Data Replication Service

Preparations

 Issue
 01

 Date
 2024-11-30





HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. 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

NUAWEI 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: <u>https://e.huawei.com</u>

Security Declaration

Product Lifecycle

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

Vulnerability

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

https://securitybulletin.huawei.com/enterprise/en/security-advisory

Initial Digital Certificate

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

Huawei Enterprise End User License Agreement

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

https://e.huawei.com/en/about/eula

Lifecycle of Product Documentation

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

Contents

1 Overview	1
2 Registering a Huawei ID and Enabling Huawei Cloud Services	3
3 Permissions Management	4
3.1 Creating a User and Granting Permissions	4
3.2 Creating a Custom Policy	5
4 From On-premises Databases to Huawei Cloud	7
4.1 Accessing Huawei Cloud over a Public Network	7
4.2 Accessing Huawei Cloud over a VPN	
5 From Other Cloud Databases to Huawei Cloud	12
5.1 Accessing Huawei Cloud over a Public Network	12
5.2 Accessing Huawei Cloud over a VPN	
6 From Huawei Cloud to Huawei Cloud	17
6.1 Accessing Huawei Cloud Through a VPC (Same Region and Same VPC)	17
6.2 Accessing Huawei Cloud Through a VPC (Same Region and Different VPCs)	
6.3 Accessing Huawei Cloud over a Public Network (Different Regions)	21
6.4 Accessing Huawei Cloud Through a VPN (Different Regions)	22
7 From ECS-Hosted Databases on Huawei Cloud to Huawei Cloud	26
7.1 Accessing Huawei Cloud Through a VPC (Same Region and Same VPC)	
7.2 Accessing Huawei Cloud Through a VPC (Same Region and Different VPCs)	
7.3 Accessing Huawei Cloud over a Public Network (Different Regions)	
7.4 Accessing Huawei Cloud Through a VPN (Different Regions)	32
8 Getting Started with Common Practices	

Overview

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

ltem	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 .
Databas e	 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
Networ k	The source database is deployed on a local host.	For details, see From On-premises Databases to Huawei Cloud.

 Table 1-1 Preparations

ltem	Description	Reference						
	The source is a database of other cloud.	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- hosted 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



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

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.

Log in and verify permissions. 3.

> 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



If you use DRS to access databases in the on-premises data center through a public network, bind an EIP when creating the DRS task and configure the onpremises 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 through a public network and bind an EIP to the DRS instance.

When creating a DRS task through a public network, you can bind an EIP to the DRS instance on the instance details page.

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 4-3 shows how to use DRS to migrate data from on-premises databases to Huawei Cloud databases using a VPN.



Figure 4-3 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 4-4 shows the operation process.



	Huawei Cloud		IDC		Huawe	ei Cloud
Create a DRS task.	View the VPC information.	Buy and configure a VPN.	Configure a VPN in the IDC.	Configure the whitelist of the source DB.	(Optional) Configure the network ACL and security group.	Test the connection.
Record the associated subnet and the DRS private IP address.	Query the VPC where the target RDS instance is located.	Buy a VPN and configure it based on the VPC and subnet associated with the DRS replication instance.	Configure a VPN on the firewall or server software in the IDC.	Add the DRS private IP address to the whitelist of the source DB in the IDC.	Configure the network ACL and security group to allow DRS to access the source DB in the IDC.	On the Configure Source and Destination Databases page, enter the IP address of the source DB and test the connectivity between the source DB and DRS instance.

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 4-5	Replication	instance	information
------------	-------------	----------	-------------

Replication Instance De	tails 0
The following information cannot be n	nodilad after you go to the net, page.
* Data Flow	To the cloud Out of the cloud Self built to self built
	The destination database must be a database in the current cloud. If you want to migrate data between database, select To the cloud.
* Source DB Engine	MySQL MySQL schema and logic table Mongo08 Reds
* Destination D8 Engine	MpSQL DDM Gexin01/for MpSQL Primary/Standby Ed.
* Network Type	VPN or Direct Connect •
* Destination D8 Instance	Soliet an instance C Wee DB Instance Veer Unselectable DD Instance
Replication Instance Subnet	Solect the solovet
* Migration Type	Ful-transition Ful
	This migration type allows you to migrate data with minimal dountime. After a full migration initializes the destination database, an incremental migration parses logs to ensure data consistency between the source and destination databases.
* Destination DB Instance Access	backey backwise During the regulator, the declaration Self national becomes read-only to ensure the interprise of data respection. Where the task is complete, the Self national becomes readable and website. This process tables a like instructs. This optima is accommended

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

Figure 4-6 Private IP address of the DRS instance

Create Replication Instance Configure Source and Destination Databases	— (3) Set Task ———	— (4) Check Task ——	5 Compare Parameters —	(6) Confirm Task
The replication instance is created and its IP address is	. To ensure networ	k connectivity, add this I	P address to the network whitelist	of the source database.

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.

< rds-5206	Available							G Feedback	Viev Metric	Reboot	
Basic Information	Create Read Replica										
Backups & Restorations											
BR											
Connection	D8 Information										
Management.	DB Instance Name	rds-5206 🗇			DB Instance ID		đ				
Accounts	Description	-2			DB Engine Version	MySQL 8.02	21 Upgrade Minor Version				
Databases	Maintenance Window 🕥	0200 - 0600 Change			DB Instance Type	Single					
Logs	Instance Class	rds.mysql. Change			551	C Ce	nttate 🛓				
SQL Audits	Lindestator	and East Dessared			Enterreixa Desiart	Adust					
Parameters					Dispirot Project.	UCON.					
Advanced O&M	Event Scheduler (1)				12	223					
Tags											
Database Proxy	Connection Information				Connecto	n Management	Storage Space				
	Floating IP Address	Change	Private Domain Name			0		50	* Congu	N Autoscaling	
	VPC	default_yp;	Database Port	3306 🖉 🛞			 Ubra-high (/0) Not encrypt 	ted	_		
	Subnet	default_subret (1000)	Recommended Max. Connections	800			Used/Allocated 2.44/40 GB			6.19	

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 when creating the DRS task 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 through a public network and bind an EIP to the DRS instance.

When creating a DRS task through a public network, you can bind an EIP to the DRS instance on the instance details page.

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 5-3 shows how to use DRS to migrate data from other cloud databases to Huawei Cloud databases over a VPN.



Figure 5-3 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 5-4** shows the process.

Figure 5-4 Flowchart

 	 Huawei Cloud]			Oth	er clo	oud			Hua	we	i Cloud
Create a DRS task.	View the VPC information.		Buy and configure a VPN.		Buy and configure a VPN.		Configure the whitelist of the source DB.			(Optional) Configure the network ACL and security group.		Test the connection.
Record the associated subnet and the DRS private IP address.	 Query the VPC where the target RDS instance is located.		Buy a VPN and configure it based on the VPC and subnet associated with the DRS replication instance.	•	Buy a VPN and configure the VPN based on the HUAWEI CLOUD VPN configurations.	_,	Add the DRS private IP oddress to the whitelist of the source DB in the IDC.	-	-•	Configure the network ACL and security group to allow DRS to access other cloud database.	-•	On the Configure Source and Destination Databases page, enter the IP address of the source DB and feat the connectivity between the source DB and DRS instance.

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 5-5 Replication instance information



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

Figure 5-6 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.

< rds-5206	 Available 							G Feedback	View Metric	Reboot
Basic Information Backups & Restorations	Create Read Replica									
BPs										
Connection	DB Information									
Management	DB Instance Name	rds-5206 🗇			DB Instance ID		đ			
Accounts	Description	-2			DB Engine Version	MySQL 8.0.	21 Upgrade Minor Version			
Databases	Maintenance Window (?)	02:00 - 06:00 (hance			DB Instance Type	Sincle				
Logs										
SQL Audits	Instance Liass	resmysqu Unange			22	0.0	nnam 3			
Parameters	Administrator	root. Reset Rassword			Enterprise Project	default				
Advanced OBM	Event Scheduler 🔞				AZ.	823				
Taos										
Database Prozy	Connection Information				Connection N	laragement	Storage Space			
	Floating IP Address	🗇 Ovange	Private Domain Name		- 0			Scal	e Configure	e Autoscaling
	VPC	default_vpc	Database Port	3306 🖉 💮			🕘 Ultra-high (/O 👩 Not encryp	ted		
	Subnet	default_subnet ()	Recommended Max. Connections	800			Used/Allocated 2/44/40 GB			6.1%

Figure 5-7 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

Configure Source and Destination Databases	3 Set Task	- (4) Check Task	5 Compare Parameters	— (6) Confirm Task
The replication instance is created and its IP address is	. To ensure network	connectivity, add this IP a	ddress to the network whitelist of t	he source database.

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.





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 about how to create a VPC peering connection with another VPC in your account, see Creating a VPC Peering Connection with Another VPC in Your Account.

 For details about how to create a VPC peering connection with a VPC in another account, see Creating a VPC Peering Connection with a VPC in Another Account.

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

Create Replication Instance Configure Source and Destination Databases	(3) Set Task (4) Che	ck Task 5 Compare Parameters	6 Confirm Task
The replication instance is created and its IP address is	To ensure network connectiv	vity, add this IP address to the network wh	itelist of the source database.

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.

If the source database is a Huawei Cloud RDS for MySQL database, bind and unbind an EIP by referring to **Binding and Unbinding an EIP**.

Step 2 Create a DRS task through a public network and bind an EIP to the DRS instance.

When creating a DRS task through a public network, you can bind an EIP to the DRS instance on the instance details page.

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 6-9 shows how to use DRS to migrate data across databases in different regions over a VPN network on Huawei Cloud.

Figure 6-9 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. Then, configure outbound rules for the network ACL and security group associated with the replication instance in Region-B to allow outbound traffic. Figure 6-10 shows the process.

Figure 6-10 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	5-11	Replication	instance	information

Replication Instance Details 💿					
The following information cannot be m	offiel after you go to the rest page.				
* Data Flow	To the cloud Out of the cloud Self-built to self-built				
	The destination database must be a database in the current cloud. If you want to migrate data between databases, select To the cloud.				
* Source DB Engine	MgSQL MgSQL schema and logic table MongoDB Reds				
* Destination DB Engine	MySQL DDM GaussDillfor MySQL Primary/Standby Ed				
* Network Type	VPIK or Direct Connect • 0				
* Destination DB Instance	Select an instance 🔹 C View DB Instance View Unselectable DB Instance				
Replication Instance Subnet	Select the subset.				
* Migration Type	Fell-Incremental Fell				
	This migration type allows you to migrate data with minimal downtime. After a full migration initializes the dostination database, an incremental migration panes logs to ensure data consistency between the source and dostination databases.				
* Destination DB Instance Access	Read-only Read/Write				
	During the migration, the distination DB Instance becomes mad-only to ensure the integrity and secones of data migration. When the task is complete, the DB Instance becomes readable and wettable. This process takes a few minutes. This option is recommended.				

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

Figure 6-12 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 6-13 Destination database information

< rds-5206	Available							G Feedback	View Metric	Reboot
Basic Information	Create Read Replica									
Backups & Restanations										
BPs										
Connection	DB Information									
Management	DB Instance Name	rds-5206 🗇			D8 Instance ID		đ			
Accounts	Description	-2			D8 Engine Version	MySQL 8.0.21	Upgrade Minor Version			
Databases	Maintenance Window 🔞	02:00 - 06:00 Change			D8 Instance Type	Single				
Logs	Instance (The	alt most Onum			0		Note 1			
SQL Audits		carde carde					inat 2			
Parameters	Administrator	root Reset Password			Enterprise Project	default				
Advanced O&M	Event Scheduler 🔞				AZ	az3				
Tags										
Database Proxy	Connection Information				Connection Mar	agement	Storage Space			
	Floating IP Address	Change	Private Domain Name		- 0			50	le Configu	re Autoscaling
	VPC	default.pc	Database Port	3306 2 ③			😑 Ultra-high (/Ö 🙁 Nist encryp	pted		
	Subnet	delault_subnet ()	Recommended Max. Connections	800			Used/Wilocated 2.44/40 GB			6.1%
	Security Group	default 🖉	Read/Write Splitting Address	Apply						

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

Create Replication Instance 2 Configure Source and Destination Databases	(3) Set Task	(4) Check Task	5 Compare Parameters	(6) Confirm Task
The replication instance is created and its IP address is	. To ensure netw	ork connectivity, add this I	P address to the network whitelist	of the source database.

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.





Network Configurations

Step 1 Create a VPC peering connection.

- For details about how to create a VPC peering connection with another VPC in your account, see Creating a VPC Peering Connection with Another VPC in Your Account.
- For details about how to create a VPC peering connection with a VPC in another account, see Creating a VPC Peering Connection with a VPC in Another Account.

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.

If the source database is a Huawei Cloud RDS for MySQL database, bind and unbind an EIP by referring to **Binding and Unbinding an EIP**.

Step 2 Create a DRS task through a public network and bind an EIP to the DRS instance.

When creating a DRS task through a public network, you can bind an EIP to the DRS instance on the instance details page.

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 7-9 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 7-9 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 7-10 shows the process.





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 7-11 Replication instance information

Replication Instance De	Replication Instance Details 💿				
The following information cannot be n	nedfied after you go to the nest page.				
* Data Flow	To the cloud Out of the cloud Self-built to self-built.				
	The destination database must be a database in the current cloud. If you want to migrate data between databases, select To the cloud.				
* Source DB Engine	MySQL MySQL schema and logic table MicropiCB Reds				
* Destination D8 Engine	MySQL DDM GaussDR(for MySQL)				
* Network Type	VPW or Direct Connect.				
* Destination D8 Instance	Select an instance 👻 C Wew DB Instance Wew Unevictable DB Instance				
Replication Instance Subnet	Select the solvest				
* Migration Type	Fall-homental Fall				
	This migration type allows you to migrate data with minimal downtime. After a full migration initializes the destination database, an incremental migration parses logs to ensure data consistency between the source and destination databases.				
* Destination DB Instance Access	Read-only Read/Write				
	During the migration, the dedisation DB instance becomes read-only to ensure the integrity and success of data migration. When the task is complete, the DB instance becomes readable and writable. This process takes a few minutes. This option is recommended.				

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

Figure 7-12 Private IP address of the DRS instance

The replication instance is created and its IP address is	s 1 To ensure ne	etwork connectivity, add this	IP address to the network whitelist	of the source database.

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 7-13 Destination database information

< rds-5206	Available								🕞 Feedback	View Metric	Reboot
Basic Information	Creato Read Replica										
EPs											
Connection	D8 Information										
Management	DB Instance Name	nto-5206 🗇			D8 Instance	D		0			
Accounts	Description	-2			D8 Engine V	lersion	MySQL 8.0.2	11 Upgrade Minor Version			
Databases	Maintenance Window 🔞	02:00 - 06:00 Change			D8 Instance	Type	Single				
Logs	Instance Class	rds.mysql. Change			55L		Cer	titate <u>i</u>			
Farameters	Administrator	root. Reset Reserverd			Enterprise P	roject.	default				
Advanced O&M	Event Scheduler 🕥				AZ		az3				
Tags Database Provi	Connection Information					Connection Mar	agement.	Storage Space			
Constant Comp	Floating IP Address	Change	Private Domain Name			- 0			So	ale Configure	Autoscaling
	VPC	default_ypc	Database Fort	3306 🖉 💮				🔘 Ubra-high (/O 🙁 Not encryp	ted		
	Subnet	default_subset ()	Recommended Max. Connections	800				Used/Allocated 244/40 G8			6.19
	Security Group	telast A	Read/Write Salition Address	Andy							

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.

Scenar	io	Practice	Description
Creati ng a Task	Real- Time Migra tion	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.

Table 8-1	Common	practices
-----------	--------	-----------

Scenario	1	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.
Backu p Migra tion		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.	
	Backu o Migra tion	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.
R T S r a	Real- Time Synch roniz ation	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.
Quer Real- ying Time Task Migra Progr tion		Querying the Migration Progress	DRS shows the task progress using a progress bar, helping you keep track of the status of a task.
Progr ess	Real- Time Synch roniz ation	Querying the Synchronization Progress	
	Real- Time DR	Querying the DR Progress	
Comp aring Data	Real- Time Migra tion	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
	Real- Time Synch roniz ation	Comparing Synchronization Items	interruption duration, DRS provides multiple comparison methods.

Scenario		Practice	Description
	Real- Time DR	Comparing DR Items	
Mana ging Tasks	Real- Time Migra tion	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 Synch roniz ation	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