Data Replication Service

Preparations

Issue	01
Date	2023-05-30

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://e.huawei.com

Security Declaration

Product Life Cycle

Huawei's regulations on product life cycle are subject to the Product End of Life Policy. For details about the policy, see the following website:https://support.huawei.com/ecolumnsweb/en/warranty-policy

Vulnerability

Huawei's regulations on product vulnerability management are subject to "Vul. Response Process". For details about the policy, see the following website:https://www.huawei.com/en/psirt/vul-response-process For enterprise customers who need to obtain vulnerability information, visit:https://securitybulletin.huawei.com/enterprise/en/security-advisory

Preconfigured Digital Certificate

Huawei has released the Huawei Preset Digital Certificate Disclaimer for the preconfigured digital certificates delivered with devices. For details about the disclaimer, visit the following website:https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789

Life Cycle of Product Documentation

Huawei released the Huawei Product Documentation Lifecycle Policy for after-sales customer documentation. For details about this policy, see the website of Huawei's official website:https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761

Contents

1 Overview

Before creating a DRS task, make preparations given in the following table to meet the environment requirements.

Table 1-1 Preparations

Item	Description	Reference
Account	Prepare a Huawei account, create a user, and grant permissions to the user to use DRS.	For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services**. Register an account by referring to **Permissions Management**.
Database	Prepare the source and destination databases with required account permissions. **NOTE** • You are advised to create an independent database account for DRS task connection to prevent task failures caused by account modification. • After changing the account passwords for the source and destination databases, modify the connection information in the DRS task as soon as possible to prevent automatic retry after a task failure. Automatic retry will lock the database accounts.	Different data flow types require different databases and permissions. For details, refer to the following sections: **Supported Databases** **Real-Time Migration Overview** **Backup Migration Overview** **Real-Time Synchronization Overview** **Notes on Data Subscription** **Real-Time DR Overview**
Network	The source database is deployed on a local host.	For details, see **From On-premises Databases to Huawei Cloud**.

Item	Description	Reference
	The source is other cloud databases.	For details, see **From Other Cloud Databases to Huawei Cloud**.
	The source is a Huawei Cloud database.	For details, see **From Huawei Cloud to Huawei Cloud**.
	The source is an ECS database.	For details, see **From ECS-Hosted Databases on Huawei Cloud to Huawei Cloud**.

2 Registering a Huawei ID and Enabling Huawei Cloud Services

Before using Huawei Cloud services, you need to register a Huawei ID and enable Huawei Cloud services. With this account, you can use all services on Huawei Cloud and only need to pay for the services you use.

Log in to the Huawei Cloud official website and register an account by referring to **Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services**.

After the registration, you are automatically logged in to Huawei Cloud.

3 Permissions Management

3.1 Creating a User and Granting Permissions

This section describes how to use **Enterprise Management** or **IAM** to achieve fine-grained permissions management for your DRS tasks.

- For details about how to use Enterprise Management, see **Project Management**.
- With IAM, you can:
  - Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to DRS resources.
  - Grant only the permissions required for users to perform a specific task.
  - Entrust an account or cloud service to perform professional and efficient O&M on your DRS resources.

If your account does not require individual IAM users, skip this chapter.

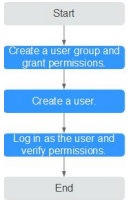
This section describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

Learn about the permissions (see **Permissions Management**) supported by DRS and choose policies or roles according to your requirements. For the system policies of other services, see **Permissions Policies**.

Process Flow

Figure 3-1 Process for granting DRS permissions



1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and assign the **DRS Administrator** policy to the group.

2. **Create a user.**

   Create a user on the IAM console and add the user to the group created in .

3. **Log in** and verify permissions.

   Log in to the management console using the newly created user, and verify that the user only has read permissions for DRS.

   Go to the DRS console, click **Create Migration Task** in the upper right corner to create a migration task. If a migration task (assume that there is only the **DRS Administrator** permission) is created, the **DRS Administrator** policy has taken effect.

3.2 Creating a Custom Policy

Custom policies can be created to supplement the system-defined policies of DRS.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a policy in JSON format or edit the JSON strings of an existing policy.

For details about how to create a custom policy, see **Creating a Custom Policy**. The following describes examples of common DRS custom policies.

Example Custom Policies

- Example 1: Allowing users to create DRS instances

```
{
    "Version": "1.1",
    "Statement": [{
                "Action": ["drs:instance:create"],
        "Effect": "Allow"
    }]
}
```

- Example 2: Denying DRS instance deletion

  A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **DRS FullAccess** policy to a user but you want to prevent the user from deleting DRS instances. Create a custom policy for denying DRS instance deletion, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on DRS instances except deleting DRS instances. The following is an example of a deny policy:

```
{
    "Version": "1.1",
    "Statement": [{
        "Action": ["drs:instance:delete"],
```

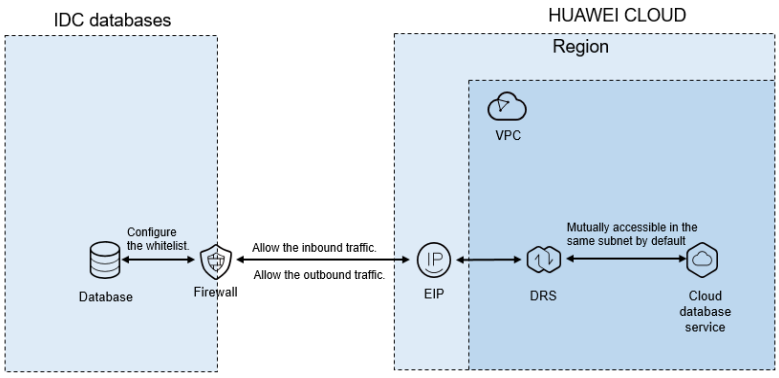
```
        "Effect": "Deny"
    }]
}
```

4 From On-premises Databases to Huawei Cloud

4.1 Accessing Huawei Cloud over a Public Network

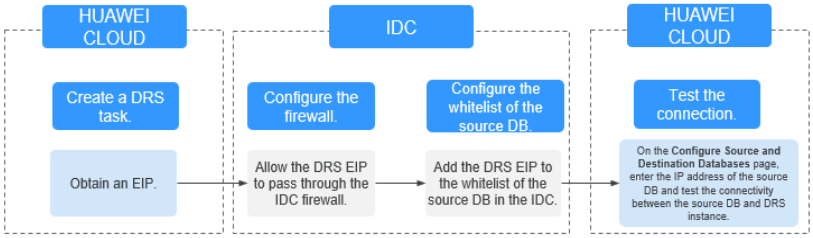
Figure 4-1 shows how to use DRS to migrate data from on-premises databases to Huawei Cloud databases over a public network.

Figure 4-1 Network diagram



To access databases in the on-premises data center, configure the source database to accept connections from the EIP of the DRS instance. Figure 4-2 shows the process.

Figure 4-2 Flowchart

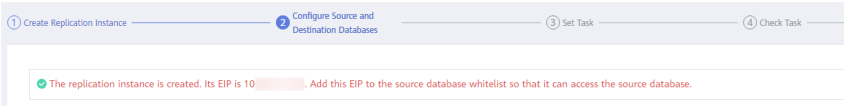


Network Configurations

Step 1 Create a DRS task and obtain the EIP of the DRS instance.

The IP address displayed on the **Configure Source and Destination Databases** page is the EIP of the DRS instance.

Figure 4-3 EIP of the DRS instance



Step 2 Configure the firewall of the local data center.

The firewall of the local data center must allow access from the EIP of the DRS instance so that the DRS instance can access the on-premises databases.

Inbound access is the access from the EIP of the DRS instance to the database listening port.

Outbound access is the transfer of data from the database listening port to the EIP of the DRS instance.

Step 3 Configure the IP address whitelist for the on-premises database.

Add the EIP of the DRS instance to the whitelist of the on-premises database to allow the access from the DRS instance.

The method for configuring the whitelist depends on the database type. For details, see the official documents of each database.

Step 4 Test the connection.

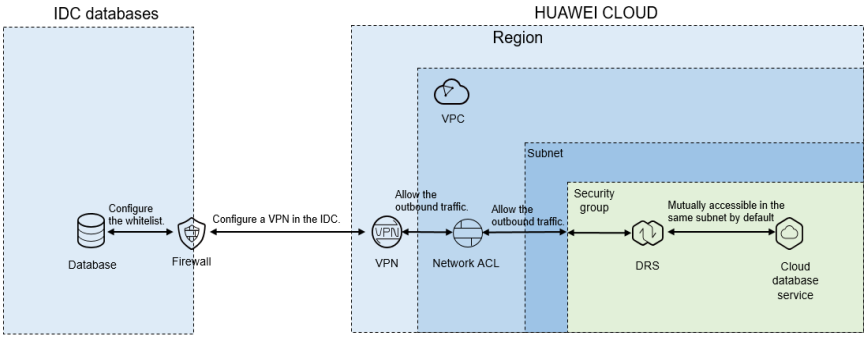
Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the on-premises database and then click **Test Connection** to check whether the connection is successful.

----End

4.2 Accessing Huawei Cloud over a VPN

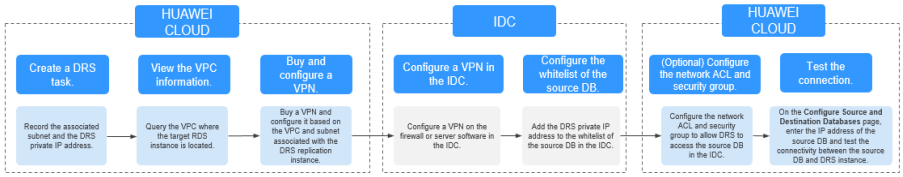
Figure 4-4 shows how to use DRS to migrate data from on-premises databases to Huawei Cloud databases using a VPN.

Figure 4-4 Network diagram



To access a database in the local data center using a VPN, purchase the VPN service on Huawei Cloud and configure the VPN to connect to the VPC that contains the DRS instance. In addition, you need to configure the VPN device on the firewall or host in the local data center. **Figure 4-5** shows the operation process.

Figure 4-5 Flowchart

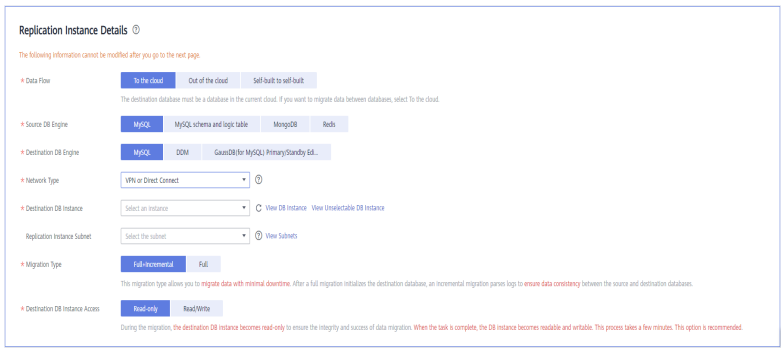


Network Configurations

Step 1 Create a DRS instance and obtain the subnet and private IP address of the DRS instance.

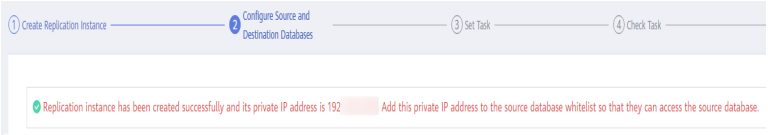
By default, the DRS instance is in the same subnet as the destination database.

Figure 4-6 Replication instance information



After the DRS replication instance is created, the private IP address of the DRS replication instance is displayed.

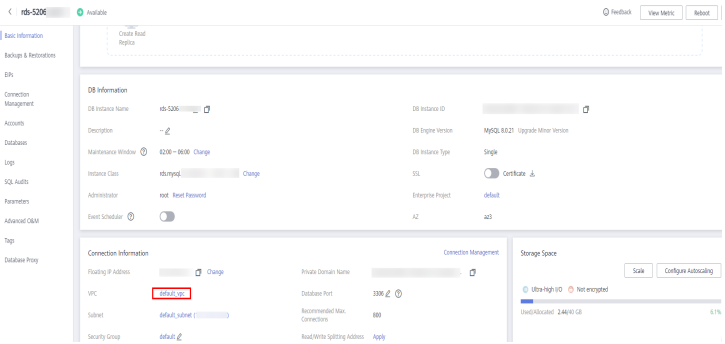
Figure 4-7 Private IP address of the DRS instance



Step 2 Query the name of the VPC to which the DRS instance belongs.

By default, the DRS replication instance and the destination RDS instance are created in the same VPC. You can log in to the destination RDS instance to view information about the VPC where the replication instance is located.

Figure 4-8 Destination database information



Step 3 Purchase a VPN and configure the VPN gateway and connection.

For details, see **Getting Started with Virtual Private Network**.

When you create a VPN gateway, configure the VPC by referring to the VPC information obtained in **Step 2**. When you create a VPN connection, configure the subnet associated with the replication instance by referring to the subnet information obtained in **Step 1**.

Step 4 Configure the VPN device in the local data center.

The configuration method of the VPN device depends on the type of the firewall or host in the local data center. For details, see **Configuring the Remote Device**.

Step 5 Configure the IP address whitelist for the on-premises database.

Add the private IP address of the DRS instance to the whitelist of the on-premises database to allow access from the DRS instance.

The method for configuring the whitelist depends on the database type. For details, see the official documents of each database.

Step 6 Configure a security group and an access control list (ACL).

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS instance in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the DRS private network IP address to the IP address and listening port of the on-premises database is allowed.

Network ACL: Ensure that the outbound traffic from the DRS private network IP address and random port to the IP address and listening port of the on-premises database is allowed.

Step 7 Test the connection.

Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page,

enter the IP address, port, username, and password of the on-premises database and then click **Test Connection** to check whether the connection is successful.

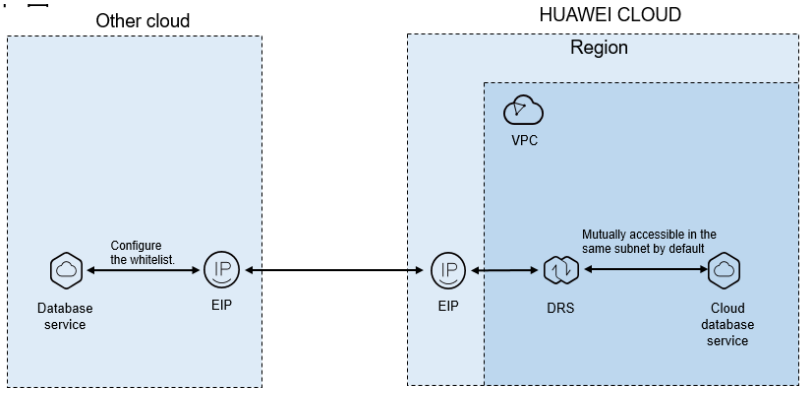
----End

5 From Other Cloud Databases to Huawei Cloud

5.1 Accessing Huawei Cloud over a Public Network

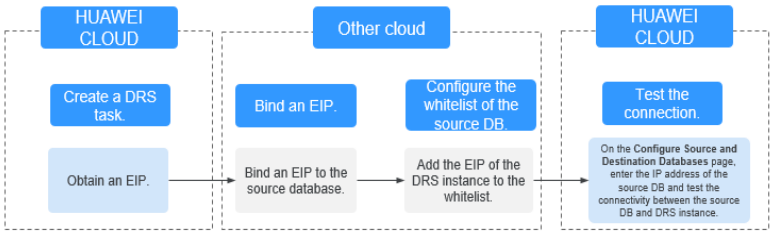
Figure 5-1 shows how to use DRS to migrate data from other cloud databases to Huawei Cloud databases over a public network.

Figure 5-1 Network diagram



If you use DRS to access other cloud databases through a public network, bind an EIP to the cloud database and add the EIP of the DRS instance to the whitelist of the cloud database. After that, the DRS instance can access the cloud database through the EIP. Figure 5-2 shows the operation process.

Figure 5-2 Flowchart

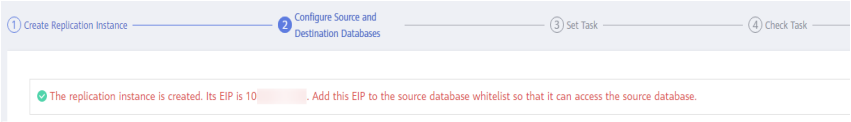


Network Configurations

Step 1 Create a DRS task and obtain the EIP of the DRS instance.

The IP address displayed on the **Configure Source and Destination Databases** page is the EIP of the DRS instance.

Figure 5-3 EIP of the DRS instance



Step 2 Apply for an EIP and bind it to the database on the other cloud.

The configuration method depends on the database type. For details, see the official documents of the corresponding cloud platform.

Step 3 Configure the IP address whitelist for the database on the other cloud.

Add the EIP of the DRS instance to the whitelist to allow the traffic from the EIP.

The method for configuring the whitelist depends on the cloud database vendor. For details, see the official documents of the corresponding cloud database vendor.

Step 4 Test the connection.

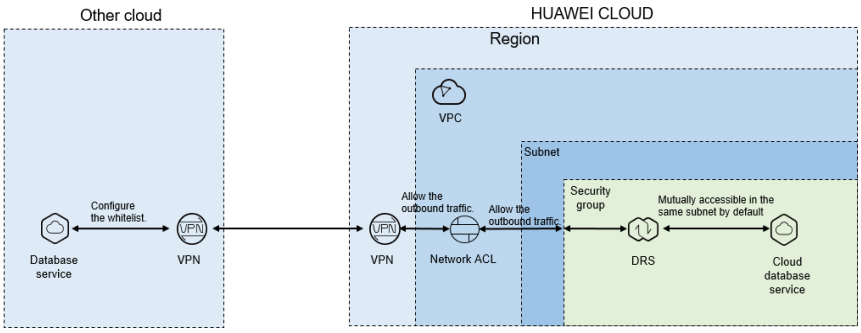
Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the database on the other cloud and then click **Test Connection** to check whether the connection is successful.

----End

5.2 Accessing Huawei Cloud over a VPN

Figure 5-4 shows how to use DRS to migrate data from other cloud databases to Huawei Cloud databases over a VPN.

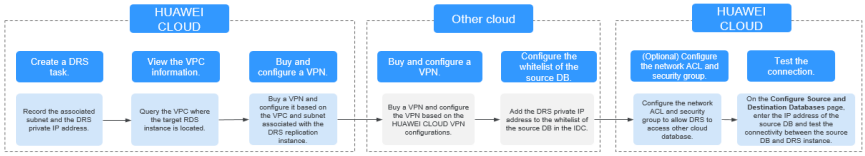
Figure 5-4 Network diagram



If you use DRS to access other cloud databases over a VPN, purchase a VPN on Huawei Cloud and configure the VPN to connect to the VPC that contains the DRS

instance. In addition, you need to purchase and configure a VPN on the other cloud to enable communication between the DRS instance and the source database. **Figure 5-5** shows the process.

Figure 5-5 Flowchart

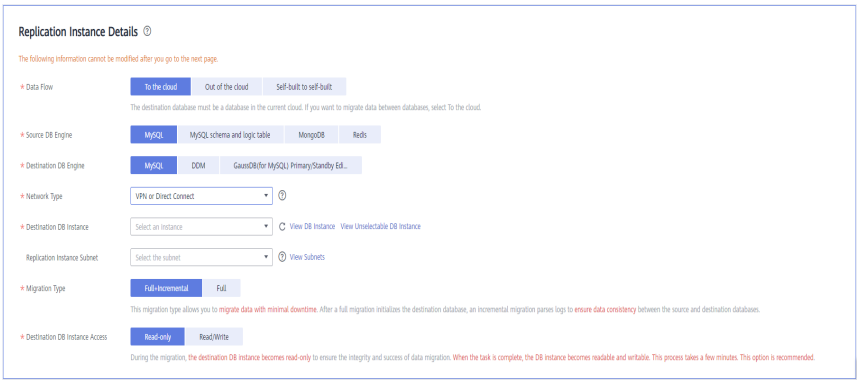


Network Configurations

Step 1 Create a DRS instance and obtain the subnet and private IP address of the DRS instance.

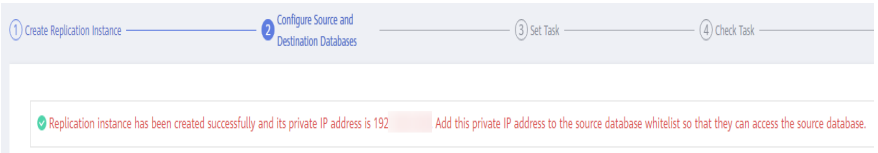
By default, the DRS instance is in the same subnet as the destination database.

Figure 5-6 Replication instance information



After the DRS replication instance is created, the private IP address of the replication instance is displayed.

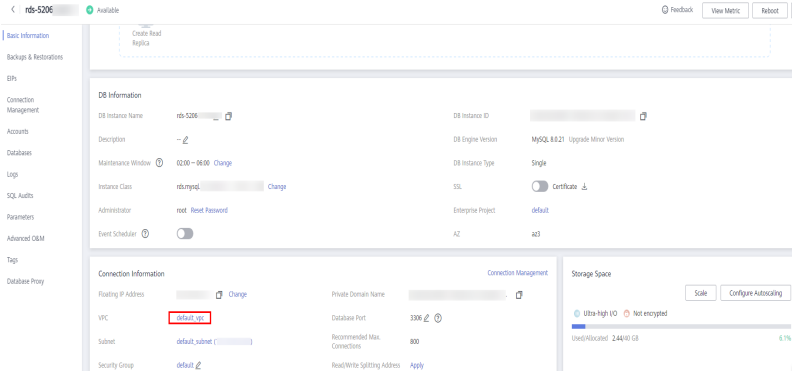
Figure 5-7 Private IP address of the DRS instance



Step 2 Query the name of the VPC to which the DRS instance belongs.

By default, the DRS replication instance and the destination RDS instance are created in the same VPC. You can log in to the destination RDS instance to view information about the VPC where the replication instance is located.

Figure 5-8 Destination database information



Step 3 Purchase a VPN and configure the VPN gateway and connection.

For details, see **Getting Started with Virtual Private Network**.

When you create a VPN gateway, configure the VPC by referring to the VPC information obtained in **Step 2**. When you create a VPN connection, configure the subnet associated with the replication instance by referring to the subnet information obtained in **Step 1**.

Step 4 Purchase a VPN on the other cloud and connect to the VPN based on the Huawei Cloud VPN configuration.

For details, see the documents on the official websites of the corresponding cloud database.

Step 5 Configure the IP address whitelists for the other cloud database.

Add the private IP address of the replication instance to the whitelist. The method for configuring the whitelist depends on the cloud database vendor. For details, see the official documents of the corresponding database.

Step 6 Configure a security group and an access control list (ACL).

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS instance in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the DRS private network IP address to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the DRS private network IP address and random port to the IP address and listening port of the source database is allowed.

Step 7 Test the connection.

Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the database on the other

cloud and then click **Test Connection** to check whether the connection is successful.

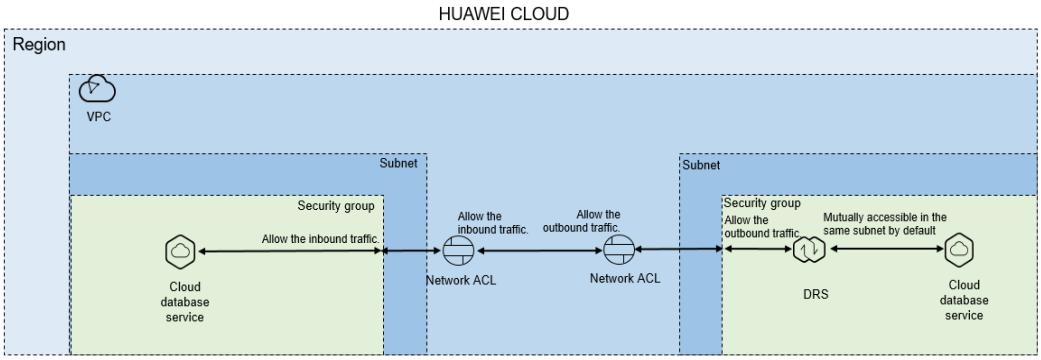
----End

6 From Huawei Cloud to Huawei Cloud

6.1 Accessing Huawei Cloud Through a VPC (Same Region and Same VPC)

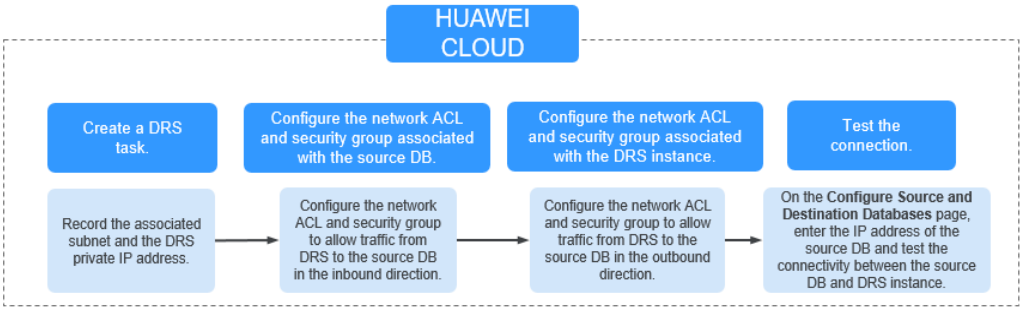
Figure 6-1 shows how to use DRS to migrate data across databases in the same region and VPC on Huawei Cloud.

Figure 6-1 Network diagram



If the DRS instance, the source and the destination RDS databases are in the same VPC and region, ensure that the network ACL and security group associated with the source database allow inbound traffic, and the network ACL and security group associated with the replication instance allow the outbound traffic. **Figure 6-2** shows the process.

Figure 6-2 Flowchart

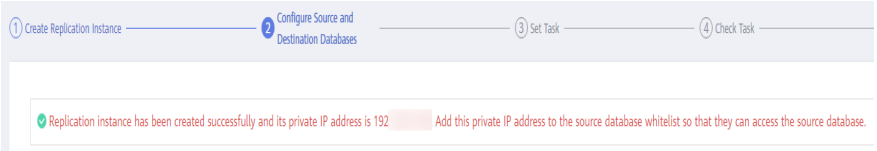


Network Configurations

Step 1 Create a DRS instance and obtain the private IP address of the DRS instance.

After the DRS replication instance is created, the private IP address of the replication instance is displayed.

Figure 6-3 Private IP address of the DRS instance



Step 2 Configure inbound rules for the network ACL and security group associated with the source database.

Security group: Add an inbound rule to allow traffic from the private IP address of the DRS replication instance to the source database listening port.

Network ACL: By default, a VPC does not have a network ACL. If you have a network ACL, add an inbound rule to allow traffic from the private IP address and random port of the DRS replication instance to the IP address and listening port of the source database.

Step 3 Configure outbound rules for the network ACL and security group associated with the replication instance.

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS database in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the DRS private network IP address to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the DRS private network IP address and random port to the IP address and listening port of the source database is allowed.

Step 4 Test the connection.

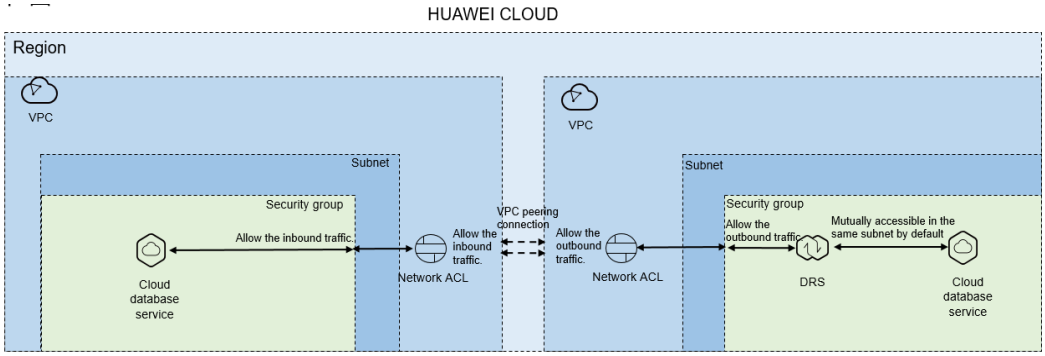
Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the source database and then click **Test Connection** to check whether the connection is successful.

----End

6.2 Accessing Huawei Cloud Through a VPC (Same Region and Different VPCs)

Figure 6-4 shows how to use DRS to migrate data across databases in the same region but different VPCs on Huawei Cloud.

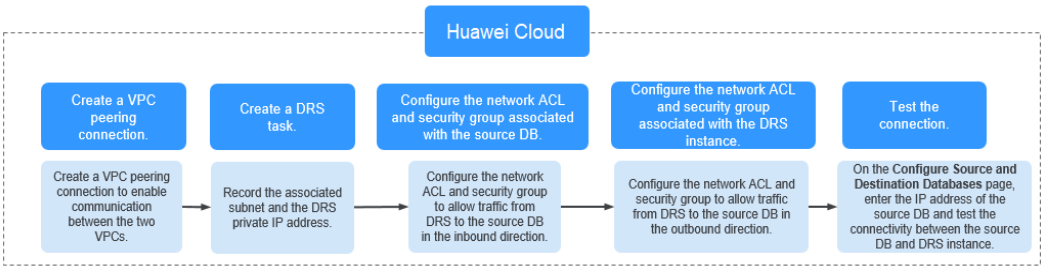
Figure 6-4 Network diagram



If you use DRS to access databases in a different VPC in the same region, create a VPC peering connection between the two VPCs. Ensure that the network ACL and security group associated with the source database allow inbound traffic, and the network ACL and security group associated with the replication instance allow the outbound traffic. If the source and destination databases are not in the same VPC, the CIDR blocks of the source and destination databases must be different.

Figure 6-5 shows the process.

Figure 6-5 Flowchart



Network Configurations

Step 1 Create a VPC peering connection.

For details, see **Virtual Private Cloud User Guide**.

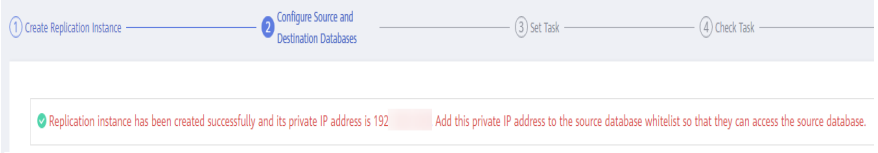
After the VPC peering connection is established, you need to add routes for the peer subnets in both the local and peer VPCs. For details, see **Adding Routes for a VPC Peering Connection**.

When you add routes for the VPC peering connection, you are advised to add network segment route information. If a point-to-point route is added, you need to add the route again after a DRS task is rebuilt and the instance IP address changes. Otherwise, the network will be disconnected.

Step 2 Create a DRS instance and obtain the private IP address of the DRS instance.

After the DRS replication instance is created, the private IP address of the replication instance is displayed.

Figure 6-6 Private IP address of the DRS instance



Step 3 Configure inbound rules for the network ACL and security group associated with the source database.

Security group: Add an inbound rule to allow traffic from the private IP address of the DRS replication instance to the database listening port.

Network ACL: By default, a VPC does not have a network ACL. If you have a network ACL, add an inbound rule to allow traffic from the private IP address and random port of the DRS replication instance to the IP address and listening port of the source database.

Step 4 Configure outbound rules for the network ACL and security group associated with the replication instance.

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS database in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the DRS private network IP address to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the DRS private network IP address and random port to the IP address and listening port of the source database is allowed.

Step 5 Test the connection.

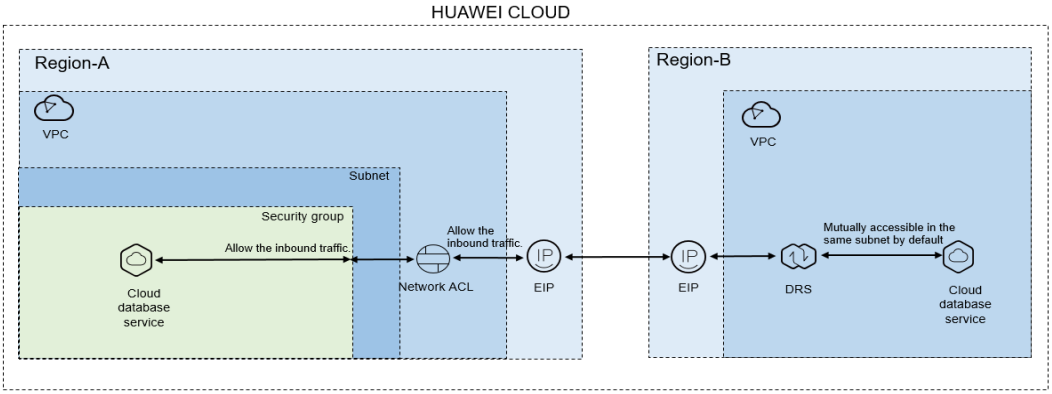
Log in to the DRS console. Locate the DRS task and click **Edit** in the **Operation** column. On the displayed **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the source database for the connection test.

----End

6.3 Accessing Huawei Cloud over a Public Network (Different Regions)

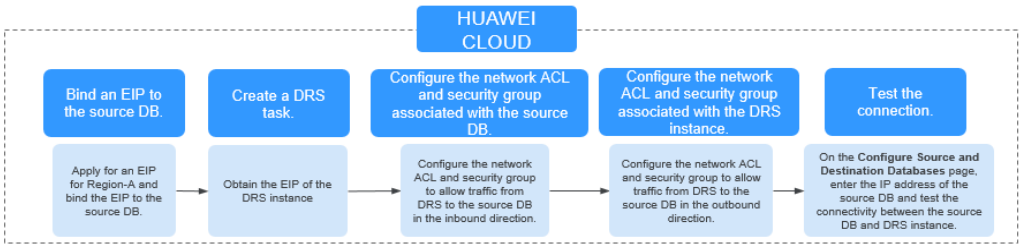
Figure 6-7 shows how to use DRS to migrate data across databases in different regions over a public network on Huawei Cloud.

Figure 6-7 Network diagram



If you use DRS to access a cross-region RDS database over a public network, bind an EIP to the RDS source database and configure inbound rules for the network ACL and security group associated with the source database in Region-A to allow inbound traffic from the EIP of the DRS replication instance. In addition, configure the outbound rules for the network ACL and security group associated with the DRS replication instance in Region-B to allow the outbound traffic. Figure 6-8 shows the process.

Figure 6-8 Flowchart



Network Configurations

Step 1 Bind an EIP to the source database.

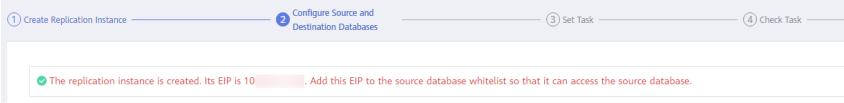
For details, see the official documents of Huawei Cloud databases.

For example, with Huawei Cloud RDS for MySQL as the source, see **Getting Started with Relational Database Service**.

Step 2 Create a DRS task and obtain the EIP of the DRS instance.

The IP address displayed on the **Configure Source and Destination Databases** page is the EIP of the DRS instance.

Figure 6-9 EIP of the DRS instance



Step 3 Configure inbound rules for the network ACL and security group associated with the source database.

Security group: Add an inbound rule to allow traffic from the EIP of the DRS replication instance to the database listening port.

Network ACL: By default, a VPC does not have a network ACL. If you have a network ACL, add an inbound rule to allow traffic from the EIP and random port of the DRS replication instance to the IP address and listening port of the source database.

Step 4 Configure outbound rules for the network ACL and security group associated with the replication instance.

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS database in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the security group associated with the replication instance to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the VPC where the replication instance resides and the DRS random port to the IP address and listening port of the source database is allowed.

Step 5 Test the connection.

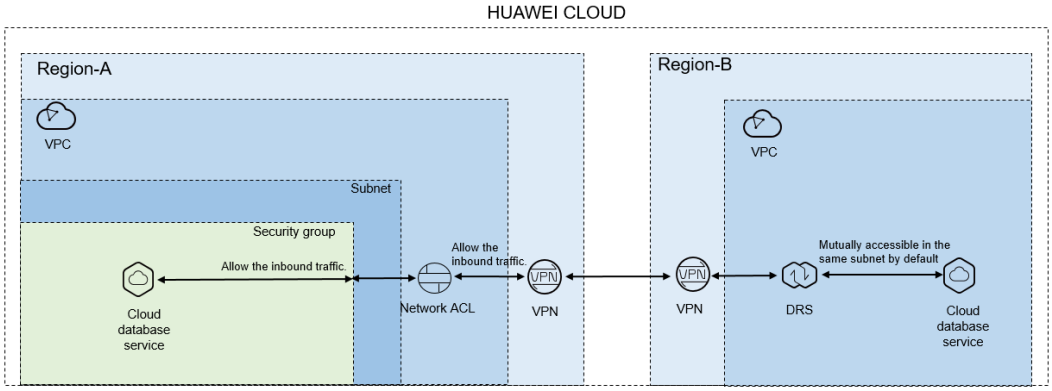
Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the source database and then click **Test Connection** to check whether the connection is successful.

----End

6.4 Accessing Huawei Cloud Through a VPN (Different Regions)

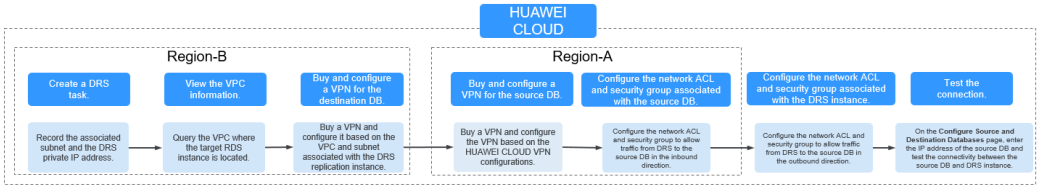
Figure 6-10 shows how to use DRS to migrate data across databases in different regions over a VPN network on Huawei Cloud.

Figure 6-10 Network diagram



If you use DRS to access a cross-region database through a VPN, create the VPN service on Huawei Cloud in Region-B and configure the VPC and subnet associated with the DRS replication instance. In addition, create the VPN service in Region-A, configure the VPN peer device, and add inbound rules for the network ACL and security group associated with the source database in Region-A to allow traffic from the private IP address of the replication instance. Then, configure outbound rules for the network ACL and security group associated with the replication instance in Region-B to allow outbound traffic. **Figure 6-11** shows the process.

Figure 6-11 Flowchart

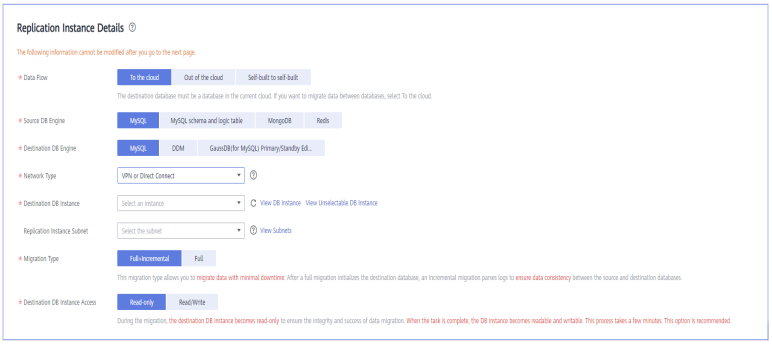


Network Configurations

Step 1 Create a DRS instance and obtain the subnet and private IP address of the DRS instance.

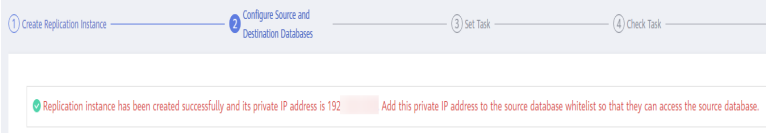
By default, the DRS instance is in the same subnet as the destination database.

Figure 6-12 Replication instance information



After the DRS replication instance is created, the private IP address of the replication instance is displayed.

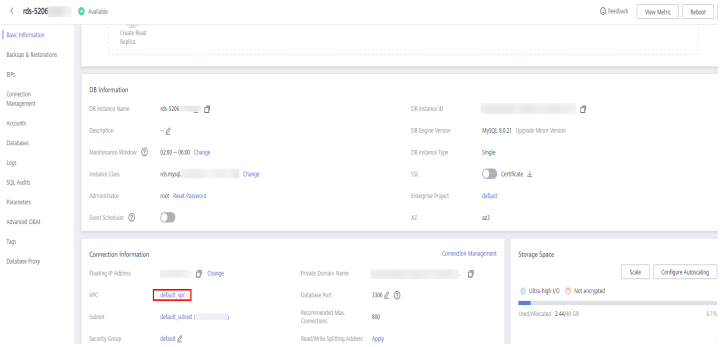
Figure 6-13 Private IP address of the DRS instance



Step 2 Query the name of the VPC to which the DRS instance belongs.

By default, the DRS replication instance and the destination RDS database are created in the same VPC. You can log in to the destination RDS instance to view information about the VPC where the replication instance is located.

Figure 6-14 Destination database information



Step 3 Create a VPN in the target region and configure the VPN gateway and connection.

For details, see **Getting Started with Virtual Private Network**.

When you create a VPN gateway, configure the VPC by referring to the VPC information obtained in **Step 2**. When you create a VPN connection, configure the subnet associated with the replication instance by referring to the subnet information obtained in **Step 1**.

Step 4 Create a VPN in the source region and configure the VPN peer device.

For details, see **Configuring the Remote Device** in *Getting Started with Virtual Private Network*.

Step 5 Configure inbound rules for the network ACL and security group associated with the source database.

Security group: Add an inbound rule to allow traffic from the private IP address of the DRS replication instance to the database listening port.

Network ACL: By default, a VPC does not have a network ACL. If you have a network ACL, add an inbound rule to allow traffic from the private IP address and random port of the DRS replication instance to the IP address and listening port of the source database.

Step 6 Configure outbound rules for the network ACL and security group associated with the replication instance.

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS

database in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the security group associated with the replication instance to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the VPC where the replication instance resides and the DRS random port to the IP address and listening port of the source database is allowed.

Step 7 Test the connection.

Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the source database and then click **Test Connection** to check whether the connection is successful.

----End

Helpful Links

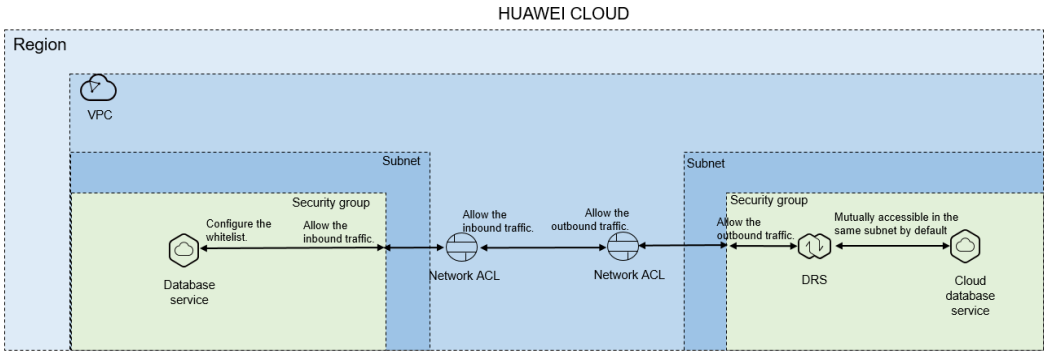
From RDS for MySQL to DDM

7 From ECS-Hosted Databases on Huawei Cloud to Huawei Cloud

7.1 Accessing Huawei Cloud Through a VPC (Same Region and Same VPC)

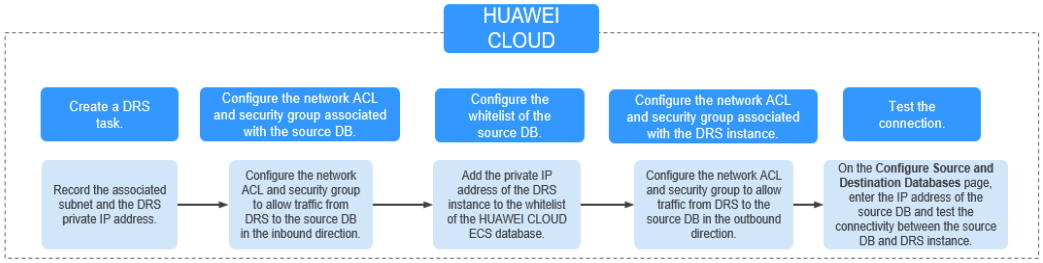
Figure 7-1 shows how to use DRS to migrate data from an ECS database to a database in the same region and VPC on Huawei Cloud.

Figure 7-1 Network diagram



You can use an ECS database as the source. If the source and destination databases are in the same VPC and region and DRS uses the VPC network, ensure that the network ACL and security group associated with the source database allow inbound traffic from the DRS replication instance. In addition, add the IP address of the replication instance to the whitelist of the source database, and ensure that the network ACL and security group associated with the DRS replication instance allow outbound traffic. **Figure 7-2** shows the process.

Figure 7-2 Flowchart

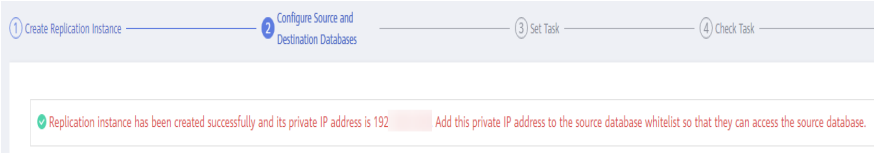


Network Configurations

Step 1 Create a DRS instance and obtain the private IP address of the DRS instance.

After the DRS replication instance is created, the private IP address of the replication instance is displayed.

Figure 7-3 Private IP address of the DRS instance



Step 2 Configure inbound rules for the network ACL and security group associated with the source database.

Security group: Add an inbound rule to allow traffic from the private IP address of the DRS replication instance to the database listening port.

Network ACL: By default, a VPC does not have a network ACL. If you have a network ACL, add an inbound rule to allow traffic from the private IP address and random port of the DRS replication instance to the IP address and listening port of the source database.

Step 3 Configure the IP address whitelist for the ECS database.

Add the private IP address of the DRS instance to the whitelist of the ECS database. The method for configuring the whitelist depends on the cloud database type. For details, see the official documents of the corresponding database.

Step 4 Configure outbound rules for the network ACL and security group associated with the replication instance.

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS database in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the DRS private network IP address to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the DRS private network IP address and random port to the IP address and listening port of the source database is allowed.

Step 5 Test the connection.

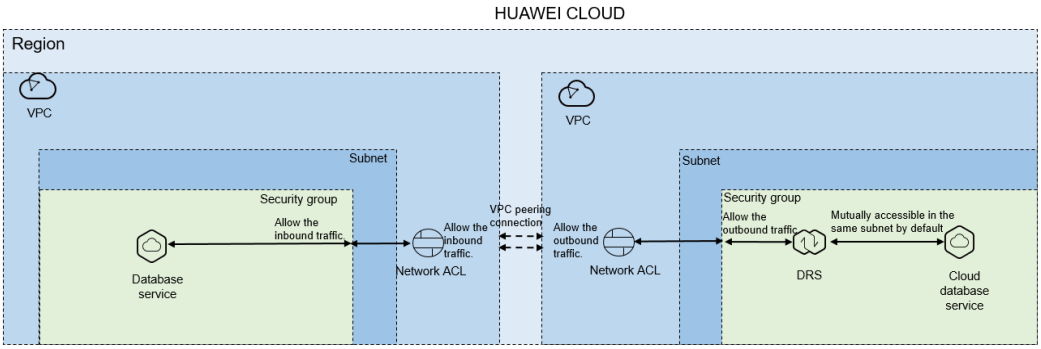
Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the source database and then click **Test Connection** to check whether the connection is successful.

----End

7.2 Accessing Huawei Cloud Through a VPC (Same Region and Different VPCs)

Figure 7-4 shows how to use DRS to migrate data from an ECS database to a database in the same region but different VPCs on Huawei Cloud.

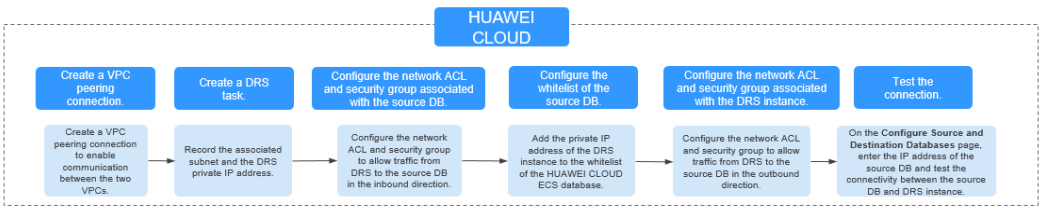
Figure 7-4 Network diagram



You can use an ECS database as the source. If the source and destination databases are in two different VPCs in the same region, create a VPC peering connection between the two VPCs. Ensure that the network ACL and security group associated with the source database allow inbound traffic from the DRS replication instance. In addition, add the replication instance IP address to the whitelist of the source database, and ensure that the network ACL and security group associated with the DRS replication instance allow outbound traffic. If the source and destination databases are not in the same VPC, the CIDR blocks of the source and destination databases must be different.

Figure 7-5 shows the process.

Figure 7-5 Flowchart



Network Configurations

Step 1 Create a VPC peering connection.

For details, see **Virtual Private Cloud User Guide**.

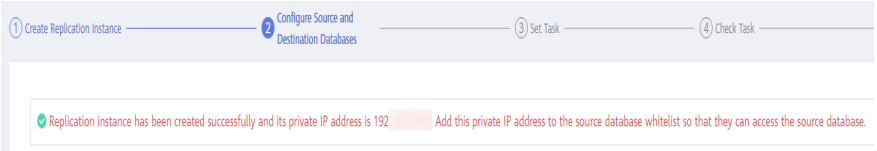
After the VPC peering connection is established, you need to add routes for the peer subnets in both the local and peer VPCs. For details, see **Adding Routes for a VPC Peering Connection**.

When you add routes for the VPC peering connection, you are advised to add network segment route information. If a point-to-point route is added, you need to add the route again after a DRS task is rebuilt and the instance IP address changes. Otherwise, the network will be disconnected.

Step 2 Create a DRS instance and obtain the private IP address of the DRS instance.

After the DRS replication instance is created, the private IP address of the replication instance is displayed.

Figure 7-6 Private IP address of the DRS instance



Step 3 Configure inbound rules for the network ACL and security group associated with the source database.

Security group: Add an inbound rule to allow traffic from the private IP address of the DRS replication instance to the database listening port.

Network ACL: By default, a VPC does not have a network ACL. If you have a network ACL, add an inbound rule to allow traffic from the private IP address and random port of the DRS replication instance to the IP address and listening port of the source database.

Step 4 Configure the IP address whitelist for the ECS database.

Add the private IP address of the DRS instance to the whitelist of the ECS database. The method for configuring the whitelist depends on the cloud database type. For details, see the official documents of the corresponding database.

Step 5 Configure outbound rules for the network ACL and security group associated with the replication instance.

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS database in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the DRS private network IP address to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the DRS private network IP address and random port to the IP address and listening port of the source database is allowed.

Step 6 Test the connection.

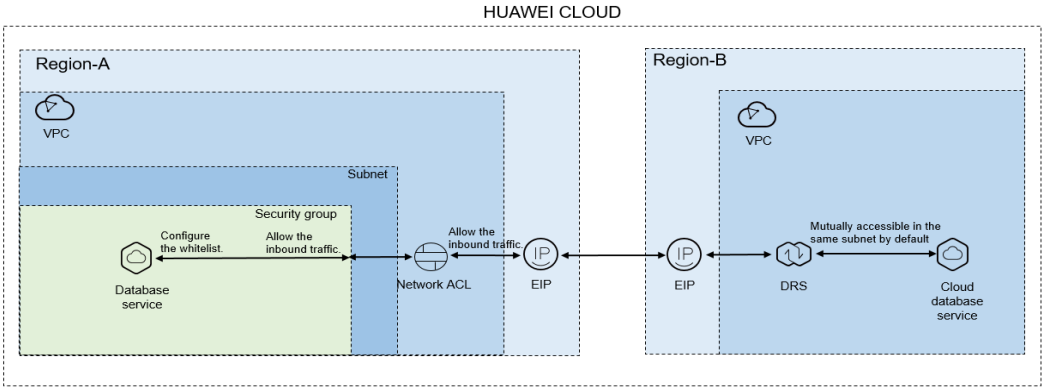
Log in to the DRS console. Locate the DRS task and click **Edit** in the **Operation** column. On the displayed **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the source database for the connection test.

----End

7.3 Accessing Huawei Cloud over a Public Network (Different Regions)

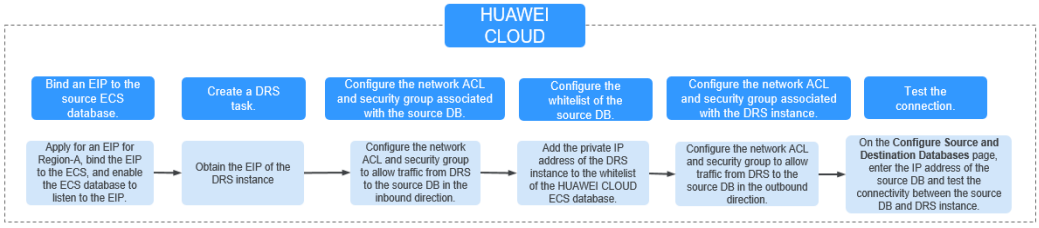
Figure 7-7 shows how to use DRS to migrate data from an ECS database to a database in different regions over a public network on Huawei Cloud.

Figure 7-7 Network diagram



You can use an ECS database as the source. If the source and destination databases are in different regions and DRS uses a public network, bind an EIP to the ECS where the source database is located, configure the inbound rules for the network ACL and security group associated with the source database in Region-A to allow inbound traffic from the EIP of the DRS replication instance, add the EIP of the DRS replication instance to the whitelist of the source database, and configure the outbound rules for the network ACL and security group associated with the DRS replication instance in Region-B to allow outbound traffic. **Figure 7-8** shows the process.

Figure 7-8 Flowchart



Network Configurations

Step 1 Bind an EIP to the source database.

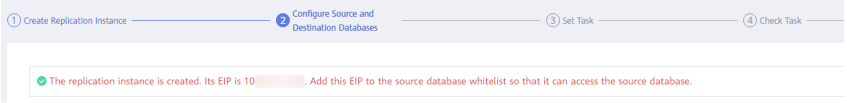
For details, see the official documents of Huawei Cloud databases.

For example, with Huawei Cloud RDS for MySQL as the source, see **Getting Started with Relational Database Service**.

Step 2 Create a DRS task and obtain the EIP of the DRS instance.

The IP address on the **Configure Source and Destination Databases** page is the EIP of the DR instance.

Figure 7-9 EIP of the DRS instance



Step 3 Configure inbound rules for the network ACL and security group associated with the source database.

Security group: Add an inbound rule to allow traffic from the EIP of the DRS replication instance to the database listening port.

Network ACL: By default, a VPC does not have a network ACL. If you have a network ACL, add an inbound rule to allow traffic from the EIP and random port of the DRS replication instance to the IP address and listening port of the source database.

Step 4 Configure the IP address whitelist for the ECS database.

Add the private IP address of the DRS instance to the whitelist of the ECS database. The method for configuring the whitelist depends on the cloud database type. For details, see the official documents of the corresponding database.

Step 5 Configure outbound rules for the network ACL and security group associated with the replication instance.

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS database in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the security group associated with the replication instance to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the VPC where the replication instance resides and the DRS random port to the IP address and listening port of the source database is allowed.

Step 6 Test the connection.

Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page,

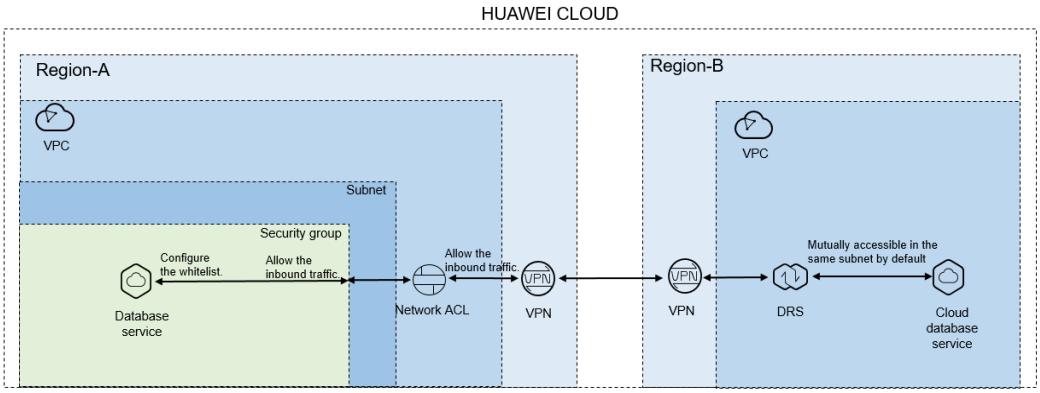
enter the IP address, port, username, and password of the source database and then click **Test Connection** to check whether the connection is successful.

----End

7.4 Accessing Huawei Cloud Through a VPN (Different Regions)

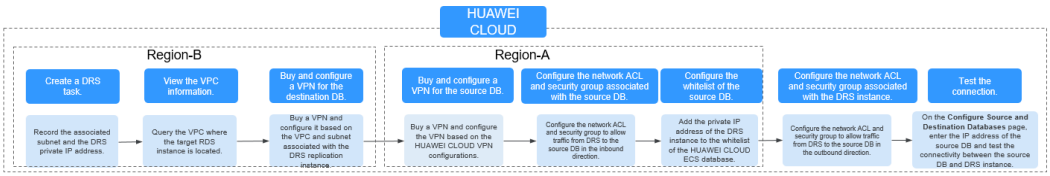
Figure 7-10 shows how to use DRS to migrate data from an ECS database to a database in different regions over a VPN network on Huawei Cloud.

Figure 7-10 Network diagram



You can use an ECS database as the source. If the source and destination databases are in different regions and DRS uses a VPN, create the VPN service on Huawei Cloud in Region-B and configure the VPC and subnet associated with the DRS replication instance. In addition, create the VPN service in Region-A, configure the VPN peer device, add inbound rules for the network ACL and security group associated with the source database in Region-A to allow traffic from the private IP address of the DRS replication instance, add the private IP address of the DRS replication instance to the source database whitelist, and configure outbound rules for the network ACL and security group associated with the replication instance in Region-B to allow outbound traffic. **Figure 7-11** shows the process.

Figure 7-11 Flowchart

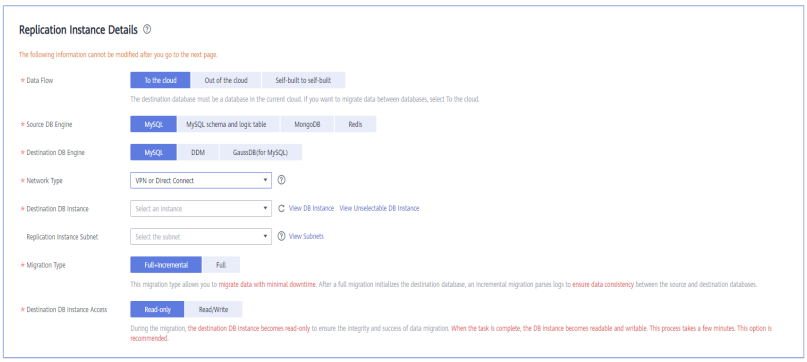


Network Configurations

Step 1 Create a DRS instance and obtain the subnet and private IP address of the DRS instance.

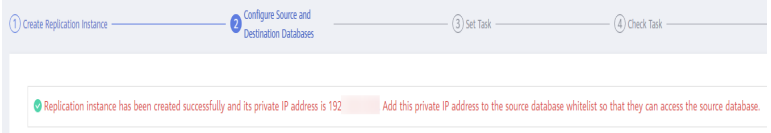
By default, the subnet associated with the DRS instance is the same as that of the destination database.

Figure 7-12 Replication instance information



After the DRS replication instance is created, the private IP address of the replication instance is displayed.

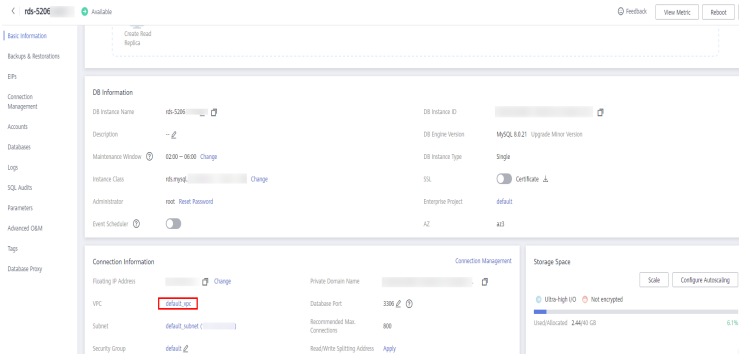
Figure 7-13 Private IP address of the DRS instance



Step 2 Query the name of the VPC to which the DRS instance belongs.

By default, the DRS replication instance and the destination RDS database are created in the same VPC. You can log in to the destination RDS instance to view information about the VPC where the replication instance is located.

Figure 7-14 Destination database information



Step 3 Create a VPN in the target region and configure the VPN gateway and connection.

For details, see **Getting Started with Virtual Private Network**.

When you create a VPN gateway, configure the VPC by referring to the VPC information obtained in **Step 2**. When you create a VPN connection, configure the subnet associated with the replication instance by referring to the subnet information obtained in **Step 1**.

Step 4 Create a VPN in the source region and configure the VPN peer device.

For details, see **Configuring the Remote Device** in *Getting Started with Virtual Private Network*.

Step 5 Configure inbound rules for the network ACL and security group associated with the source database.

Security group: Add an inbound rule to allow traffic from the private IP address of the DRS replication instance to the database listening port.

Network ACL: By default, a VPC does not have a network ACL. If you have a network ACL, add an inbound rule to allow traffic from the private IP address and random port of the DRS replication instance to the IP address and listening port of the source database.

Step 6 Configure the IP address whitelist for the source database.

Add the private IP address of the DRS replication instance to the whitelist of the source database. The method for configuring the whitelist depends on the cloud database type. For details, see the official documents of the corresponding database.

Step 7 Configure outbound rules for the network ACL and security group associated with the replication instance.

By default, a VPC does not have a network ACL, and the default security group rules allow all outbound traffic. The replication instance and destination RDS database in the same security group can communicate with each other by default, so you do not need to configure a network ACL.

If you have configured a network ACL or security group, log in to the VPC management console and check the settings:

Security group: Ensure that the outbound traffic from the security group associated with the replication instance to the IP address and listening port of the source database is allowed.

Network ACL: Ensure that the outbound traffic from the VPC where the replication instance resides and the DRS random port to the IP address and listening port of the source database is allowed.

Step 8 Test the connection.

Log in to the DRS console, locate the created DRS task, and click **Edit** in the **Operation** column. On the **Configure Source and Destination Databases** page, enter the IP address, port, username, and password of the source database and then click **Test Connection** to check whether the connection is successful.

----End

8 Getting Started with Common Practices

After completing basic preparations such as accounts, permissions, databases, and networks, you can view common practices to better use DRS.

Table 8-1 Common practices

Scenario		Practice	Description
Creating a Task	Real-Time Migration	**From Other Cloud MySQL to RDS for MySQL**	This practice describes how to use DRS to migrate data from a MySQL database on another cloud to a Huawei Cloud RDS for MySQL instance through a public network.
		From Other Cloud MySQL to GaussDB(for MySQL)	This practice describes how to use DRS to migrate data from a MySQL database on another cloud to a Huawei Cloud GaussDB(for MySQL) instance through a public network.
		From Other Cloud MongoDB to DDS	This practice describes how to use DRS to migrate data from a MongoDB database on another cloud to a Huawei Cloud DDS instance through a public network.
		From ECS-hosted MySQL to RDS for MySQL	This practice describes how to use DRS to migrate data from a MySQL database built on an ECS to an RDS for MySQL instance in the same VPC of the same region through a VPC.
		From ECS-hosted MySQL to GaussDB(for MySQL)	This practice describes how to use DRS to migrate data from a MySQL database built on an ECS to a GaussDB(for MySQL) instance in the same VPC of the same region through a VPC.

Scenario		Practice	Description
		From ECS-hosted MongoDB to DDS	This practice describes how to use DRS to migrate data from a MongoDB database built on an ECS to a DDS instance in the same VPC of the same region through a VPC.
		From On-Premises MySQL to RDS for MySQL	This practice describes how to use DRS to migrate data from an on-premises MySQL database to a Huawei Cloud RDS for MySQL instance through a public network.
		From On-Premises MongoDB to DDS	This practice describes how to use DRS to migrate data from an on-premises MongoDB database to a Huawei Cloud DDS instance through a public network.
		From RDS for MySQL to DDM	This practice describes how to use DRS to migrate data from a Huawei Cloud RDS for MySQL instance to a DDM instance in different regions through a VPN.
		From MySQL Schema and Logic Table to DDM	This practice describes how to use DRS to migrate data from MySQL shards and tables to a DDM instance through a public network.
	Backup Migration	**Migrating Microsoft SQL Server Backup Data to RDS for SQL Server**	This practice describes how to use DRS to restore local Microsoft SQL Server data backups to an RDS for SQL Server instance. DRS supports full backup migration and full+incremental backup migration.
	Real-Time Synchronization	**From Other Cloud PostgreSQL to RDS for PostgreSQL**	This practice describes how to use DRS to synchronize data from a PostgreSQL database on another cloud to an RDS for PostgreSQL instance through a public network.
		From ECS-hosted PostgreSQL to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from a PostgreSQL database built on an ECS to an RDS for PostgreSQL instance through a VPC.
		From On-Premises PostgreSQL to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from an on-premises PostgreSQL database to an RDS for PostgreSQL instance through a public network.

Scenario		Practice	Description
		From On-Premises Oracle to GaussDB	This practice describes how to use DRS to create a full+incremental task to continuously synchronize data from an on-premise Oracle database to a GaussDB instance through a public network.
		From On-Premises Oracle to DDM	This practice describes how to use DRS to create a full+incremental task to continuously synchronize data from an on-premise Oracle database to a DDM instance through a public network.
		From RDS for MySQL to Kafka	This practice describes how to use DRS to create an incremental task to synchronize incremental data from an RDS for MySQL instance to a Kafka instance through a VPC.
	Real-Time DR	**Configuring Remote Single-Active DR for an RDS for MySQL Instance Using DRS**	This practice describes how to use DRS to synchronize data from an RDS for MySQL instance in the production center to an RDS for MySQL instance in the DR center through a public network to implement data DR between the primary instance and the DR instance across regions.
Querying Task Progress	Real-Time Migration	**Querying the Migration Progress**	DRS shows the task progress using a progress bar, helping you keep track of the status of a task.
	Real-Time Synchronization	**Querying the Synchronization Progress**	
	Real-Time DR	**Querying the DR Progress**	
Comparing Data	Real-Time Migration	**Comparing Migration Items**	Data comparison allows you to check data consistency between source and destination databases before and after the migration. To minimize the impact on services and shorten the service interruption duration, DRS provides multiple comparison methods.
	Real-Time Synchronization	**Comparing Synchronization Items**	

Scenario		Practice	Description
	Real-Time DR	**Comparing DR Items**	
Managing Tasks	Real-Time Migration	**Migration Task Life Cycle**	During the life cycle of a DRS task, you can edit, pause, reset, resume and stop the task, and modify the flow control mode of the task as required.
	Real-Time Synchronization	**Synchronization Task Life Cycle**	
	Real-Time DR	**DR Task Life Cycle**	

More Information

- **Real-Time Migration Overview**
- **Backup Migration Overview**
- **Real-Time Synchronization Overview**
- **Real-Time DR Overview**

