## **Data Replication Service**

## Preparations

 Issue
 01

 Date
 2022-09-30





HUAWEI TECHNOLOGIES CO., LTD.

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

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

### **Trademarks and Permissions**

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: https://www.huawei.com
- Email: <u>support@huawei.com</u>

## **Contents**

1 Overview	1
2 Registering a Huawei Cloud Account	2
3 Permissions Management	3
3.1 Creating a User and Granting Permissions	3
3.2 Creating a Custom Policy	4
4 From On-premises Databases to Huawei Cloud	6
4.1 Accessing Huawei Cloud over a Public Network	6
4.2 Accessing Huawei Cloud over a VPN	7
5 From Other Cloud Databases to Huawei Cloud	11
5.1 Accessing Huawei Cloud over a Public Network	11
5.2 Accessing Huawei Cloud over a VPN	12
6 From Huawei Cloud to Huawei Cloud	16
6.1 Accessing Huawei Cloud Through a VPC (Same Region and Same VPC)	
6.2 Accessing Huawei Cloud Through a VPC (Same Region and Different VPCs)	18
6.3 Accessing Huawei Cloud over a Public Network (Different Regions)	19
6.4 Accessing Huawei Cloud Through a VPN (Different Regions)	21
7 From ECS Databases to Huawei Cloud	25
7.1 Accessing Huawei Cloud Through a VPC (Same Region and Same VPC)	25
7.2 Accessing Huawei Cloud Through a VPC (Same Region and Different VPCs)	27
7.3 Accessing Huawei Cloud over a Public Network (Different Regions)	29
7.4 Accessing Huawei Cloud Through a VPN (Different Regions)	31



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

ltem	Description	Reference				
Account	Prepare a cloud account, create a user, and grant permissions to the user to use DRS.	Register a HUAWEI CLOUD account by referring to <b>Registering a Huawei Cloud</b> <b>Account</b> . Register an account by referring to <b>Permissions Management</b> .				
Databas e	Prepare the source and destination databases with required user permissions.	Different scenarios require different databases and permissions. For details, refer to the following sections:				
Networ k	The source database is deployed on a local host.	For details, see <b>From On-premises</b> Databases to Huawei Cloud.				
	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 <b>From ECS Databases to</b> Huawei Cloud.				

Table 1-1 Preparations

# **2** Registering a Huawei Cloud Account

Register a HUAWEI CLOUD account. With this account, you can use all services on HUAWEI CLOUD and only need to pay for the services you use.

Go to the HUAWEI CLOUD official website and register an account by following the instructions in Account Registration Process.

Then, you can automatically log in to HUAWEI CLOUD. You can use the cloud services only after completing real-name authentication.

# **3** Permissions Management

## 3.1 Creating a User and Granting Permissions

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

- 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 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 1.

3. Log in and verify permissions.

Log in to the management console by 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: Edit JSON policies from scratch or based on 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 the 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

[			HUAWEI CLOUD	 	 10	)Ċ		1 [		HUA CL(	WEI DUD
	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.

Replication Instance De	tails O
The following information cannot be n	nodfiled 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 database, select To the cloud.
* Source DB Engine	MySQL Oracle MySQL schema and logic table MongcOB
* Destination DB Engine	MySQL DDM GaussBelfor MySQLI Primary:Standby Edl.
* Network Type	VPN or Direct Connect
* Destination DB Instance	rds-5206-50-8
* Replication Instance Subnet	default submet   The IP address is automatically allocated but it can  User Submets  View Submets  V
* Migration Type	Full-Incernetal Full
	This migration type allows you to migrate data with minimal downtime. After a full migration initializes the destruction database, an incremental migration parses logs to ensure data consistency between the source and destruction database
* Destination D8 Instance Access	Read-only Read/Write
	Configuring the destination DB instance as read-only helps ensure the migration is successful. Once the migration is complete, the DB instance automatically changes to Read/Write.

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.

<   rds-5206-zcl-8 * (	Available							G Feedback	View Metric	Reboot	
Basic Information	Create Read Replica										
Backups & Restorations											
8Ps											
Connection	D8 Information										
Management	DB Instance Name	nto-5205-ni-4 Z 🗍			DB Instance ID		0				
Accounts	Description	-1			DB Engine Version	MySQL 80.3	1 Upgrade Minor Version				
Outabases	Maintanana Washar	0200-6600 (2000			Di Instance Tune	Cincle					
Logs	Mariballe Wildow (g)	Con-wave Gauge			on resarce type	Silve					
SQL Audits	Instance Class	rds.mysql.c2.medium   1 vCPU   2 GB Change			55.	C Cer	tfrate ±				
Parameters	Administrator	root Reset Resevend			Enterprise Project	default					
Advantari OLM	Event Scheduler (2)				AZ	83					
Taga	Connection Information				Connection Ma	ragement	Storage Space				
Catabase Proxy	Floating IP Address	r Charae	Private Domain Name					s	ale Contigu	e Autoscaling	
							Ultra-high I/O O Not encryp	ned			
	WC	default_vpc	Database Port	3308 ⊵ (I)			-				
	Subnet	default_subnet ( )	Recommended Max. Connections	800			Used(Allocated 2.44/4) G8			6.1%	
	Security Group	defects of	Desriftliche Gultition Bridense	Annie							

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" in *Getting Started with Virtual Private Network*.

**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

 		HUAWEI CLOUD	 	 	Oth	er clo	oud			HU) CL	AWEI OUD
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 address 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 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 5-6 Replication instance information

Replication Instance De	talls 💿
The following information cannot be n	nodilied after you go to the next 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 Oracle MySQL schema and logic table MongoDB
* Destination DB Engine	MySQL DDM GassDR/fbr MySQL Primary/Standby Ed
* Network Type	VPN or Direct Connect •
* Destination DB Instance	nds-5205-scl-8     View DB Instance View Unselectable DB Instance
* Replication Instance Subnet	default_sidenet The IP address is automatically allocated but it can (1) View Submets View occupied IP address
* Migration Type	Ful-Incremental Full
	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
	Configuring the destination DB instance as read-only helps ensure the migration is successful. Once the migration is complete, the DB instance automatically changes to Read/Write.

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

Figure 5-7 Private IP ad	dress of the DRS instance
--------------------------	---------------------------

() (	reate Replication Instance	- Onfigure Source and Destination Databases	(3) Set Task	(4) Check Task
	Replication instance has been created successfully	y and its private IP address is 192	Add this private IP address to the source databa	ase whitelist so that they can access 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-zcl-8 *	Available							G Feedback	View Metric	Reboot
Basic Information Backups & Restorations	Create Read Replica									
EIPs										
Connection	DB Information									
Management	DB Instance Name	nts-5206-zcl-8 🖉 👩			DB Instance ID		0			
Accounts	Description	-2			DB Engine Version	MySQL 8.0.	21 Upgrade Minor Version			
Databases	Maintenance Window (7)	0200 - 0500 Change			DR Instance Type	Single				
Logs										
SQL Audits	Instance Class	rdsmysql.c2.medium   1 vCPU   2 G8 Change			SSL	( ) (e	tificate 🛓			
Parameters	Administrator	root Reset Password			Enterprise Project	default				
Advanced O&M	Event Scheduler (2)				AZ	az3				
Taos										
Database Denes	Connection Information				Connectio	n Management	Storage Space			
Unitable Provy	Floading IP Address	Change	Private Domain Name			a		Scale	Configure	Autoscaling
	VPC	default, spc	Database Port	3306 🖉 🔞			😑 Ultra-high (/O 👩 Not encryp	ted		
	Subnet	default_subret ( )	Recommended Max. Connections	800			Used/Allocated 2,44/40 GB			6.1%
	Free alles Comme	at-2.2	Provide the Parlanese Address	Annala						

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 of the source RDS database allow the inbound traffic of the DRS replication instance, and the network ACL and security group of the DRS 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

10	reate Replication Instance	Configure Source and     Destination Databases	(3) Set Task	(4) Check Task
	Seplication instance has been created successfully	and its private IP address is 192	Add this private IP address to the source datab	ase whitelist so that they can access the source database.

**Step 2** Configure the network ACL associated with the security group and subnet of 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 the network ACL associated with the security group and subnet of the DRS 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 Huawei Cloud 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.





### **Network Configurations**

**Step 1** Create a VPC peering connection.

For details, see Virtual Private Cloud User Guide.

**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

① Create Replication Instance	Configure Source and Destination Databases	(3) Set Task	④ Check Task
Replication instance has been created s	successfully and its private IP address is 192	Add this private IP address to the source databas	e whitelist so that they can access the source database.

**Step 3** Configure the network ACL associated with the security group and subnet of 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 network ACL associated with the security group and subnet of the DRS 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

# 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 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 the network ACL associated with the security group and subnet of 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 network ACL associated with the security group and subnet of the DRS 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 in a VPN network on Huawei Cloud.



### Figure 6-10 Network diagram

If you use DRS to access a cross-region RDS database through a VPN, purchase the VPN service on Huawei Cloud in Region-B and configure the VPC and subnet where DRS resides. In addition, purchase 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

				CLOUD			
[		Region-B		Regi	on-A		
	Create a DRS task.	View the VPC information.	Buy and configure a VPN for the destination DB.	Buy and configure a VPN for the source DB.	Configure the network ACL and security group associated with the source DB.	Configure the network ACL and security group associated with the DRS instance.	Test the connection.
Re s	ecord 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.	Configure the network ACL and security group to allow traffs from DRS to the source DB in the inbound direction.	Configure the network ACL and security group to allow traffic from DRS to the source DB in the outbound direction.	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.

Replication Instance De	tails 💿
The following information cannot be m	vodiled after you go to the next page.
* Data Flow	To the cloud Out of the doud Self-built to self-built
	The distinution 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 Oracle MySQL schema and logic table MongoDB
* Destination D8 Engine	MySQL DDM GaussBillfor MySQL Primary/Standby Ed.
* Network Type	VPN or Direct Connect
* Destination DB Instance	rds-5206-ad 8
* Replication Instance Subnet	default_solvet         The IP address is automatically allocated but it can         Image: The IP address is automatically allocated but it can
* Migration Type	Ful-incenental Ful
	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
	Configuring the destination DB instance as read-only helps ensure the migration is successful. Once the migration is complete, the DB instance automatically changes to Read/Write.

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

Create Replication Instance
 Orek/Task
 Orek/Task
 Orek/Task
 Orek/Task
 Orek/Task
 Orek/Task
 Orek/Task
 Orek/Task
 Orek/Task
 Orek/Task

**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

< rds-5206-zcl-8 *	Analabie							G Feedback	Vew Metric	Reboot
Basic Information	Create Read Replica									
Backups & Restorations										
EPs										
Connection	DB Information									
Management.	DB Instance Name	nts-5206 mi 8 Z 👩			D8 Instance ID		0			
Accounts	Description	-2			Dill Engine Version	MySQL 8.0.2	1 Upgrade Minor Version			
Catabases	Maintenance Window 🛞	02:00-06:00 Change			DB Instance Type	Single				
logi	Instance Cher	of music/mulan (1)(0)(1)(2). Once			c0		three i			
SQL Audits										
Parameters	Administrator	root. Reset Resolvand			Enterprise Project	detault				
Advanced O&M	Event Scheduler 🕐				AZ.	223				
Tags										
Database Proxy	Connection Information				Connection Ma	røgerert	Storage Space			
	Floating IP Address	Change	Private Domain Name		đ			8	e Configur	e Autoscaling
	VPC	- default_spc	Database Port	3336 🖉 🕥			😑 Ultza-high I/O 🙁 Not encryg	sted		
	Subnet	default_subnet ( )	Recommended Max. Connections	800			Used(Allocated 2.44/40.68			6.1%
	Security Group	default //	Read/Write Soliting Address	Apply						

**Step 3** Purchase 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** Purchase 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 the network ACL associated with the security group and subnet of 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 network ACL associated with the security group and subnet of the DRS 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

# **7** From ECS Databases 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 Huawei Cloud 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 the network ACL associated with the security group and subnet of 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 the network ACL associated with the security group and subnet of the DRS 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 Huawei Cloud 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 Flowchart

HUAWEI CLOUD										
Create a VPC peering connection.		Create a DRS task.	Cano	onfigure the network AC I security group associat with the source DB.	L led	Configure the whitelist of the source DB.		Configure the network AC and security group associa with the DRS instance.	CL ited	Test the connection.
Create a VPC peering connection to enable communication between the two VPCs.		Record the associated subnet and the DRS private IP address.		Configure the network ACL and security group to allow traffic from DRS to the source DB in the inbound direction.		Add the private IP address of the DRS instance to the whitelist of the HUAWEI CLOUD ECS database.		Configure the network ACL and security group to allow traffic from DRS to the source DB in the outbound direction.		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 VPC peering connection.

For details, see Virtual Private Cloud User Guide.

**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 the network ACL associated with the security group and subnet of 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 the network ACL associated with the security group and subnet of the DRS 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 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

## 7.3 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 Huawei Cloud 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 of the Region-A source database to allow 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 ensure that the outbound traffic from the network ACL and security group of the DRS replication instance in Region-B is allowed. **Figure 7-8** shows the operation process.





### **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 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

1 Create Replication Instance	Configure Source and     Destination Databases	(3) Set Task	④ Check Task
The replication instance is created. Its EIP is 10	. Add this EIP to the source data	base whitelist so that it can access the source database.	

**Step 3** Configure the network ACL associated with the security group and subnet of 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 the network ACL associated with the security group and subnet of the DRS 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 Huawei Cloud database in different regions over a VPN network on Huawei Cloud.





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

Replication Instance De	tails 🗇
The following information cannot be m	odilied after you go to the next 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	Mg5QL Oracle Mg5QL schema and logic table MongoDB
* Destination DB Engine	MpSQL DDM GausiDB(for MpSQL) Primary/Standby Edl.
* Network Type	VPN or Direct Connect
* Destination DB Instance	nds-5206-ad-8
* Replication Instance Subnet	default submet   The IP address is automatically allocated but it can  View Submets View coupled IP address
* Migration Type	Full-Incremental Full
	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 database.
* Destination DB Instance Access	Read-only Read/Write
	Confliction the detilection PD instance to end while accuments the relation is supervised. Once the minimum is consolided the PD instance without its dependence to Band Matrix

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

() c	reate Replication Instance	2 Configure Source and Destination Databases	(3) Set Task	(4) Check Task
	Replication instance has been created successfully	and its private IP address is 192	Add this private IP address to the source database white	ist so that they can access 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 7-14 Destination database information	
/ Left FMS and R O contact	0.000

	105-5200-201-0 -	A NUMBER							A uterrary	View Meetro	RECORT
Bit Normation         Efficient to the set of the set o	task information	Create Read Replica									
Bill Minimum         Model Statil Minipul Minimum         Bill Mini	в										
Name     Alternation     Alternation     Alternation     Alternation       Status     August Alternation     Alternation     Alternation     Alternation       Status     August Alternation     Status     Bit Norte Alternation     Alternation       Status     August Alternation     Status Alternation     Bit Norte Alternation     Alternation       Status     August Alternation     Status Alternation     Bit Norte Alternation     Alternation       Status     August Alternation     August Alternation     Alternation     Alternation       Status     August Alternation     Alternation     Alternation     Alternation       Stat	Connection	D8 Information									
Control         Separation         Mg2L21         Style More Internation           Separation         Mg2L21         Style More Internation         Style More Internation           Separation         Mg2L21         Style More Internatinte	lanagement.	D8 Instance Name	nts-5205-mi-8 Z 🗇			DB Instance ID		0			
Statum     Statum <th>kcounts</th> <td>Description</td> <td>-2</td> <td></td> <td></td> <td>DB Engine Version</td> <td>Ny5QL 80.2</td> <td>Upgrade Minor Version</td> <td></td> <td></td> <td></td>	kcounts	Description	-2			DB Engine Version	Ny5QL 80.2	Upgrade Minor Version			
00         100 m Clim         design (1 m Clim) (2 m Clim)         10         0 m C m Clim (1 m Clim) (2 m Clim)           Audia         Avance         Avance         Encypto (1 m Clim) (2 m Clim)         Audia           Audia         Avance         Encypto (1 m Clim) (2 m Clim)         Audia         Audia           Audia         Marcel (2 m Clim) (2 m Clim)         Audia         Audia         Audia         Audia           Audia         Contraction Homation         Contraction Homation         Audia         Audia         Audia           Audia         Contraction Homation         Contraction Homation         Same (2 m Clim) (2	hatabanes	Maintenance Window 💿	0200-0600 Change			DB Instance Type	Single				
Avance or to for found or to for found or to found or	ags OL Audits	Instance Class	rds.mysql.c2.medium   1 vCPU   2 GB Change			552.	Cert	fate ±			
Open State         Open State         All         Kd           Sp         Corrector Information         Corrector Information         Space	arameters	Administrator	root. Reset Reservend			Enterprise Project	default				
Operative Homestry         Connective Homestry         Source 5 plane           More 5 P Attimes         Ø         Darpe         Proce for Attimes         Ø         See 6 Configure Attimestry           Vic         Salares for         Darpe         Darpe         Balanes for         Darpe         See 6 Configure Attimestry           Vic         Salares for         Darpe         Darpe Attimes         Ø         The high (5 to 100 mg)Rd         See 6 Configure Attimestry           Vice         Salares for         Darpe Attimes         Balanes for         Balanes for         See 6 Configure Attimestry           Vice         Salares for         Darpe Attimestry         Balanes for         Balanes for         See 6 Configure Attimestry           Vice         Salares for         Darpe Attimestry         Balanes for         Balanes for         See 6 Configure Attimestry           Vice         Salares for         Darpe Attimestry         Balanes for         Balanes for         See 6 Configure Attimestry           Vice         Salares for         Darpe Attimestry         Balanes for         See 6 Configure Attimestry         See 6 Configure Attimest	iduanced OBM	Event Scheduler 🔞				AZ	83				
Nump if Adam         Charge         Processorative         Charge Adams/a           Vic         Sadau, Ser         Sadau Ser	lags Natabase Prove	Connection Information				Connection M	rogerert	Storage Space			
UC dular (μ) backen hrt 300 gℓ 0 dular hyt () 0 Unit-hyt () Unit-hyt () 0 Unit-hyt () Unit-hyt () 0 Unit-hyt () Unit-hyt () Un		Floating IP Address	🗗 Change	Private Domain Name					5	ale Configu	e Autoscaling
Salar dalar Jahor III Indonesia Lago dalar da Indonesia dalar del Registra dalar		VPC	default_yp;	Database Port	3336 🖉 🕥			😑 Ultra-high (10 🙁 Nat encry	pted		
Security Camp debuilt 🖉 Read/Unite Splitting Address Apply		Subnet	debuit_subret ( )	Recommended Max. Connections	800			Used/Allocated 244/40 GB			6.1%
		Security Group	debuit 🖉	Read/Write Splitting Address	Apply						1

**Step 3** Purchase 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** Purchase 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 the network ACL associated with the security group and subnet of 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 the network ACL associated with the security group and subnet of the DRS 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