Engine	Select <b>DDM</b> .
Network Type	<p>The public network is used as an example.</p> <p>Available options: <b>VPN or Direct Connect</b> and <b>Public network</b>. By default, the value is <b>Public network</b>.</p>
DR DB Instance	The DDM instance you created.
Disaster Recovery Instance Subnet	<p>Select the subnet where the disaster recovery instance is located. You can also click <b>View Subnet</b> to go to the network console to view the subnet where the instance resides.</p> <p>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.</p>

Parameter	Description
Destination Database Access	<p>Select <b>Read-only</b>. This parameter is available only when you select <b>Single-active</b>.</p> <p>During single-active disaster recovery, the DR database becomes read-only. To change the DR database to <b>Read/Write</b>, you can change the DR database (or destination database) to a service database by clicking <b>Promote Current Cloud</b> on the <b>Disaster Recovery Monitoring</b> tab. After the DR task is complete or deleted, you can query and read data to the DR database.</p> <p>When the external database functions as the DR database, the user with the superuser permission can set the database to read-only.</p> <p>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.</p>
Enterprise Project	<ul style="list-style-type: none"> <li>• If the DB instance has been associated with an enterprise project, select the target project from the <b>Enterprise Project</b> drop-down list.</li> <li>• You can also go to the ProjectMan console to create a project. For details about how to create a project, see <i>ProjectMan User Guide</i>.</li> </ul>
Tags	<ul style="list-style-type: none"> <li>• This setting is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 10 tags.</li> <li>• After a task is created, you can view its tag details on the <b>Tags</b> tab. For details, see <a href="#">Tag Management</a>.</li> </ul>

**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 2-24** Service database information

**Source Database**

Source Database Type

Region

DB Instance Name  [View DB Instance](#) [View Unselectable DB Instance](#)

Database Username

Database Password

**Table 2-23** Service database settings

Parameter	Description
Source Database Type	Select a service database type.
Region	The region where the service DB instance is located. This parameter is selected by default.
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 2-25** DR database information

**Destination Database**

DB Instance Name

Database Username

Database Password

**Table 2-24** DR database settings

Parameter	Description
DB Instance Name	The DDM instance you selected when you create a synchronization task. The instance name cannot be changed.
Database Username	The username for accessing the DR database.
Database Password	<p>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:</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress</b>, or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p> <p>The database username and password are encrypted and stored in the system, and will be cleared after the task is deleted.</p>


- Select **Current cloud as active** for **Disaster Recovery Relationship** in [Step 2](#).

**Figure 2-26** Service database information

### Source Database

DB Instance Name Auto-ddm-

Database Username

Database Password  

**Table 2-25** Service database settings

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

Parameter	Description
Database Username	The username for accessing the service database.
Database Password	<p>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:</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress, or Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p> <p>The database username and password are encrypted and stored in the system, and will be cleared after the task is deleted.</p>

Figure 2-27 DR database information

#### Destination Database

Database Type: DDM

Region:

DB Instance Name:  [View DB Instance](#) [View Unselectable DB Instance](#)

Database Username:

Database Password:

This button is available only after the replication instance is created successfully.

Table 2-26 DR database settings

Parameter	Description
Database Type	Type of the DR database.
Region	The region where the DDM instance is located.
DB Instance Name	<p>Name of the DR instance.</p> <p><b>NOTE</b> 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.</p>
Database Username	Username for logging in to the DR database.

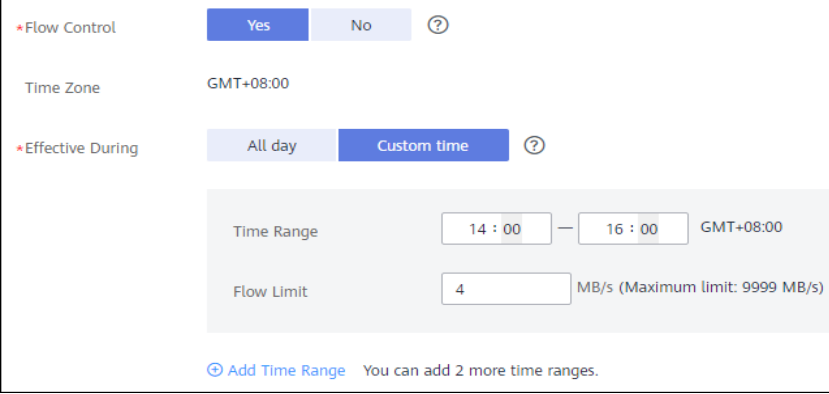
Parameter	Description
Database Password	Password for the database username.

 **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 2-27** DR settings

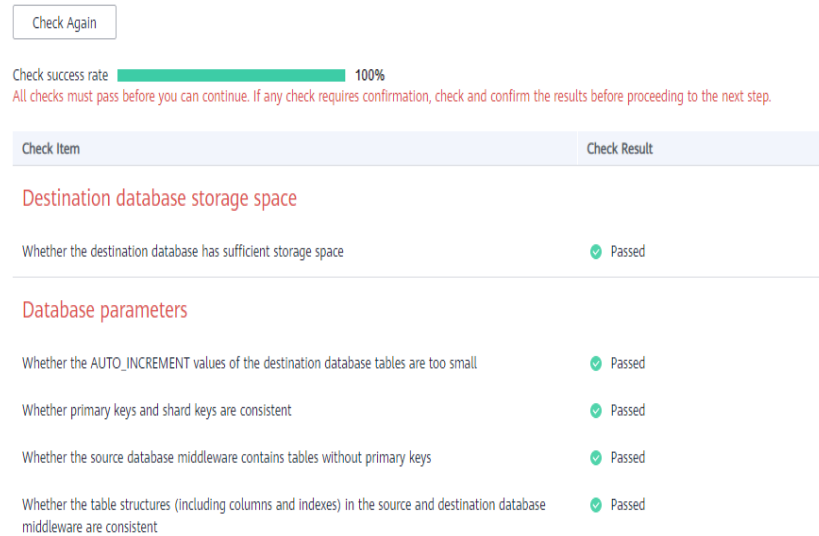
Parameter	Description
Flow Control	<p>You can choose whether to control the flow.</p> <ul style="list-style-type: none"> <li> <b>Yes</b>                      You can customize the maximum DR speed.                      In addition, you can set the time range based on your service requirements. The traffic 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 <b>All day</b>. 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.                 </li> </ul> <p><b>Figure 2-28</b> Flow control</p>  <ul style="list-style-type: none"> <li> <b>No</b>                      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.                 </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- Flow control mode takes effect only in the DR initialization phase.</li> <li>- You can also change the flow control mode when the task is in the <b>Configuration</b> state. On the <b>Basic Information</b> tab, in the <b>DR Information</b> area, click <b>Modify</b> next to <b>Flow Control</b>. In the dialog box that is displayed, change the flow control mode. The flow control mode cannot be changed for a task that is in <b>Starting</b> state.</li> </ul>

**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 [Checking Whether the Source Database Is Connected](#) in *Data Replication Service User Guide*.

Figure 2-29 Pre-check



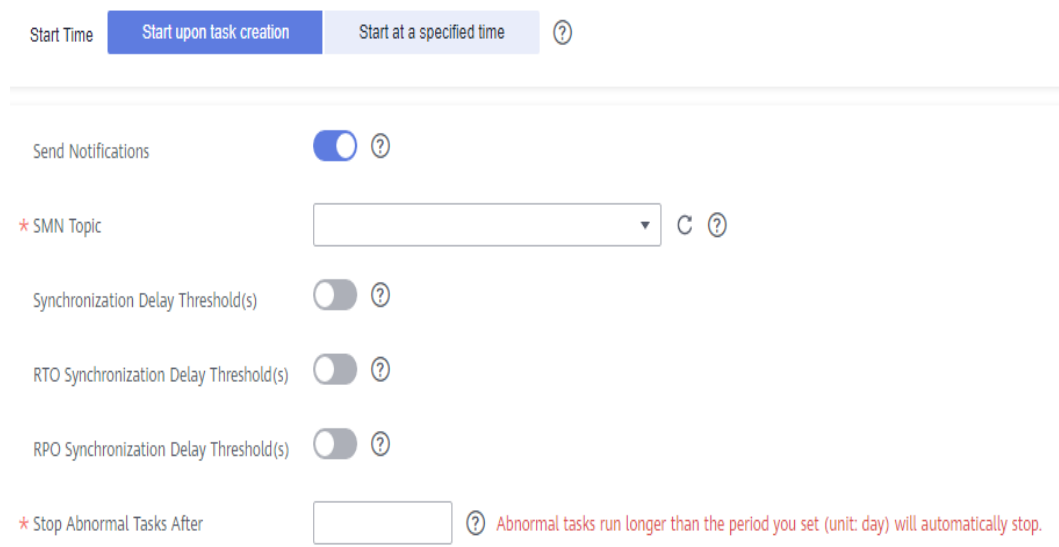
- If the check is complete and the check success rate is 100%, click **Next**.

**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 2-30 Task startup settings




**Table 2-28** Task and recipient description

Parameter	Description
Start Time	<p>Set <b>Start Time</b> to <b>Start upon task creation</b> or <b>Start at a specified time</b> based on site requirements.</p> <p><b>NOTE</b> 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.</p>
Send Notifications	<p>SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.</p>
SMN Topic	<p>This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber.</p> <p>For details, see <a href="#">Simple Message Notification User Guide</a>.</p>
Synchronization Delay Threshold	<p>During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database.</p> <p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RTO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the RTO delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>

Parameter	Description
RPO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> <li>• 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.</li> </ul>
Stop Abnormal Tasks After	<p>Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is <b>14</b>.</p> <p><b>NOTE</b></p> <p>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.</p>

**Step 7** After the DR 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.

----End

## 2.4 From GaussDB(for MySQL) Primary/Standby to GaussDB(for MySQL) Primary/Standby (Single-Active DR)

### Supported Source and Destination Databases

**Table 2-29** Supported databases

Service database	DR Database
<ul style="list-style-type: none"> <li>• GaussDB(for MySQL) primary/standby</li> </ul>	<ul style="list-style-type: none"> <li>• GaussDB(for MySQL) primary/standby</li> </ul>



## 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. 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 2-30** Precautions

Type	Restrictions
Database permissions	<ul style="list-style-type: none"> <li>● The service database 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.</li> <li>● The DR database 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.</li> <li>● The <b>root</b> account of the GaussDB(for MySQL) primary/standby instance has the preceding permissions by default.</li> </ul>
Disaster recovery objects	<ul style="list-style-type: none"> <li>● Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery.</li> <li>● System tables are not supported.</li> <li>● Triggers and events do not support disaster recovery.</li> <li>● Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery.</li> <li>● Backup and disaster recovery, cross-database DDL, and rename operations cannot be performed on some specified service databases. Otherwise, the disaster recovery fails.</li> </ul>
Service database configuration	<ul style="list-style-type: none"> <li>● The binlog of the service database must be enabled and use the row-based format.</li> <li>● If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days.</li> <li>● GTID must be enabled for the database.</li> <li>● The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_).</li> <li>● The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '&lt;&gt;\'</li> </ul>

Type	Restrictions
DR database configuration	<ul style="list-style-type: none"><li>• The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal.</li><li>• The DR DB instance must have sufficient storage space.</li><li>• The major version of the DR database must be the same as that of the service database.</li><li>• The DR database must be an empty instance. After the DR task starts, the DR database is set to read-only.</li><li>• The binlog of the DR database must be enabled and use the row-based format.</li><li>• GTID must be enabled for the DR database.</li></ul>

Type	Restrictions
Precautions	<ul style="list-style-type: none"> <li>● 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.</li> <li>● The service database does not support point-in-time recovery (PITR).</li> <li>● Binlogs cannot be forcibly deleted. Otherwise, the DR task fails.</li> <li>● 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.</li> <li>● If the DCC does not support instances with 4 vCPUs and 8 GB memory or higher instance specifications, the DR task cannot be created.</li> <li>● Resumable upload is supported, but data may be repeatedly inserted into a table that does not have a primary key.</li> <li>● Migration or synchronization tasks cannot be created when a DR task exists.</li> <li>● 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.</li> <li>● 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.</li> <li>● 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.</li> <li>● 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.</li> <li>● 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.</li> <li>● During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal.</li> </ul>

Type	Restrictions
	<ul style="list-style-type: none"> <li>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.</li> </ul>

## 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, specify the task name, description, and the DR instance details, and click **Next**.

**Figure 2-31** DR task information

**Table 2-31** Task and recipient description

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

**Figure 2-32** DR instance information

**Disaster Recovery Instance Details**

The following information cannot be modified after you go to the next page.

- \* DR Type:  Single-active  Dual-active ⓘ
- \* Disaster Recovery Relationship:  Current cloud as standby  Current cloud as active
- \* Service DB Engine:  MySQL  Cassandra  DDM  GaussDB(for MySQL) Primary/Standby Ed...
- \* DR DB Engine:  GaussDB(for MySQL) Primary/Standby Ed...
- \* Network Type:  ⓘ
- I understand that an EIP will be automatically bound to the replication instance and released after the synchronization task is complete.
- \* DR DB Instance:  ⓘ [View DB Instance](#) [View Unselectable DB Instance](#)
- \* Disaster Recovery Instance Subnet:  ⓘ [View Subnets](#) [View occupied IP address](#)
- \* Destination DB Instance Access:  Read-only

During the disaster recovery, the destination DB instance becomes read-only to ensure the integrity and success of disaster recovery. When the disaster recovery is complete, it becomes readable and writable.

---

- \* Enterprise Project:  ⓘ [View Project Management](#) ⓘ

---

Tags

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) ⓘ

You can add 10 more tags.

**Table 2-32** DR instance settings

Parameter	Description
DR Type	Select <b>Single-active</b> . The DR type can be single-active or dual-active. If <b>Dual-active</b> is selected, two subtasks are created by default, a forward DR task and a backward DR task. <b>NOTE</b> 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 <b>Service Tickets &gt; Create Service Ticket</b> to submit a service ticket.
Disaster Recovery Relationship	Select <b>Current cloud as standby</b> . This parameter is available only when you select <b>Single-active</b> . By default, <b>Current cloud as standby</b> is selected. You can also select <b>Current cloud as active</b> . <ul style="list-style-type: none"> <li>• <b>Current cloud as standby</b>: The DR database is on the current cloud.</li> <li>• <b>Current cloud as active</b>: The service database is on the current cloud.</li> </ul>
Service DB Engine	Select <b>GaussDB(for MySQL) Primary/Standby Edition</b> .
DR DB Engine	Select <b>GaussDB(for MySQL) Primary/Standby Edition</b> .

Parameter	Description
Network Type	The public network is used as an example. Available options: <b>VPN or Direct Connect</b> and <b>Public network</b> . By default, the value is <b>Public network</b> .
DR DB Instance	The GaussDB(for MySQL) primary/standby instance you created.
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click <b>View Subnet</b> 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 <b>Read-only</b> . This parameter is available only when you select <b>Single-active</b> .  During single-active disaster recovery, the DR database becomes read-only. To change the DR database to <b>Read/Write</b> , you can change the DR database (or destination database) to a service database by clicking <b>Promote Current Cloud</b> on the <b>Disaster Recovery Monitoring</b> tab. After the DR task is complete or deleted, you can query and read data to the DR database.  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.
Enterprise Project	<ul style="list-style-type: none"> <li>• If the DB instance has been associated with an enterprise project, select the target project from the <b>Enterprise Project</b> drop-down list.</li> <li>• You can also go to the ProjectMan console to create a project. For details about how to create a project, see <i>ProjectMan User Guide</i>.</li> </ul>
Tags	<ul style="list-style-type: none"> <li>• This setting is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 10 tags.</li> <li>• After a task is created, you can view its tag details on the <b>Tags</b> tab. For details, see <a href="#">Tag Management</a>.</li> </ul>

**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 2-33** Service database information

### Source Database

**Table 2-33** Service database settings

Parameter	Description
Source Database Type	By default, <b>Self-built on ECS</b> is selected. The source database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b> . After selecting <b>RDS DB instance</b> , 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 <b>RDS DB instance</b> 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	<p>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:</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress</b>, or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p>
SSL Connection	<p>SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- The maximum size of a single certificate file that can be uploaded is 500 KB.</li> <li>- If the SSL certificate is not used, your data may be at risk.</li> </ul>
Region	<p>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 <b>RDS DB instance</b>.</p>
DB Instance Name	<p>The name of the service DB instance. This parameter is available only when the source database is an <b>RDS DB instance</b>.</p>
Database Username	<p>The username for accessing the service database.</p>
Database Password	<p>The password for the service database username.</p>

 **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 2-34** DR database information

### Destination Database

DB Instance Name

Database Username

Database Password  

 Test successful

**Table 2-34** DR database settings

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

- Select **Current cloud as active** for **Disaster Recovery Relationship** in [Step 2](#).

**Figure 2-35** Service database information

**Source Database**

DB Instance Name

Database Username

Database Password

**Table 2-35** Service database settings

Parameter	Description
DB Instance Name	The GaussDB(for MySQL) primary/standby instance you selected when creating the DR. This parameter cannot be changed.
Database Username	The username for accessing the service database.
Database Password	<p>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:</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress, or Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p> <p>The database username and password are encrypted and stored in the system, and will be cleared after the task is deleted.</p>

**Figure 2-36** DR database information

**Source Database**

Source Database Type  Self-built on ECS  RDS DB instance

Region

DB Instance Name  [View DB Instance](#) [View Unselectable DB Instance](#)

Database Username

Database Password

✔ Test successful

**Table 2-36** DR database settings

Parameter	Description
Database Type	By default, <b>Self-built on ECS</b> is selected. The destination database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b> . If you select <b>RDS DB instance</b> , you need to select the region where the destination database is located.
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.
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 <b>Starting, Initializing, Disaster recovery in progress</b> , or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b> . 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.  <b>NOTE</b> The maximum size of a single certificate file that can be uploaded is 500 KB.
Region	Region where the GaussDB (for MySQL) primary/standby instance is located. This parameter is available only when the source database is an RDS DB instance.
DB Instance Name	DR instance name. This parameter is available only when the source database is an RDS DB instance.  <b>NOTE</b> 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**.

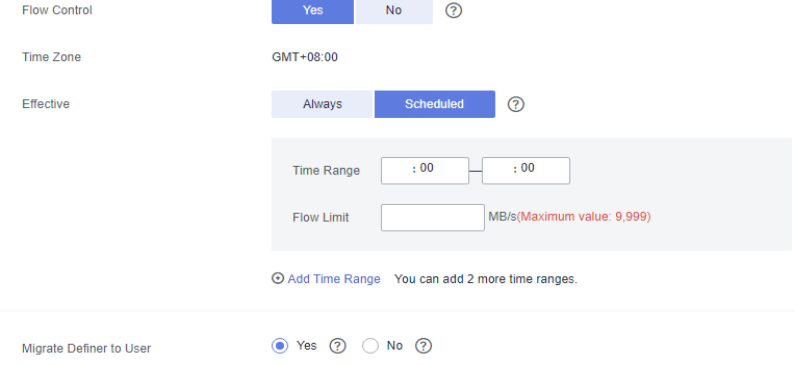
**Figure 2-37** DR settings



The screenshot shows a configuration interface for DR settings. It contains two rows of settings:

- Flow Control:** A toggle switch with 'Yes' (light blue) and 'No' (dark blue) options. The 'No' option is selected. A help icon (?) is visible to the right.
- Migrate Definer to User:** A radio button selection with 'Yes' (selected, blue circle) and 'No' (unselected, white circle) options. Help icons (?) are visible to the right of each option.

**Table 2-37** DR settings

Parameter	Description
Flow Control	<p>You can choose whether to control the flow.</p> <ul style="list-style-type: none"> <li> <b>Yes</b>                      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 <b>All day</b>. 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.                 </li> </ul> <p><b>Figure 2-38</b> Flow control</p>  <ul style="list-style-type: none"> <li> <b>No</b>                      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.                 </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Flow control mode takes effect during the initial DR phase only.</li> <li>You can also change the flow control mode when the task is in the <b>Configuration</b> state. On the <b>Basic Information</b> tab, in the <b>DR Information</b> area, click <b>Modify</b> next to <b>Flow Control</b>. In the dialog box that is displayed, change the flow control mode. The flow control mode cannot be changed for a task that is in <b>Starting</b> state.</li> </ul>

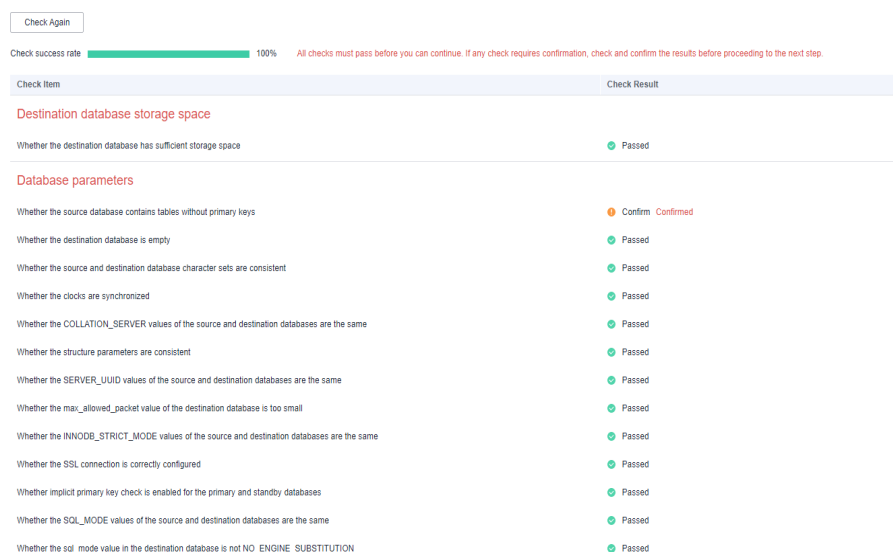
Parameter	Description
Migrate Definer to User	<ul style="list-style-type: none"> <li> <b>Yes</b>                      The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see <a href="#">How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?</a> </li> <li> <b>No</b>                      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.                 </li> </ul>

**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 [Checking Whether the Source Database Is Connected](#) in *Data Replication Service User Guide*.

**Figure 2-39** Pre-check



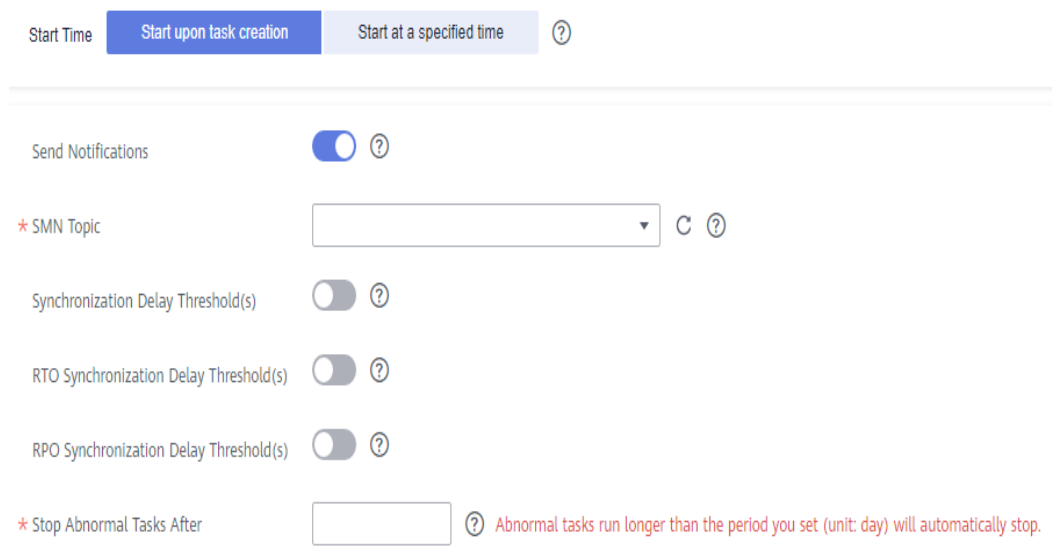
- If the check is complete and the check success rate is 100%, click **Next**.

**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 2-40** Task startup settings




**Table 2-38** Task and recipient description

Parameter	Description
Start Time	Set <b>Start Time</b> to <b>Start upon task creation</b> or <b>Start at a specified time</b> based on site requirements. <b>NOTE</b> 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 <a href="#">Simple Message Notification User Guide</a> .
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. <b>NOTE</b> <ul style="list-style-type: none"> <li>Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>



Parameter	Description
RTO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the RTO delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RPO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> <li>• 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.</li> </ul>
Stop Abnormal Tasks After	<p>Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is <b>14</b>.</p> <p><b>NOTE</b></p> <p>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.</p>

**Step 7** After the DR 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.

----End

## 2.5 From MySQL to MySQL (Dual-Active DR)

### Supported Source and Destination Databases

Table 2-39 Supported databases

Service database	DR Database
<ul style="list-style-type: none"><li>On-premises MySQL databases</li><li>MySQL databases on an ECS</li><li>MySQL databases on other clouds</li><li>RDS for MySQL</li></ul>	<ul style="list-style-type: none"><li>RDS for MySQL</li></ul>

### 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. 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
Database permissions	<ul style="list-style-type: none"> <li>• The service database 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.</li> <li>• The DR database 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.</li> <li>• The <b>root</b> account of the RDS MySQL DB instance has the preceding permissions by default.</li> </ul>
Disaster recovery objects	<ul style="list-style-type: none"> <li>• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery.</li> <li>• System tables are not supported.</li> <li>• Triggers and events do not support disaster recovery.</li> <li>• Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery.</li> <li>• DDL operations cannot be executed on the active database 2.</li> </ul>

Type	Restrictions
Service database configuration	<ul style="list-style-type: none"> <li>● The binlog of the MySQL service database must be enabled and use the row-based format.</li> <li>● If the storage space is sufficient, you are advised to store the service database binlog for as long as possible. The recommended retention period is seven days.</li> <li>● The service database username or password cannot be empty.</li> <li>● <b>server_id</b> in the MySQL service database must be set. If the service database version is MySQL 5.6 or earlier, the <b>server_id</b> value ranges from <b>2</b> to <b>4294967296</b>. If the service database is MySQL 5.7 or later, the <b>server_id</b> value ranges from <b>1</b> to <b>4294967296</b>.</li> <li>● GTID must be enabled for the database.</li> <li>● The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_).</li> <li>● The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '&lt;&gt;/\</li> <li>● If the <b>expire_logs_days</b> value of the database is set to <b>0</b>, the disaster recovery may fail.</li> </ul>
DR database configuration	<ul style="list-style-type: none"> <li>● The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal.</li> <li>● The DR DB instance must have sufficient storage space.</li> <li>● The major version of the active database 1 must be the same as that of the active database 2.</li> <li>● 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.</li> </ul>

Type	Restrictions
Precautions	<ul style="list-style-type: none"> <li>● Only whitelisted users can use this function. To use this function, submit a service ticket.</li> <li>● 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 heavy 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 <a href="#">Common Exceptions in Real-Time Disaster</a>.</li> <li>● During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal.</li> <li>● 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.             <ul style="list-style-type: none"> <li>– When the deletion operation is performed, data is deleted and DRS does not perform any operation.</li> <li>– When the insert operation is performed, DRS updates data with the latest inserted data.</li> <li>– When the update operation is performed, the original data has been updated and DRS directly insert the new data.</li> </ul> </li> <li>● 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.</li> <li>● 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.</li> <li>● Cascade operations cannot be performed on tables with foreign keys.</li> <li>● The dual-active DR is different from the single-active DR. Therefore, no active/standby switchover is required.</li> <li>● 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.)</li> </ul>

Type	Restrictions
	<ul style="list-style-type: none"> <li>• Ensure that the tables, columns, and rows are consistent in both the databases. (The table structures of both the active databases are consistent.)</li> <li>• 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.</li> <li>• 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.</li> </ul>

## 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, specify the task name, description, and the DR instance details, and click **Next**.

**Figure 2-41** 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.
Task Name	The task name consists of 4 to 50 characters, starts with a letter, and can contain only letters (case-insensitive), digits, hyphens (-), and underscores (_).
Description	The description consists of a maximum of 256 characters and cannot contain special characters !=<>'&"\

**Figure 2-42** DR instance information

**Disaster Recovery Instance Details**

The following information cannot be modified after you go to the next page.

\* DR Type: Single-active **Dual-active** ⓘ

\* Current Cloud RDS Instance Role: Active 1 **Active 2**  
Active 2 indicates that the database is empty and waiting for initial data synchronization. If this role is not correctly selected, the precheck will fail. [Learn more about the role selection.](#)  
 In the initial phase, if the databases at both ends are empty, you can select either Active 1 or Active 2.

\* Service DB Engine: **MySQL** Cassandra DDM GaussDB(for MySQL) Primary/Standby Ed...

\* DR DB Engine: **MySQL**

\* Network Type: Public network ⓘ  
 I understand that an EIP will be automatically bound to the replication instance and released after the synchronization task is complete.

\* DR DB Instance: Select an instance ⓘ [View DB Instance](#) [View Unselectable DB Instance](#)

\* Disaster Recovery Instance Subnet: Select the subnet ⓘ [View Subnets](#)

---

\* Enterprise Project: --Select-- ⓘ [View Project Management](#) ⓘ

---

Tags: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) ⓘ

You can add 10 more tags.

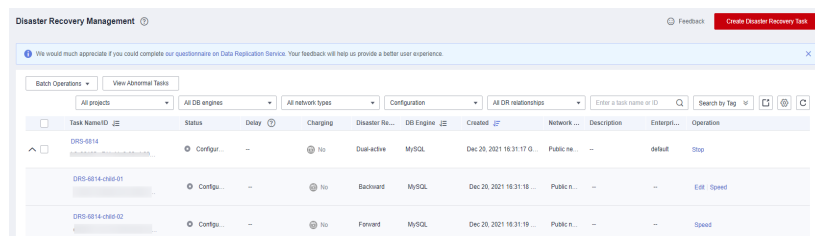
**Table 2-42** DR instance settings

Parameter	Description
DR Type	Select <b>Dual-active</b> . The DR type can be single-active or dual-active. If <b>Dual-active</b> is selected, two subtasks are created by default, a forward DR task and a backward DR task. <b>NOTE</b> 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 <b>Service Tickets &gt; Create Service Ticket</b> to submit a service ticket.
Current Cloud RDS Instance Role	Select <b>Active 1</b> or <b>Active 2</b> . This parameter specifies the role of the current RDS DB instance in the DR relationship and is available when <b>DR Type</b> is set to <b>Dual-active</b> . For details about how to choose active 1 and 2, see <a href="#">How Do I Select Active Database 1 and 2 for Dual-Active DR?</a> <ul style="list-style-type: none"> <li>Active 1: Initial data is available on the current cloud RDS when a task is created.</li> <li>Active 2: The RDS DB instance on the current cloud is empty when a task is created.</li> </ul> Active 2 is used as an example.
Service DB Engine	Select <b>MySQL</b> .
DR DB Engine	Select <b>MySQL</b> .

Parameter	Description
Network Type	The public network is used as an example. Available options: <b>VPN or Direct Connect</b> and <b>Public network</b> . By default, the value is <b>Public network</b> .
DR DB Instance	The RDS MySQL instance you created.
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click <b>View Subnet</b> 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.
Enterprise Project	<ul style="list-style-type: none"> <li>If the DB instance has been associated with an enterprise project, select the target project from the <b>Enterprise Project</b> drop-down list.</li> <li>You can also go to the ProjectMan console to create a project. For details about how to create a project, see <i>ProjectMan User Guide</i>.</li> </ul>
Tags	<ul style="list-style-type: none"> <li>This setting is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 10 tags.</li> <li>After a task is created, you can view its tag details on the <b>Tags</b> tab. For details, see <a href="#">Tag Management</a>.</li> </ul>

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

**Figure 2-43** 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 2-44** Service database information

Source Database

Source Database Type:  Self-built on ECS  RDS DB Instance

IP Address or Domain Name:

Port:

Database Username:

Database Password:

SSL Connection:

If you want to enable SSL connection, ensure that SSL has been enabled on the source database, related parameters have been correctly configured, and an SSL certificate has been uploaded.

Encryption Certificate:

**Table 2-43** Service database settings

Parameter	Description
Source Database Type	By default, <b>Self-built on ECS</b> is selected. The source database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b> . After selecting <b>RDS DB instance</b> , 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 <b>RDS DB instance</b> 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 <b>Starting</b> , <b>Initializing</b> , <b>Disaster recovery in progress</b> , or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Update Password</b> next to the <b>Source Database Password</b> field. In the displayed dialog box, change the password. This action only updates DRS with the changed 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. <b>NOTE</b> <ul style="list-style-type: none"> <li>The maximum size of a single certificate file that can be uploaded is 500 KB.</li> <li>If the SSL certificate is not used, your data may be at risk.</li> </ul>
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 <b>RDS DB instance</b> .
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an <b>RDS DB instance</b> .
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 2-45** DR database information

### Destination Database

DB Instance Name

Database Username

Database Password

 Test successful

**Table 2-44** DR database settings

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

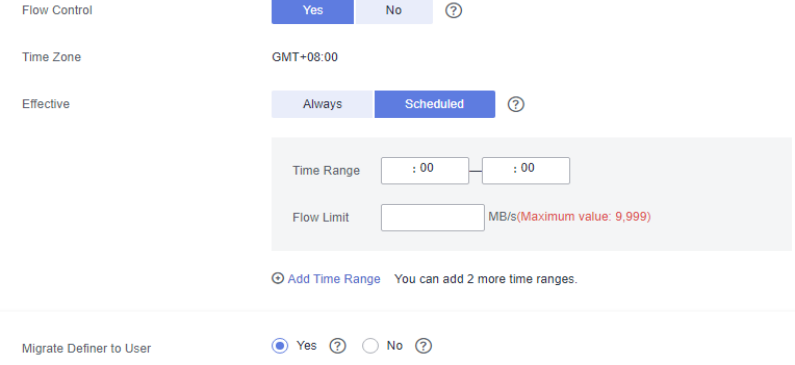
Parameter	Description
Database Username	The username for accessing the DR database.
Database Password	<p>The password for the database username. The password can be changed after a task is created.</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress</b>, or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Update Password</b> next to the <b>Destination Database Password</b> field. In the displayed dialog box, change the password. This action only updates DRS with the changed password.</p> <p>The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.</p>

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

**Figure 2-46** DR settings



**Table 2-45** DR settings

Parameter	Description
Flow Control	<p>You can choose whether to control the flow.</p> <ul style="list-style-type: none"> <li> <b>Yes</b>                      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 <b>All day</b>. 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.                 </li> </ul> <p><b>Figure 2-47</b> Flow control</p>  <ul style="list-style-type: none"> <li> <b>No</b>                      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.                 </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Flow control mode takes effect during the initial DR phase only.</li> <li>You can also change the flow control mode when the task is in the <b>Configuration</b> state. On the <b>Basic Information</b> tab, in the <b>DR Information</b> area, click <b>Modify</b> next to <b>Flow Control</b>. In the dialog box that is displayed, change the flow control mode. The flow control mode cannot be changed for a task that is in <b>Starting</b> state.</li> </ul>

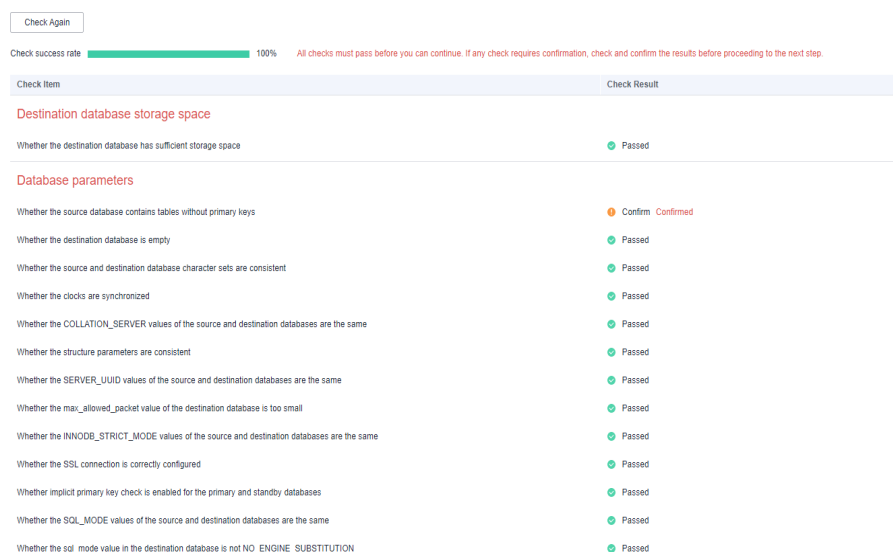
Parameter	Description
Migrate Definer to User	<ul style="list-style-type: none"> <li><b>Yes</b> The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see <a href="#">How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?</a></li> <li><b>No</b> 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.</li> </ul>

**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 [Checking Whether the Source Database Is Connected](#) in *Data Replication Service User Guide*.

**Figure 2-48** 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**, **Stop Abnormal Tasks After** and DR instance details. Then, click **Submit**.


**Figure 2-49** Task startup settings

**Table 2-46** Task and recipient description

Parameter	Description
Start Time	Set <b>Start Time</b> to <b>Start upon task creation</b> or <b>Start at a specified time</b> based on site requirements. <b>NOTE</b> 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 <a href="#">Simple Message Notification User Guide</a> .
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. <b>NOTE</b> <ul style="list-style-type: none"> <li>Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>

Parameter	Description
RTO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the RTO delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RPO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> <li>• 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.</li> </ul>
Stop Abnormal Tasks After	<p>Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is <b>14</b>.</p> <p><b>NOTE</b></p> <p>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.</p>

**Step 8** After the DR 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.

----End

## 2.6 From GaussDB(for MySQL) Primary/Standby to GaussDB(for MySQL) Primary/Standby (Dual-Active DR)

### Supported Source and Destination Databases

Table 2-47 Supported databases

Service database	DR Database
<ul style="list-style-type: none"><li>GaussDB(for MySQL) primary/standby</li></ul>	<ul style="list-style-type: none"><li>GaussDB(for MySQL) primary/standby</li></ul>

### 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. 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 2-48** Precautions

Type	Restrictions
Database permissions	<ul style="list-style-type: none"> <li>• The service database 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.</li> <li>• The DR database 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.</li> <li>• The <b>root</b> account of the GaussDB(for MySQL) primary/standby instance has the preceding permissions by default.</li> </ul>
Disaster recovery objects	<ul style="list-style-type: none"> <li>• Tables with storage engine different to MyISAM and InnoDB do not support disaster recovery.</li> <li>• System tables are not supported.</li> <li>• Triggers and events do not support disaster recovery.</li> <li>• Accounts that have operation permissions on customized objects in the system database cannot be used for disaster recovery.</li> <li>• DDL operations cannot be executed on the active database 2.</li> </ul>

Type	Restrictions
Service database configuration	<ul style="list-style-type: none"> <li>● The binlog of the service database must be enabled and use the row-based format.</li> <li>● If the storage space is sufficient, store the service database binlog for as long as possible. The recommended retention period is seven days.</li> <li>● The service database username or password cannot be empty.</li> <li>● GTID must be enabled for the database.</li> <li>● The service database name must contain 1 to 64 characters, including only lowercase letters, digits, hyphens (-), and underscores (_).</li> <li>● The table name and view name in the service database cannot contain non-ASCII characters, or the following characters: '&lt;&gt;\'</li> <li>● If the <b>expire_logs_days</b> value of the database is set to <b>0</b>, the disaster recovery may fail.</li> </ul>
DR database configuration	<ul style="list-style-type: none"> <li>● The DR DB instance is running properly. If the DR DB instance is a primary/standby instance, the replication status must also be normal.</li> <li>● The DR DB instance must have sufficient storage space.</li> <li>● The major version of the active database 1 must be the same as that of the active database 2.</li> <li>● 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.</li> <li>● The binlog of the DR database must be enabled and use the row-based format.</li> <li>● GTID must be enabled for the DR database.</li> </ul>

Type	Restrictions
Precautions	<ul style="list-style-type: none"> <li>● 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 heavy 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 <a href="#">Common Exceptions in Real-Time Disaster</a>.</li> <li>● During the DR initialization, do not perform DDL operations on the source database. Otherwise, the DR task may be abnormal.</li> <li>● 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.             <ul style="list-style-type: none"> <li>– When the deletion operation is performed, data is deleted and DRS does not perform any operation.</li> <li>– When the insert operation is performed, DRS updates data with the latest inserted data.</li> <li>– When the update operation is performed, the original data has been updated and DRS directly insert the new data.</li> </ul> </li> <li>● 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.</li> <li>● 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.</li> <li>● The dual-active DR is different from the single-active DR. Therefore, no active/standby switchover is required.</li> <li>● 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.)</li> <li>● Ensure that the tables, columns, and rows are consistent in both the databases. (The table structures of both the active databases are consistent.)</li> <li>● 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.</li> </ul>

Type	Restrictions
	<ul style="list-style-type: none"> <li>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.</li> </ul>

## 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, specify the task name, description, and the DR instance details, and click **Next**.

**Figure 2-50** DR task information

The screenshot shows a form with three fields:
 

- Region:** A dropdown menu with a location pin icon.
- \* Task Name:** A text input field containing "DRS-7117" and a help icon (?).
- Description:** A text area with a help icon (?) and a character count "0/256" at the bottom right.

**Table 2-49** Task and recipient description

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

**Figure 2-51** DR instance information

**Disaster Recovery Instance Details**

The following information cannot be modified after you go to the next page.

\* DR Type:  Single-active  Dual-active ⓘ

\* Current Cloud RDS Instance Role:  Active 1  Active 2  
Active 2 indicates that the database is empty and waiting for initial data synchronization. If this role is not correctly selected, the precheck will fail. [Learn more about the role selection.](#)  
 In the initial phase, if the databases at both ends are empty, you can select either Active 1 or Active 2.

\* Service DB Engine:  MySQL  Cassandra  DDM  GaussDB(for MySQL) Primary/Standby Ed...

\* DR DB Engine:  GaussDB(for MySQL) Primary/Standby Ed...

\* Network Type:  ⓘ

I understand that an EIP will be automatically bound to the replication instance and released after the synchronization task is complete.

\* Instance Type:  single  primary/standby

\* DR DB Instance:  ⓘ [View DB Instance](#) [View Unselectable DB Instance](#)

\* Disaster Recovery Instance Subnet:  ⓘ [View Subnets](#)

\* AZ:  az1  az2  az3  az4  
Select the AZ where you want to create the DRS instance. Selecting the one housing the source or destination database for the instance will offer you a better performance.

---

\* Enterprise Project:  ⓘ [View Project Management](#) ⓘ

---

Tags: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) ⓘ

You can add 10 more tags.

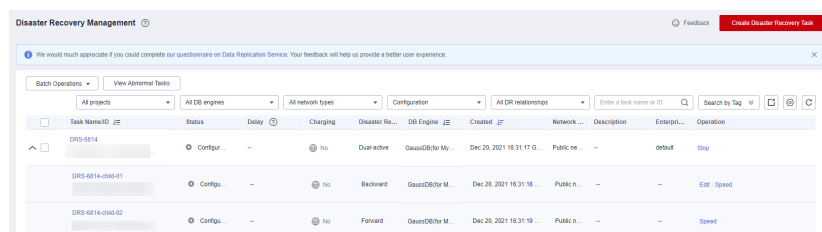
**Table 2-50** DR instance settings

Parameter	Description
DR Type	Select <b>Dual-active</b> . The DR type can be single-active or dual-active. If <b>Dual-active</b> is selected, two subtasks are created by default, a forward DR task and a backward DR task. <b>NOTE</b> 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 <b>Service Tickets &gt; Create Service Ticket</b> to submit a service ticket.
Current Cloud RDS Instance Role	Select <b>Active 1</b> or <b>Active 2</b> . This parameter specifies the role of the current RDS DB instance in the DR relationship and is available when <b>DR Type</b> is set to <b>Dual-active</b> . For details about how to choose active 1 and 2, see <a href="#">How Do I Select Active Database 1 and 2 for Dual-Active DR?</a> <ul style="list-style-type: none"> <li>Active 1: Initial data is available on the current cloud RDS when a task is created.</li> <li>Active 2: The RDS DB instance on the current cloud is empty when a task is created.</li> </ul> Active 2 is used as an example.
Service DB Engine	Select <b>GaussDB(for MySQL) Primary/Standby Edition</b> .
DR DB Engine	Select <b>GaussDB(for MySQL) Primary/Standby Edition</b> .

Parameter	Description
Network Type	The public network is used as an example. Available options: <b>VPN or Direct Connect</b> and <b>Public network</b> . By default, the value is <b>Public network</b> .
DR DB Instance	The GaussDB(for MySQL) primary/standby instance you created.
Disaster Recovery Instance Subnet	Select the subnet where the disaster recovery instance is located. You can also click <b>View Subnet</b> 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.
Enterprise Project	<ul style="list-style-type: none"> <li>If the DB instance has been associated with an enterprise project, select the target project from the <b>Enterprise Project</b> drop-down list.</li> <li>You can also go to the ProjectMan console to create a project. For details about how to create a project, see <i>ProjectMan User Guide</i>.</li> </ul>
Tags	<ul style="list-style-type: none"> <li>This setting is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 10 tags.</li> <li>After a task is created, you can view its tag details on the <b>Tags</b> tab. For details, see <a href="#">Tag Management</a>.</li> </ul>

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

**Figure 2-52** 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 2-53** Service database information

Source Database

Source Database Type:  Self-built on ECS  RDS DB Instance

IP Address or Domain Name:

Port:

Database Username:

Database Password:

SSL Connection:

If you want to enable SSL connection, ensure that SSL has been enabled on the source database, related parameters have been correctly configured, and an SSL certificate has been uploaded.

Encryption Certificate:

**Table 2-51** Service database settings

Parameter	Description
Source Database Type	By default, <b>Self-built on ECS</b> is selected. The source database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b> . After selecting <b>RDS DB instance</b> , 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 <b>RDS DB instance</b> 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 <b>Starting</b> , <b>Initializing</b> , <b>Disaster recovery in progress</b> , or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Update Password</b> next to the <b>Source Database Password</b> field. In the displayed dialog box, change the password. This action only updates DRS with the changed password.

Parameter	Description
SSL Connection	<p>SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>The maximum size of a single certificate file that can be uploaded is 500 KB.</li> <li>If the SSL certificate is not used, your data may be at risk.</li> </ul>
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 <b>RDS DB instance</b> .
DB Instance Name	The name of the service DB instance. This parameter is available only when the source database is an <b>RDS DB instance</b> .
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 2-54** DR database information

### Destination Database

DB Instance Name

XXXXXXXXXXXX


Database Username

root

Database Password

.....

Test Connection

 Test successful



**Table 2-52** DR database settings

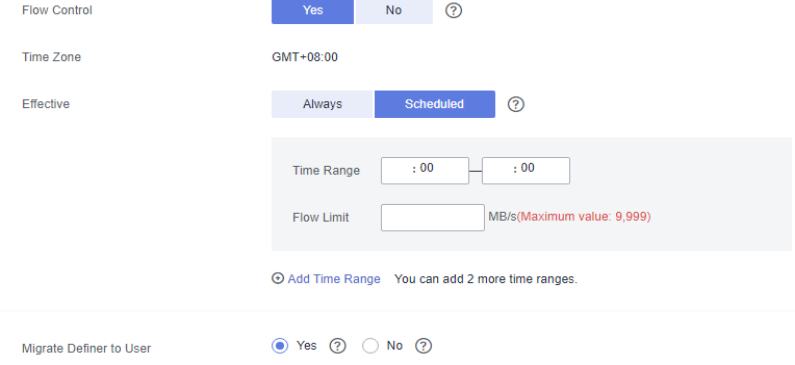
Parameter	Description
DB Instance Name	The GaussDB(for MySQL) primary/standby instance you selected when creating the DR. This parameter cannot be changed.
Database Username	The username for accessing the DR database.
Database Password	<p>The password for the database username. The password can be changed after a task is created.</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress, or Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Update Password</b> next to the <b>Destination Database Password</b> field. In the displayed dialog box, change the password. This action only updates DRS with the changed password.</p> <p>The database username and password are encrypted and stored in DRS, and will be cleared after the task is deleted.</p>

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

**Figure 2-55** DR settings



**Table 2-53** DR settings

Parameter	Description
Flow Control	<p>You can choose whether to control the flow.</p> <ul style="list-style-type: none"> <li> <b>Yes</b>                      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 <b>All day</b>. 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.                 </li> </ul> <p><b>Figure 2-56</b> Flow control</p>  <ul style="list-style-type: none"> <li> <b>No</b>                      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.                 </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Flow control mode takes effect during the initial DR phase only.</li> <li>You can also change the flow control mode when the task is in the <b>Configuration</b> state. On the <b>Basic Information</b> tab, in the <b>DR Information</b> area, click <b>Modify</b> next to <b>Flow Control</b>. In the dialog box that is displayed, change the flow control mode. The flow control mode cannot be changed for a task that is in <b>Starting</b> state.</li> </ul>

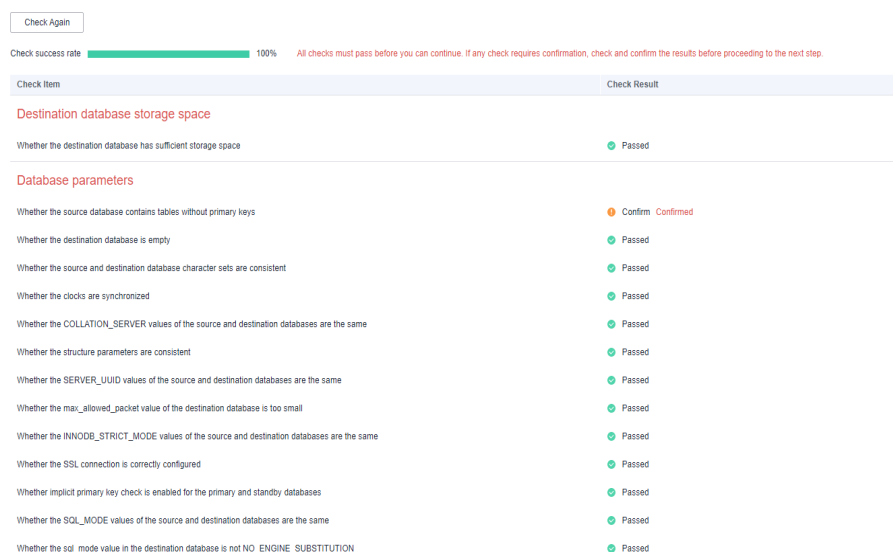
Parameter	Description
Migrate Definer to User	<ul style="list-style-type: none"> <li><b>Yes</b> The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see <a href="#">How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?</a></li> <li><b>No</b> 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.</li> </ul>

**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 [Checking Whether the Source Database Is Connected](#) in *Data Replication Service User Guide*.

**Figure 2-57** 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**, **Stop Abnormal Tasks After** and DR instance details. Then, click **Submit**.


**Figure 2-58** Task startup settings

**Table 2-54** Task and recipient description

Parameter	Description
Start Time	Set <b>Start Time</b> to <b>Start upon task creation</b> or <b>Start at a specified time</b> based on site requirements. <b>NOTE</b> 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 <a href="#">Simple Message Notification User Guide</a> .
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. <b>NOTE</b> <ul style="list-style-type: none"> <li>Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>

Parameter	Description
RTO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the RTO delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RPO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> <li>• 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.</li> </ul>
Stop Abnormal Tasks After	<p>Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is <b>14</b>.</p> <p><b>NOTE</b></p> <p>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.</p>

**Step 8** After the DR 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.

----End

# 3 Task Management

---

## 3.1 Creating a DR Task

### Scenario

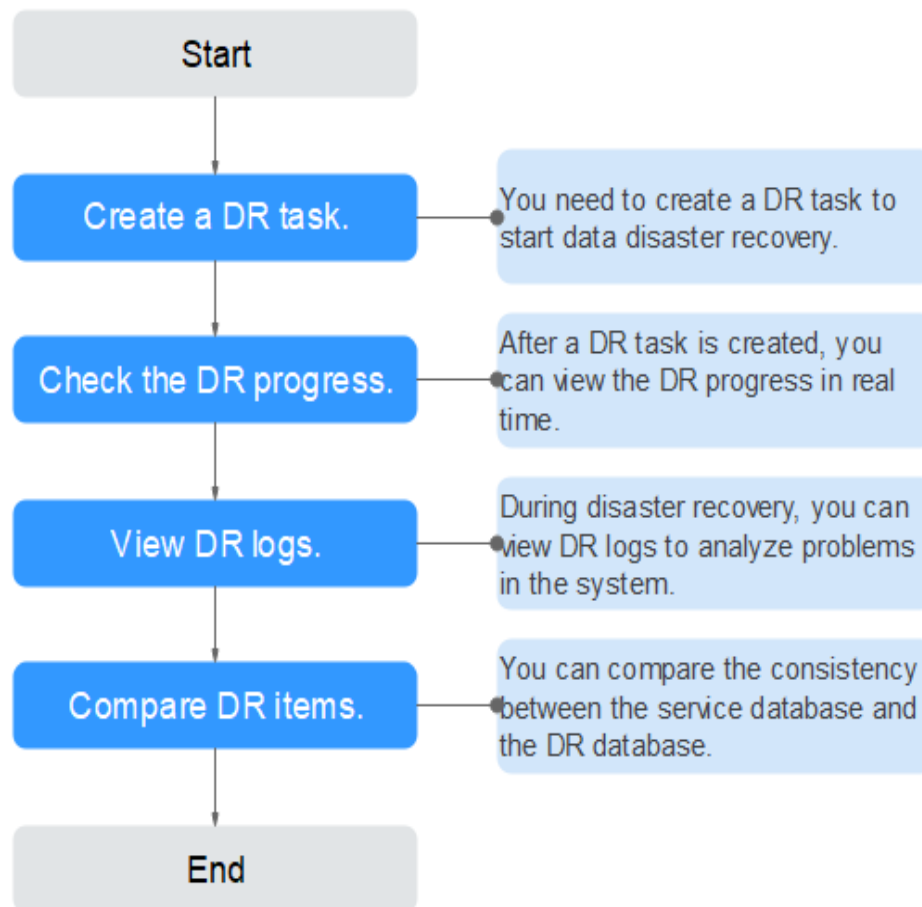
To prevent service unavailability caused by regional faults, DRS provides disaster recovery to ensure service continuity. If the region where the primary instance is located encounters a natural disaster and cannot be connected, you can switch the remote instance to the primary instance. To reconnect 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 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. 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, specify the task name, description, and the DR instance details, and click **Next**.

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



**Figure 3-3** DR instance information

**Disaster Recovery Instance Information**

The following information cannot be modified after you go to the next page.

\* DR Type: Single-active Dual-active ⓘ

\* Disaster Recovery Relationship: Current cloud as standby Current cloud as active

\* Service DB Engine: MySQL Cassandra DDM

\* DR DB Engine: MySQL GaussDB(for MySQL) Cassandra DDM

\* Network Type: Public network ⓘ

I acknowledge that an EIP will be automatically bound to the disaster recovery instance and released after the task is completed.

\* DR DB Instance: ... [View DB Instance](#) [View Unselectable DB Instance](#)

\* Disaster Recovery Instance Subnet: ... ⓘ [View Subnets](#)

\* Destination Database Access: Read-only

During the disaster recovery, the destination database becomes read-only to ensure the integrity and success rate of disaster recovery. After the disaster recovery is completed, it becomes readable and writable.

Tags: Tag key Tag value

You can add 10 more tags.

**Table 3-2** DR instance settings

Parameter	Description
DR Type	Select <b>Single-active</b> . The DR type can be single-active or dual-active. If <b>Dual-active</b> is selected, two subtasks are created by default, a forward DR task and a backward DR task. <b>NOTE</b> 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 <b>Service Tickets &gt; Create Service Ticket</b> to submit a service ticket.
Disaster Recovery Relationship	Select <b>Current cloud as standby</b> . This parameter is available only when you select <b>Single-active</b> . By default, <b>Current cloud as standby</b> is selected. You can also select <b>Current cloud as active</b> . <ul style="list-style-type: none"> <li><b>Current cloud as standby</b>: The DR database is on the current cloud.</li> <li><b>Current cloud as active</b>: The service database is on the current cloud.</li> </ul>
Service DB Engine	Select <b>MySQL</b> .
DR DB Engine	Select <b>MySQL</b> .
Network Type	The public network is used as an example. Available options: <b>VPN or Direct Connect</b> and <b>Public network</b> . By default, the value is <b>Public network</b> .

Parameter	Description
DR DB Instance	The RDS instance you created.
Disaster Recovery Instance Subnet	<p>Select the subnet where the disaster recovery instance is located. You can also click <b>View Subnet</b> to go to the network console to view the subnet where the instance resides.</p> <p>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.</p>
Destination Database Access	<p>Select <b>Read-only</b>. This parameter is available only when you select <b>Single-active</b>.</p> <p>During single-active disaster recovery, the DR database becomes read-only. To change the DR database to <b>Read/Write</b>, you can change the DR database (or destination database) to a service database by clicking <b>Promote Current Cloud</b> on the <b>Disaster Recovery Monitoring</b> tab. After the DR task is complete or deleted, you can query and read data to the DR database.</p> <p>When the external database functions as the DR database, the user with the superuser permission can set the database to read-only.</p> <p>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.</p>
Enterprise Project	<ul style="list-style-type: none"> <li>• If the DB instance has been associated with an enterprise project, select the target project from the <b>Enterprise Project</b> drop-down list.</li> <li>• You can also go to the ProjectMan console to create a project. For details about how to create a project, see <i>ProjectMan User Guide</i>.</li> </ul>
Tags	<ul style="list-style-type: none"> <li>• This setting is optional. Adding tags helps you better identify and manage your tasks. Each task can have up to 10 tags.</li> <li>• After a task is created, you can view its tag details on the <b>Tags</b> tab. For details, see <a href="#">Tag Management</a>.</li> </ul>

**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 3-4** Service database information

Source Database

Source Database Type  Self-built on ECS  RDS DB Instance

IP Address or Domain Name

Port

Database Username

Database Password

SSL Connection

If you want to enable SSL connection, ensure that SSL has been enabled on the source database, related parameters have been correctly configured, and an SSL certificate has been uploaded.

Encryption Certificate

**Table 3-3** Service database settings

Parameter	Description
Source Database Type	By default, <b>Self-built on ECS</b> is selected. The source database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b> . After selecting <b>RDS DB instance</b> , 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 <b>RDS DB instance</b> 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	<p>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:</p> <p>If the task is in the <b>Starting, Initializing, Disaster recovery in progress, or Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p>
SSL Connection	<p>SSL encrypts the connections between the source and destination databases. If SSL is enabled, upload the SSL CA root certificate.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- The maximum size of a single certificate file that can be uploaded is 500 KB.</li> <li>- If the SSL certificate is not used, your data may be at risk.</li> </ul>
Region	<p>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 <b>RDS DB instance</b>.</p>
DB Instance Name	<p>The name of the service DB instance. This parameter is available only when the source database is an <b>RDS DB instance</b>.</p>
Database Username	<p>The username for accessing the service database.</p>
Database Password	<p>The password for the service database username.</p>

 **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 3-5** DR database information

### Destination Database

DB Instance Name

Database Username

Database Password

✔ Test successful

**Table 3-4** 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 <b>Starting, Initializing, Disaster recovery in progress</b> , or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b> . 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.

- Select **Current cloud as active** for **Disaster Recovery Relationship** in [Step 2](#).

**Figure 3-6** Service database information

### Source Database

DB Instance Name

Database Username

Database Password

✔ Test successful

**Table 3-5** 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	<p>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:</p> <p>If the task is in the <b>Starting</b>, <b>Initializing</b>, <b>Disaster recovery in progress</b>, or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b>. In the displayed dialog box, change the password.</p> <p>The database username and password are encrypted and stored in the system and will be cleared after the task is deleted.</p>

**Figure 3-7** DR database information

**Destination Database**

Database Type: Self-built on ECS **RDS DB instance**

Region:

DB Instance Name:  [View DB Instance](#) [View Unselectable DB Instance](#)  
If used as a DR database, the instance becomes read-only.

Database Username:

Database Password:

This button is available only after the replication instance is created successfully.

**Table 3-6** DR database settings

Parameter	Description
Database Type	<p>By default, <b>Self-built on ECS</b> is selected.</p> <p>The destination database can be a <b>Self-built on ECS</b> or an <b>RDS DB instance</b>. If you select <b>RDS DB instance</b>, you need to select the region where the destination database is located.</p>

Parameter	Description
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.
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 <b>Starting, Initializing, Disaster recovery in progress</b> , or <b>Disaster recovery failed</b> status, in the <b>DR Information</b> area on the <b>Basic Information</b> tab, click <b>Modify Connection Details</b> . 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.  <b>NOTE</b> The maximum size of a single certificate file that can be uploaded is 500 KB.
Region	The region where the RDS DB instance is located. This parameter is available only when the source database is an RDS DB instance.
DB Instance Name	DR instance name. This parameter is available only when the source database is an RDS DB instance.  <b>NOTE</b> 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 3-8** DR settings

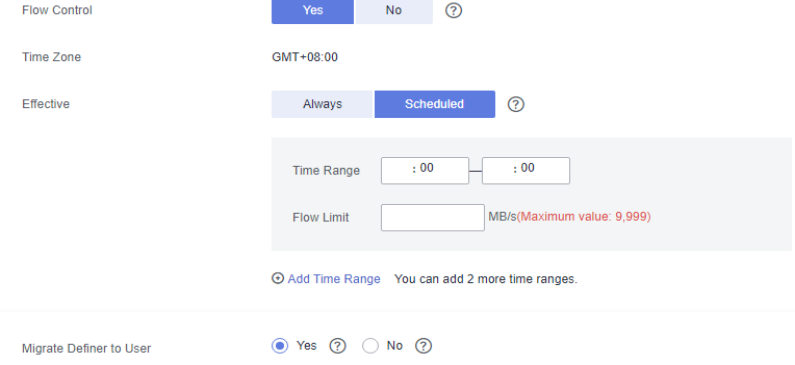


The image shows a configuration interface for DR settings. It contains two rows of settings, each enclosed in a dashed box. The first row is for 'Flow Control', with 'Yes' and 'No' buttons and a help icon. The 'No' button is selected. The second row is for 'Migrate Definer to User', with radio buttons for 'Yes' and 'No', and help icons. The 'Yes' radio button is selected.

Flow Control	<input type="button" value="Yes"/>	<input checked="" type="button" value="No"/>	<input type="button" value="?"/>
Migrate Definer to User	<input checked="" type="radio"/>	<input type="radio"/>	<input type="button" value="?"/>



**Table 3-7** DR settings

Parameter	Description
Flow Control	<p>You can choose whether to control the flow.</p> <ul style="list-style-type: none"> <li> <b>Yes</b>                      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 <b>All day</b>. 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.                 </li> </ul> <p><b>Figure 3-9</b> Flow control</p>  <ul style="list-style-type: none"> <li> <b>No</b>                      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.                 </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Flow control mode takes effect during the initial DR phase only.</li> <li>You can also change the flow control mode when the task is in the <b>Configuration</b> state. On the <b>Basic Information</b> tab, in the <b>DR Information</b> area, click <b>Modify</b> next to <b>Flow Control</b>. In the dialog box that is displayed, change the flow control mode. The flow control mode cannot be changed for a task that is in <b>Starting</b> state.</li> </ul>

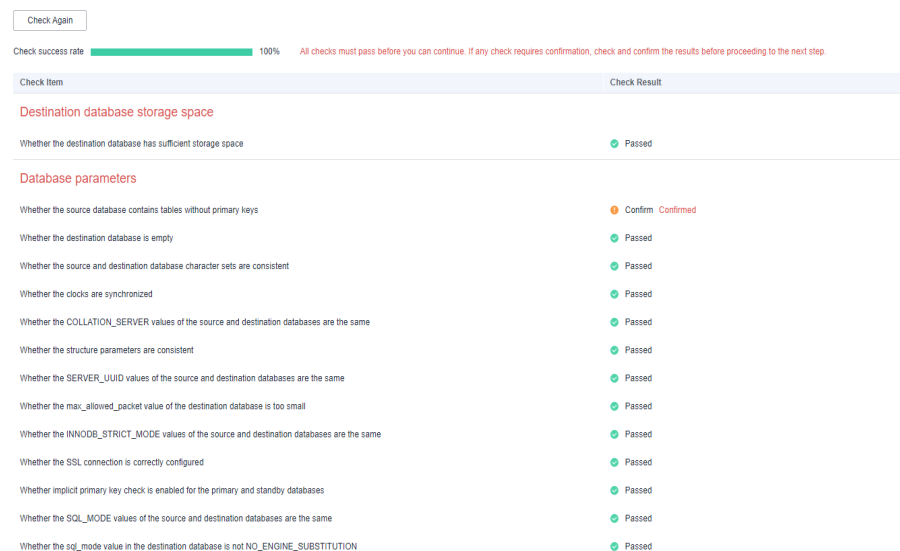
Parameter	Description
Migrate Definer to User	<ul style="list-style-type: none"> <li><b>Yes</b> The Definers of all source database objects will be migrated to the user. Other users do not have permissions for database objects unless these users are authorized. For details about authorization, see <a href="#">How Do I Maintain the Original Service User Permission System After Definer Is Forcibly Converted During MySQL Migration?</a></li> <li><b>No</b> 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.</li> </ul>

**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 [Checking Whether the Source Database Is Connected](#) in *Data Replication Service User Guide*.

**Figure 3-10** 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 3-11** Modifying common parameters

Parameter Name	Source Database Value	Destination Database Value	Result
character_set_server	utf8	utf8	Consistent
collation_server	utf8_general_ci	utf8_general_ci	Consistent
connect_timeout	10	10	Consistent
explicit_defaults_for_timestamp	OFF	ON	Inconsistent
innodb_flush_log_at_trx_commit	1	1	Consistent
innodb_lock_wait_timeout	50	50	Consistent
max_connections	800	800	Consistent
net_read_timeout	30	30	Consistent
net_write_timeout	60	60	Consistent
tx_isolation	REPEATABLE-READ	REPEATABLE-READ	Consistent

- 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 3-12** One-click modification

Parameter Name	Source Database Value	Destination Database Value	Change To	Allowed Destination Database Value	Result
binlog_cache_size	32768	32768	5	4096 - 1677216	Consistent
binlog_stmt_cache_size	32768	32768	8	4096 - 1677216	Consistent
bulk_insert_buffer_size	8388608	8388608		0 - 18446744073709551615	Consistent
innodb_buffer_pool_size	536870912	85526368	4	134217728 - 536870912	Inconsistent
long_query_time	1.000000	1.000000		0.01 - 3600	Consistent
read_buffer_size	262144	262144	64	4096 - 262144	Consistent
read_rnd_buffer_size	524288	524288	128	4096 - 524288	Consistent
sort_buffer_size	262144	262144		32768 - 18446744073709551615	Consistent
sync_binlog	1	1		0 - 4294967295	Consistent

**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 3-13 One-click modification

Parameter Type: Common parameters Performance parameters

Select the destination database parameters you want to change. Some changes take effect only after you restart the destination database. You are advised to restart the destination database before or after the migration.

Use Source Database Value Save Change

Parameter Name	Source Database Value	Destination Database Value	Change To	Allowed Destination Database Va...	Result
<input type="checkbox"/> linklog_cache_size	32768	32768	8	+4096 ~ 32768	4096-16777216 <span>Consistent</span>
<input type="checkbox"/> linklog_stream_cache_size	32768	32768	8	+4096 ~ 32768	4096-16777216 <span>Consistent</span>
<input type="checkbox"/> bulk_insert_buffer_size	8388608	8388608			0-18446744073709551615 <span>Consistent</span>
<input checked="" type="checkbox"/> innodb_buffer_pool_size	536879512	805206336	4	-134317728 ~ 536879512	536879512-117946518 <span>Inconsistent</span>
<input type="checkbox"/> long_query_time	1.000000	1.000000			0.01-3000 <span>Consistent</span>
<input type="checkbox"/> read_buffer_size	262144	262144	64	+4096 ~ 262144	8192-2147483647 <span>Consistent</span>
<input type="checkbox"/> read_rnd_buffer_size	524288	524288	128	+4096 ~ 524288	1-2147483647 <span>Consistent</span>
<input type="checkbox"/> sort_buffer_size	262144	262144			32768-18446744073709551615 <span>Consistent</span>
<input type="checkbox"/> sync_binlog	1	1			0-4294967295 <span>Consistent</span>

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 3-14 Task startup settings

Start Time Start upon task creation Start at a specified time (?)

---

Send Notifications  (?)

\* SMN Topic  (?)

Synchronization Delay Threshold(s)  (?)

RTO Synchronization Delay Threshold(s)  (?)

RPO Synchronization Delay Threshold(s)  (?)


\* Stop Abnormal Tasks After  (?) *Abnormal tasks run longer than the period you set (unit: day) will automatically stop.*

**Table 3-8** Task and recipient description

Parameter	Description
Start Time	<p>Set <b>Start Time</b> to <b>Start upon task creation</b> or <b>Start at a specified time</b> based on site requirements.</p> <p><b>NOTE</b> 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.</p>
Send Notifications	<p>SMN topic. This parameter is optional. If an exception occurs during disaster recovery, the system will send a notification to the specified recipients.</p>
SMN Topic	<p>This parameter is available only after you enable Send Notifications and create a topic on the SMN console and add a subscriber.</p> <p>For details, see <a href="#">Simple Message Notification User Guide</a>.</p>
Synchronization Delay Threshold	<p>During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database.</p> <p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RTO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the RTO delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>

Parameter	Description
RPO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> <li>• 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.</li> </ul>
Stop Abnormal Tasks After	<p>Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is <b>14</b>.</p> <p><b>NOTE</b></p> <p>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.</p>

**Step 8** After the DR 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.

----End

## 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.

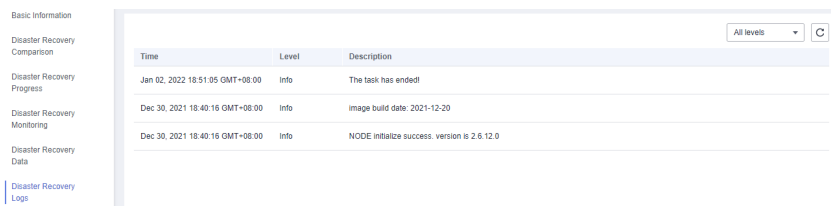
### Prerequisites

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 3-15** Viewing DR Logs



----End

### 3.4 Comparing DR Items

You can check the data consistency by comparing DR items in the service and DR databases. DR supports object-level and data-level comparisons.

- Object-level comparison: compares databases, events, indexes, tables, views, stored procedures, functions, and triggers.
- Data-level comparison: compares rows and values of tables. To ensure that the comparison results are valid, compare data during off-peak hours by select **Start at a specified time** or compare data that is rarely accessed or modified.
- Account comparison: compares the account names and permissions of the source and destination databases.

**NOTE**

- If you modify data in the DR database, the data comparison results may be inaccurate.
- 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 source database is a relational database, the row comparison duration is 60 minutes. If the source database is a non-relational database, the row comparison duration is 30 minutes.

**Table 3-9** Supported comparison mode

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




DR Direction	Data Flow	Object-level Comparison	Row Comparison	Value Comparison	Account-level Comparison
Current cloud as standby	DDM -> DDM	Yes	Yes	No	No
Current cloud as active	DDM -> DDM	Yes	Yes	No	No
Current cloud as standby	GaussDB(for MySQL) primary/standby -> GaussDB(for MySQL) primary/standby	Yes	Yes	Yes	Yes
Current cloud as active	GaussDB(for MySQL) primary/standby -> GaussDB(for MySQL) primary/standby	Yes	Yes	Yes	Yes
Dual-Active DR	MySQL->MySQL	Yes	Yes	Yes	Yes
Dual-Active DR	GaussDB(for MySQL) primary/standby -> GaussDB(for MySQL) primary/standby	Yes	Yes	Yes	Yes

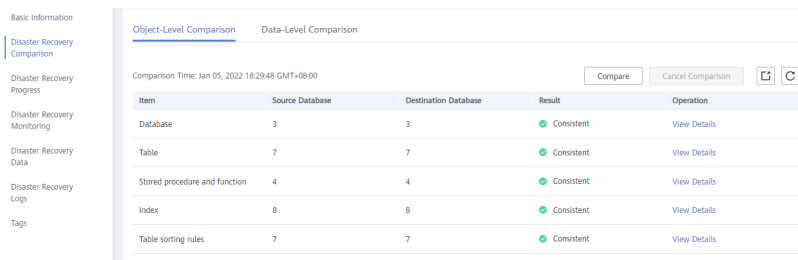
## Prerequisites

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 **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.

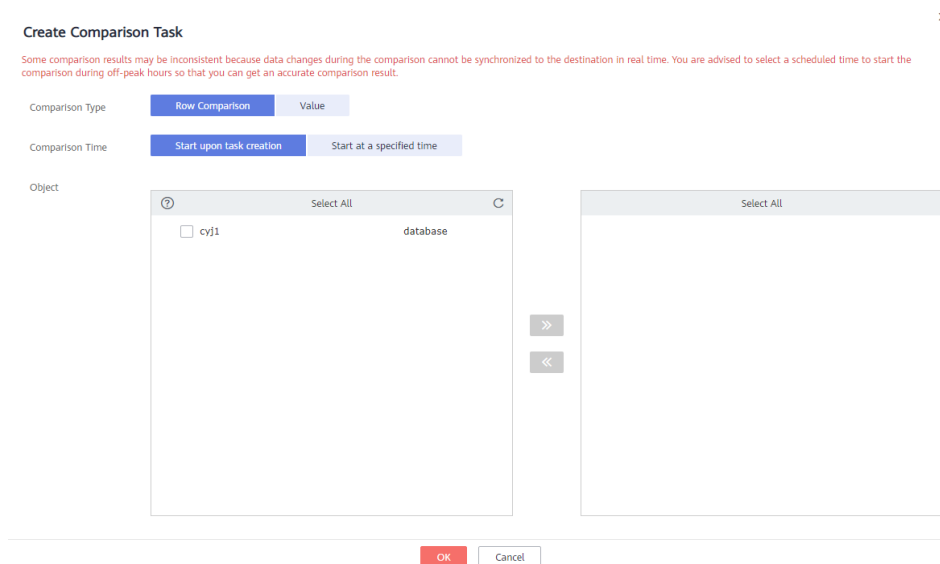
**Figure 3-16** Comparing objects



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

- 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 **Compute Method**, **Comparison Type**, **Comparison Time**, and **Object**. Then, click **OK**.

**Figure 3-17** 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

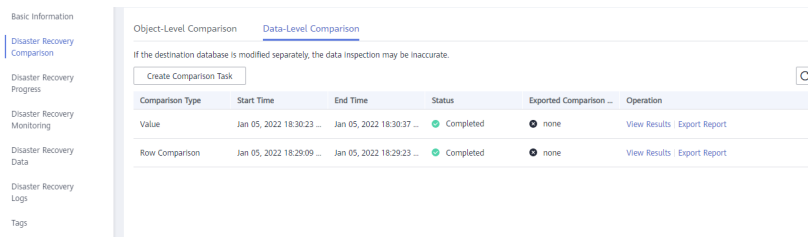
Currently, only MySQL and GaussDB(for MySQL) support the comparison mode.

- **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

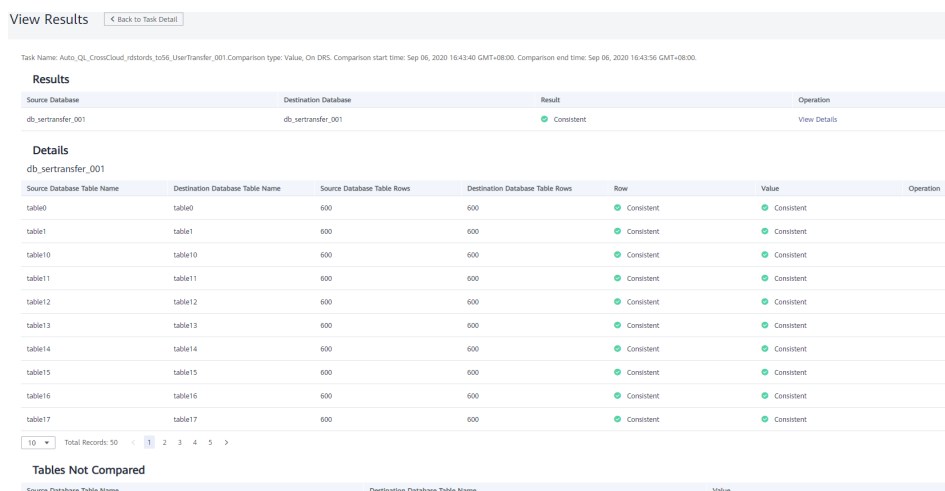
- Data-level comparison cannot be performed for tasks in initialization.
3. After the comparison creation task is submitted, the **Data-Level Comparison** tab is displayed. Click to refresh the list and view the comparison result of the specified comparison type.

**Figure 3-18** 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 3-19** Viewing comparison details



NOTE

You can also view comparison details of canceled comparison tasks.

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

**Figure 3-20** Account-level comparison

Source Database Account Attribute	Source Database Account Name	Destination Database Account Attribute	Destination Database Account Name	Migration Comparison Time	Result
CREATEDB.CREATEROLE.NONHERITPASSW...	quser1	CREATEDB.CREATEROLE.NONHERITPASSW...	quser1	Aug 19, 2021 11:39:28 GMT+08:00	Consistent

**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.

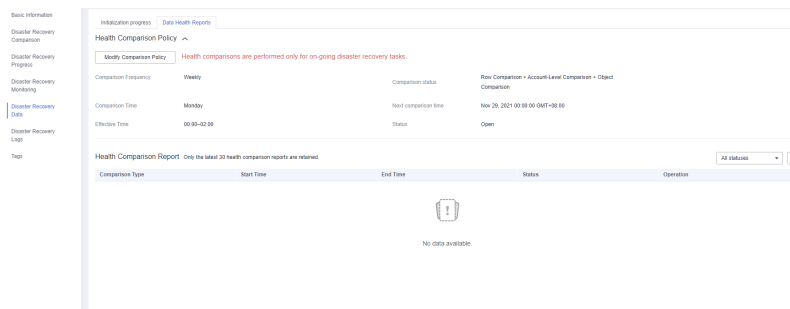
**Step 2** On the **Basic Information** tab, click the **Disaster Recovery Data** tab.

- 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**

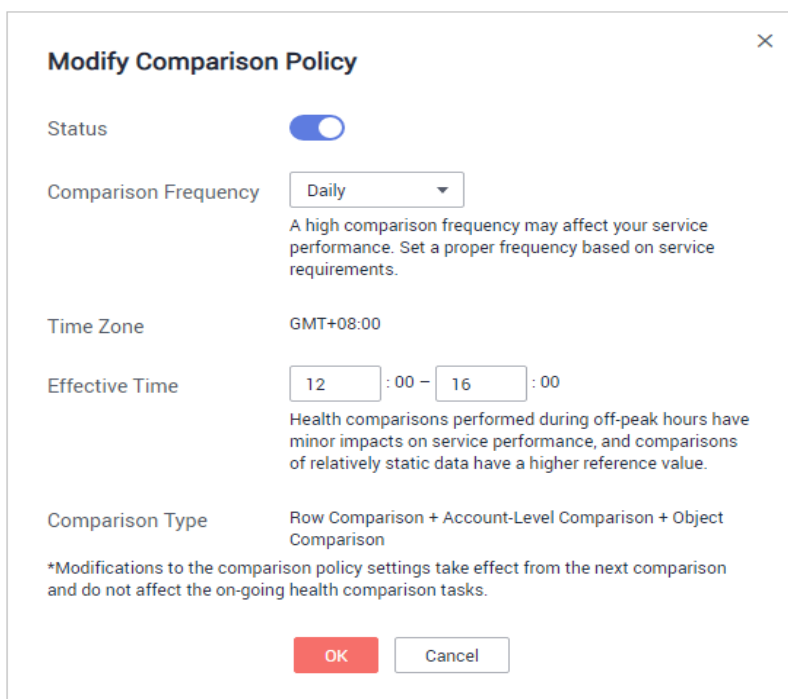
- Data comparison is performed only for disaster recovery tasks.
- Only the latest 30 health comparison reports are retained.
- The periodical health report helps you learn the data consistency between the primary and standby instances. To avoid performance loss caused by long-term comparison of the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

**Figure 3-21** 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 3-22** 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 Editing Subscription 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 3-10** Real-time DR task information

Task Information	Description
Task Name	The task name consists of 4 to 50 characters, starts with a letter, and can contain only letters (case-insensitive), 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 <a href="#">Simple Message Notification User Guide</a> .
Synchronization delay threshold	The delay ranges from 0s to 3600s. <b>NOTE</b> 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.

- 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**.

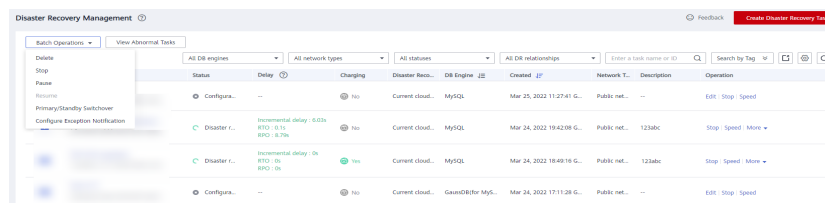
**Step 3** View the change result on the **Basic Information** tab.

----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 3-23** Batch Operations

The screenshot shows the 'Disaster Recovery Management' console. It features a table with columns for Status, Delay, Charging, Disaster Recs., DR Engine, Created, Network T., Description, and Operation. The table contains several rows representing different tasks, including configurations and disaster recovery tasks with various statuses like 'Incremental delay - 0/2h' and 'Incremental delay - 0h'.

Status	Delay	Charging	Disaster Recs.	DR Engine	Created	Network T.	Description	Operation
Configura...	...	No	Current cloud...	MySQL	Mar 25, 2022 11:27:41 G...	Public net...	...	Edit Stop Speed
Disaster r...	Incremental delay - 0/2h RTO : 0.1h RPO : 0.2h	No	Current cloud...	MySQL	Mar 24, 2022 19:42:08 G...	Public net...	123abc	Stop Speed More
Disaster r...	Incremental delay - 0h RTO : 0h RPO : 0h	Yes	Current cloud...	MySQL	Mar 24, 2022 18:49:16 G...	Public net...	123abc	Stop Speed More
Configura...	...	No	Current cloud...	GaussDB for MyS...	Mar 24, 2022 17:11:28 G...	Public net...	...	Edit Stop Speed

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

----End

### 3.5.3 Editing a DR Task

This section describes how to edit configuration information of a DR task, including information about the service and DR databases. 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**.

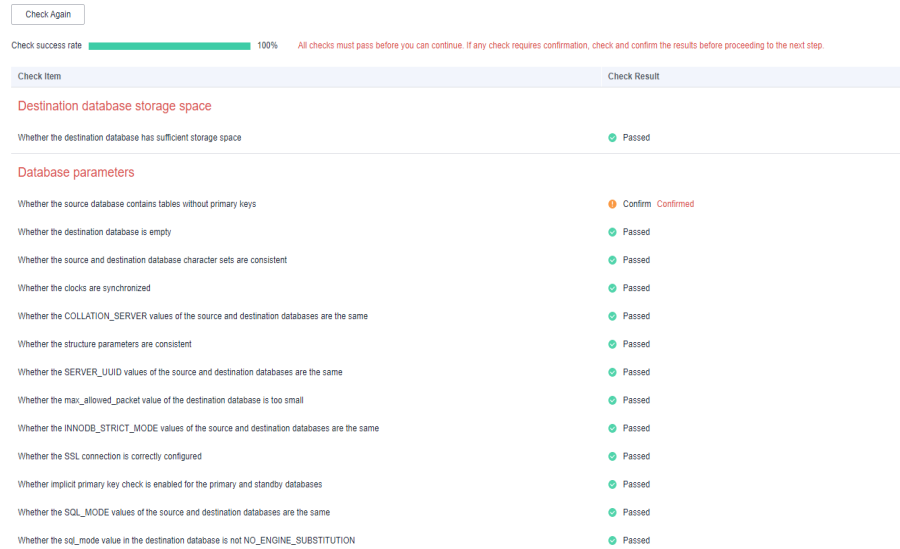
**Step 3** On the **Check Task** page, check the DR task.

- 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 [Checking Whether the Source Database Is Connected](#) in *Data Replication Service User Guide*.



Figure 3-24 Pre-check



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

**NOTE**

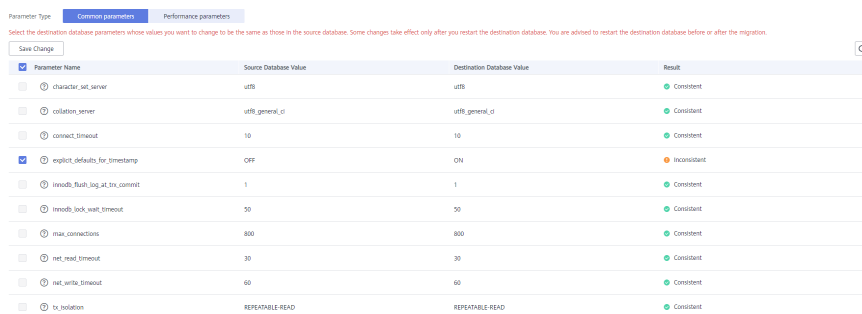
You can proceed to the next step only when all checks are successful. If there are any items that require confirmation, view and confirm the details first before proceeding to the next step.

**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 3-25 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 3-26** One-click modification

Parameter Name	Source Database Value	Destination Database Value	Change To	Allowed Destination Database Va...	Result	
<input type="checkbox"/> linklog_cache_size	32768	32768	8	+4096 = 32768	4096-1677216	Consistent
<input type="checkbox"/> linklog_stmt_cache_size	32768	32768	8	+4096 = 32768	4096-1677216	Consistent
<input type="checkbox"/> link_insert_buffer_size	838806	838806			0-1844674672739551615	Consistent
<input checked="" type="checkbox"/> innodb_buffer_pool_size	536870912	805306368	4	+134217728 = 536870912	536870912-1717969318	Inconsistent
<input type="checkbox"/> long_query_time	1.000000	1.000000			0.01-3000	Consistent
<input type="checkbox"/> read_buffer_size	262144	262144	64	+4096 = 262144	8192-2147479952	Consistent
<input type="checkbox"/> read_rnd_buffer_size	524288	524288	128	+4096 = 524288	1-2147483647	Consistent
<input type="checkbox"/> sort_buffer_size	262144	262144			32768-1844674672739551615	Consistent
<input type="checkbox"/> sync_binlog	1	1			0-4264697295	Consistent

**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 3-27** One-click modification

Parameter Name	Source Database Value	Destination Database Value	Change To	Allowed Destination Database Va...	Result	
<input type="checkbox"/> linklog_cache_size	32768	32768	8	+4096 = 32768	4096-1677216	Consistent
<input type="checkbox"/> linklog_stmt_cache_size	32768	32768	8	+4096 = 32768	4096-1677216	Consistent
<input type="checkbox"/> link_insert_buffer_size	838806	838806			0-1844674672739551615	Consistent
<input checked="" type="checkbox"/> innodb_buffer_pool_size	536870912	805306368	4	+134217728 = 536870912	536870912-1717969318	Inconsistent
<input type="checkbox"/> long_query_time	1.000000	1.000000			0.01-3000	Consistent
<input type="checkbox"/> read_buffer_size	262144	262144	64	+4096 = 262144	8192-2147479952	Consistent
<input type="checkbox"/> read_rnd_buffer_size	524288	524288	128	+4096 = 524288	1-2147483647	Consistent
<input type="checkbox"/> sort_buffer_size	262144	262144			32768-1844674672739551615	Consistent
<input type="checkbox"/> sync_binlog	1	1			0-4264697295	Consistent

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 3-28** Task startup settings

**Table 3-11** Task and recipient description

Parameter	Description
Start Time	Set <b>Start Time</b> to <b>Start upon task creation</b> or <b>Start at a specified time</b> based on site requirements. <b>NOTE</b> 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 <a href="#">Simple Message Notification User Guide</a> .

Parameter	Description
Synchronization Delay Threshold	<p>During disaster recovery, a synchronization delay indicates a time difference (in seconds) of synchronization between the service and DR database.</p> <p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RTO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the RTO delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> </ul>
RPO Synchronization Delay Threshold	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Before setting the delay threshold, enable <b>Send Notification</b>.</li> <li>• If the delay threshold is set to 0, no notifications will be sent to the recipient.</li> <li>• 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.</li> </ul>
Stop Abnormal Tasks After	<p>Number of days after which an abnormal task is automatically stopped. The value must range from 14 to 100. The default value is <b>14</b>.</p> <p><b>NOTE</b></p> <p>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.</p>

**Step 6** After the DR 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.

----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

## 3.5.4 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.
- If a snapshot-based DR task fails, it cannot be resumed.

## Prerequisites

- You have logged in to the DRS console.
- A failed DR task exists.

## 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 left corner.

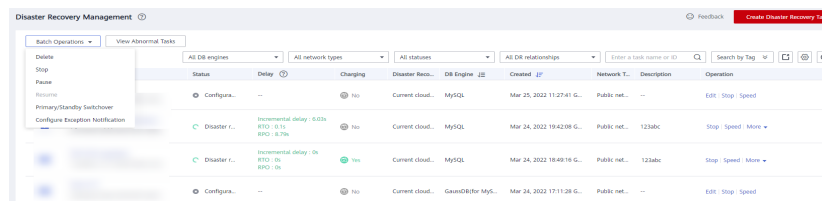
----End

## 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 3-29** Batch Operations



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

----End

## 3.5.5 Pausing a DR Task

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

### 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. It is recommended that the pause duration be less than or equal to 24 hours.
- You can use the resumable transfer function to continue the DR task.

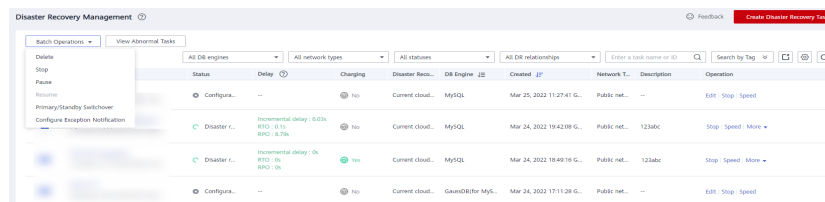
----End

## 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 3-30** Batch Operations



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

----End

### 3.5.6 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 reset.

### 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**.

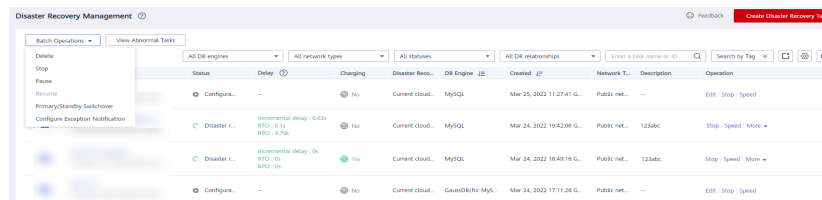
----End

## Stopping Tasks

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

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

**Figure 3-31** Batch Operations



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

----End

## 3.5.7 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.

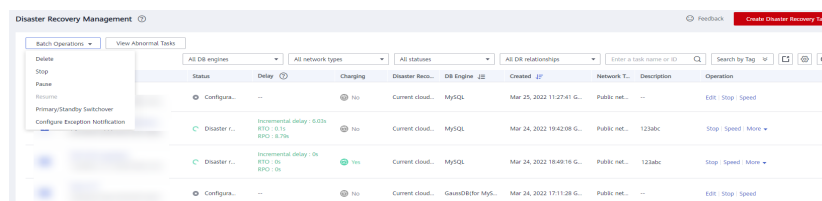
----End

### 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 3-32** 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 link 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.

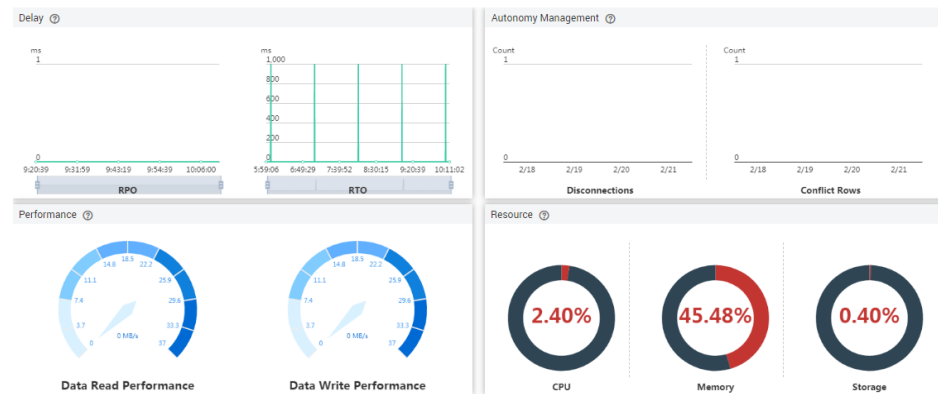
### Procedure

**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 3-33 DR monitoring



----End

### 3.5.9 Performing a Primary/Standby Switchover

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

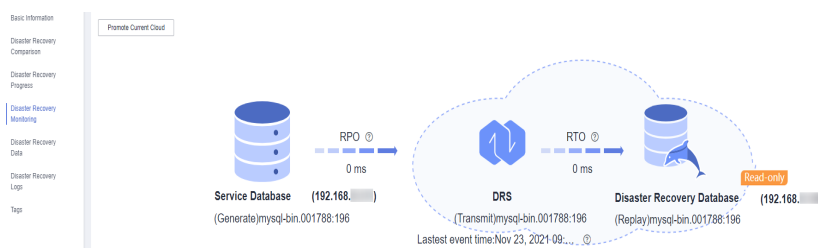
- You have logged in to the DRS console.
- You have created a DR task.

#### 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/secondary 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.

Figure 3-34 DR monitoring

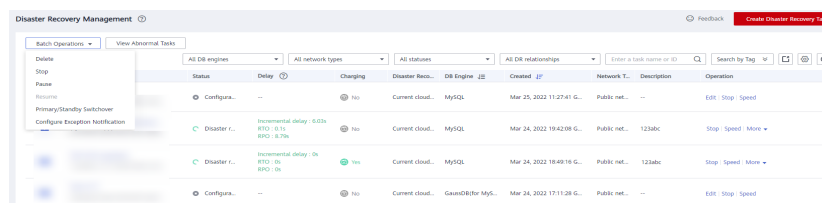


----End

## Performing Primary/Standby Switchover in Batches

- Step 1** On the **Disaster Recovery Management** page, select the tasks.
- Step 2** Click **Batch Operation** in the upper left corner and select **Primary/Standby Switchover**.

Figure 3-35 Batch Operations



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

----End

## 3.5.10 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) primary/standby
- DDM->DDM
- GaussDB(for MySQL) primary/standby -> GaussDB(for MySQL) primary/standby

### 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 **DR Information** area on the **Basic Information** tab, click **Modify** next to the **Flow Control** field.

**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

### 3.5.11 Task Statuses

DR statuses indicate different DR phases.

**Table 3-12** lists DR task statuses and descriptions.

**Table 3-12** 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 created.
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**

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 10 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** On the **Basic Information** tab, click the **Tags** tab.
- Step 3** On the **Tags** tab, click **Add Tag**. In the displayed dialog box, enter a tag key and value, and click **OK**.

**Add Tag** ×

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) ↻

To add a tag, enter a tag key and a tag value below.

Enter a tag key  Enter a tag value

10 tags available for addition.

- 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 cannot be empty and must be unique. It cannot start or end with a space and can contain 1 to 128 characters, including letters, digits, spaces, and special characters \_:=+.-@
- 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** After a tag has been added, you can view and manage it 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** On the **Basic Information** tab, click the **Tags** tab.

**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** On the **Basic Information** tab, click the **Tags** tab.

**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 Interconnecting with CTS

## 5.1 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 5-1** 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

## 5.2 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

# 6 Interconnecting with Cloud Eye

---

## 6.1 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 6-1](#) lists the DRS performance metrics.

**Table 6-1** DRS metrics

Metric ID	Metric 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	$\geq 0$ 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	$\geq 0$ 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).	$\geq 0$ bytes/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute

Metric ID	Metric 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	Metric 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_rate	DDL TPS	Number of DDLs written to the destination database per second.	≥ 0 transaction/s	Monitored object: ECS Monitored instance type: replication, synchronization, and DR instances	1 minute
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

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
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
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

## Dimensions

Key	Value
instance_id	DRS instance ID

## 6.2 Configuring Alarm Rules

### Scenarios

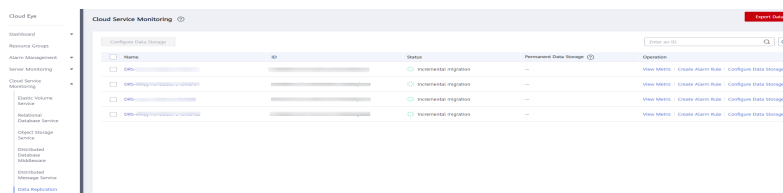
You can configure DRS alarm rules to customize the monitored objects and notification policies and learn the DRS running status in a timely manner.

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 6-1** 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 6-2** Configuring alarm information

\* Name: alarm-2elf

Description: [Empty text box]

\* Enterprise Project: default [Create Enterprise Project](#)

---

\* Resource Type: Data Replication Service

\* Dimension: DRS

\* Monitoring Scope: Specific resources

\* Monitored Object: DRS

---

\* Method: **Use template** [Create manually](#)

\* Template: alarmTemplate-6me2 [Create Custom Template](#)

Alarm Policy	Alarm Severity	Operation
Trigger an alarm if CPU Usage Raw data >= 23% for 3 consecutive periods. Trigger an alarm one day again if the alarm persists.	Major	Delete

---

Alarm Notification:

\* Notification Recipient: **Notification group** [Topic subscription](#)

- 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

## 6.3 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.

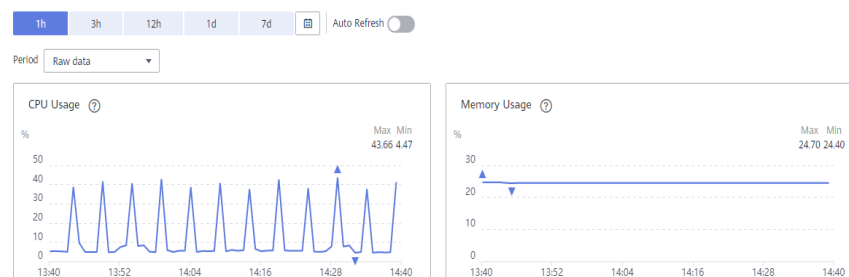
**Step 5** On the displayed page, click **View Metric** in the upper right corner of the page to go to the Cloud Eye console.

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 30 days.

**Figure 6-3** Viewing monitoring metrics



----End

---

# A Change History

---

Released On	Description
2022-09-30	This issue is the first official release.