Storage Disaster Recovery Service

User Guide

Issue	05
Date	2021-09-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.

Security Declaration

Vulnerability

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

Contents

1 Permissions Management

1.1 Creating a User and Granting SDRS Permissions

You can use **IAM** for fine-grained permissions control on SDRS resources. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing SDRS resources.
- Grant only the permissions required for users to perform a task.
- Entrust a HUAWEI ID or a cloud service to perform efficient O&M on your SDRS resources.

If your HUAWEI ID meets your permissions requirements, you can skip this section.

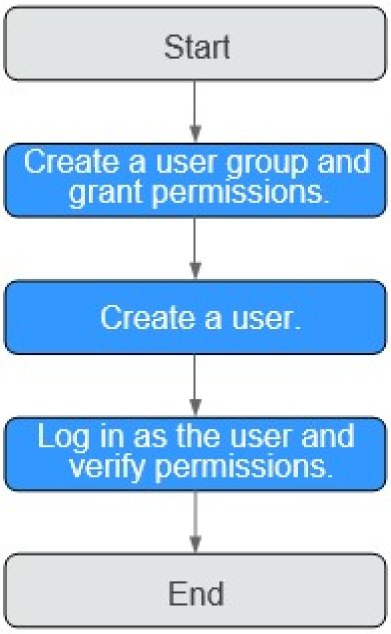
This section describes the procedure for granting permissions (see **Figure 1-1**).

Prerequisites

You have learnt about the system-defined role in **SDRS Permissions**. To grant permissions of other services, see **System Permissions**.

Process Flow

Figure 1-1 Process for granting SDRS permissions


Start
Create a user group and grant permissions.
Create a user.
Log in as the user and verify permissions.
End

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

   Create a user group on the IAM console, and attach the **SDRS Administrator** and **VPC Administrator** policies to the group.

2. **Create an IAM user and add it to the user group**.

   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 SDRS console as the created user, and verify the user's permissions for SDRS.

   – Choose **Service List** > **Storage Disaster Recovery Service**. Click **Create Protection Group** on the SDRS console. If a protection group can be successfully created, the **SDRS Administrator** policy has already taken effect.

   – Choose another service in the **Service List**. If a message appears indicating insufficient permissions to access the service, the **SDRS Administrator** policy has already taken effect.

   – Create a disaster recovery drill and select **Automatically create** for the drill VPC. If the drill is successfully created, the **VPC Administrator** policy has already taken effect.

2 Asynchronous Replication

2.1 Managing a Replica Pair

2.1.1 Creating a Replica Pair

Scenarios

You can set up the replication relationship between the production site and disaster recovery site by creating a replica pair.

Procedure

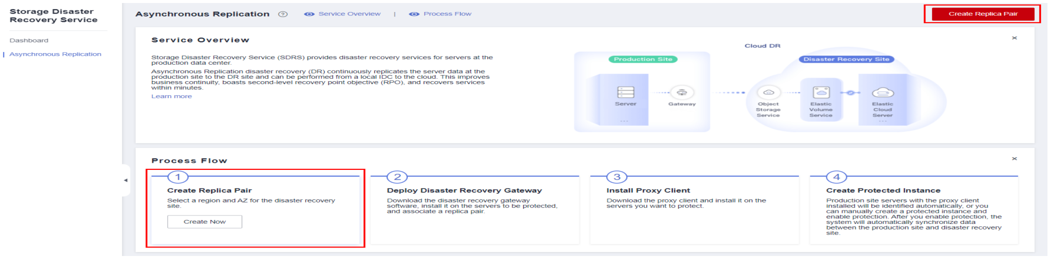
Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the upper right corner of the displayed page, click **Create Replica Pair**.

Figure 2-1 Service Overview



Service Overview

Storage Disaster Recovery Service (SDRS) provides disaster recovery services for servers at the production data center.

Asynchronous Replication disaster recovery (DR) continuously replicates the server data at the production site to the DR site and can be performed from a local IDC to the cloud. This improves business continuity, boasts second-level recovery point objective (RPO), and recovers services within minutes.

Learn more

Process Flow

1 Create Replica Pair
Select a region and AZ for the disaster recovery site.

2 Deploy Disaster Recovery Gateway
Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

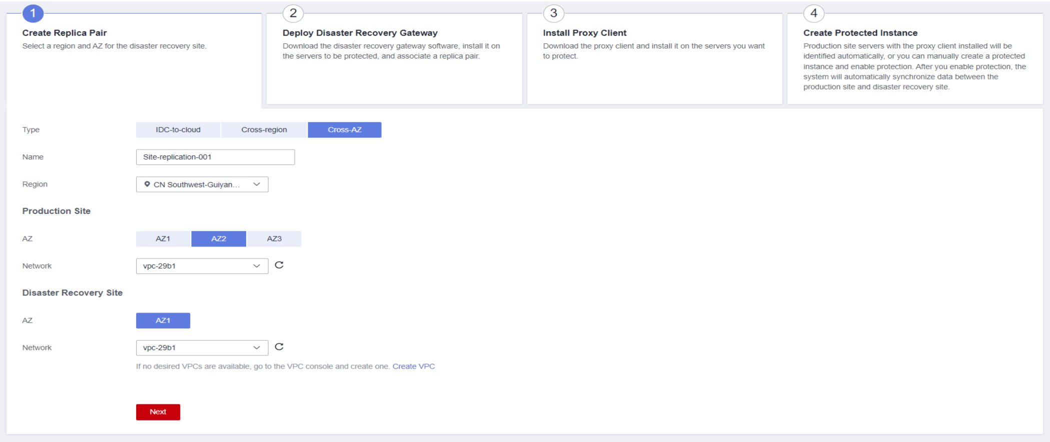
3 Install Proxy Client
Download the proxy client and install it on the servers you want to protect.

4 Create Protected Instance
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Step 4 Select the type of the replica pair you want to create and configure required parameters by referring to the following table.

1. **Cross-AZ**: The production site and disaster recovery site are located in different AZs of the same region.

Figure 2-2 Creating a cross-AZ replica pair



1 **Create Replica Pair**
Select a region and AZ for the disaster recovery site.

2 **Deploy Disaster Recovery Gateway**
Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

3 **Install Proxy Client**
Download the proxy client and install it on the servers you want to protect.

4 **Create Protected Instance**
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Type: IDC-to-cloud | Cross-region | **Cross-AZ**

Name: Site-replication-001

Region: CN Southwest-Guiyan...

Production Site

AZ: AZ1 | **AZ2** | AZ3

Network: vpc-29b1

Disaster Recovery Site

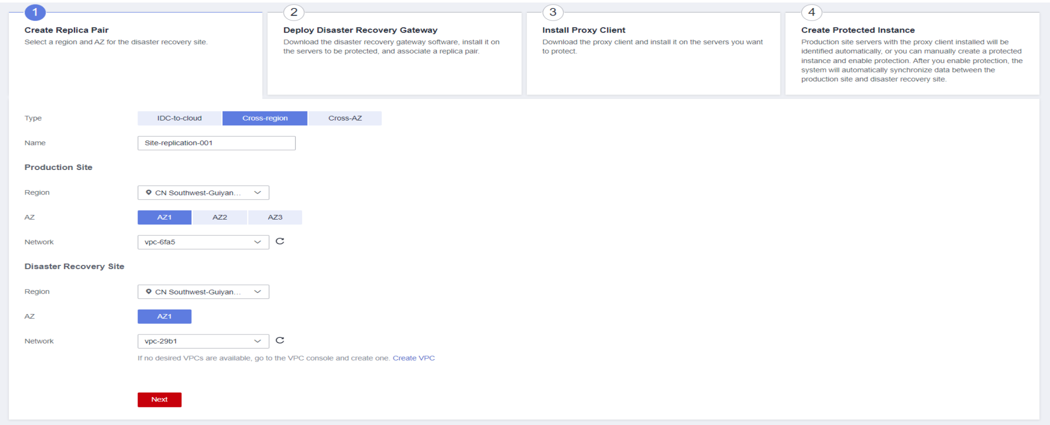
AZ: **AZ1**

Network: vpc-29b1

If no desired VPCs are available, go to the VPC console and create one. Create VPC

2. **Cross-region**: The production site and disaster recovery site are located in different regions.

Figure 2-3 Creating a cross-region replica pair



1 **Create Replica Pair**
Select a region and AZ for the disaster recovery site.

2 **Deploy Disaster Recovery Gateway**
Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

3 **Install Proxy Client**
Download the proxy client and install it on the servers you want to protect.

4 **Create Protected Instance**
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Type: IDC-to-cloud | **Cross-region** | Cross-AZ

Name: Site-replication-001

Production Site

Region: CN Southwest-Guiyan...

AZ: **AZ1** | AZ2 | AZ3

Network: vpc-6fa5

Disaster Recovery Site

Region: CN Southwest-Guiyan...

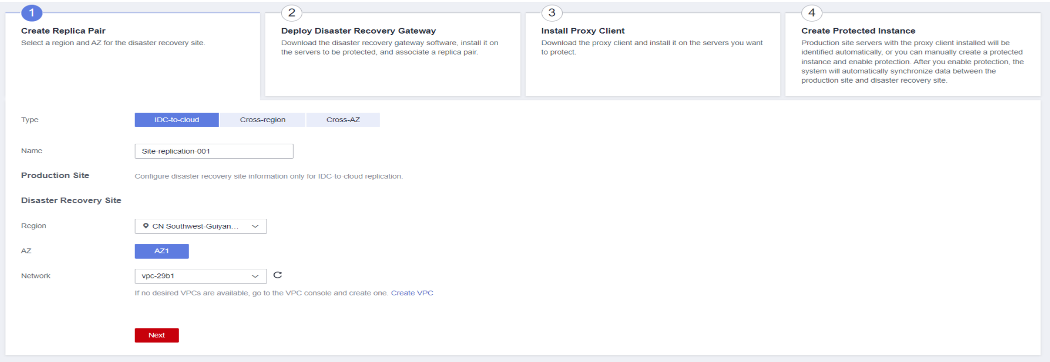
AZ: **AZ1**

Network: vpc-29b1

If no desired VPCs are available, go to the VPC console and create one. Create VPC

3. **IDC-to-cloud**: The production site is deployed in a local data center.

Figure 2-4 Create an IDC-to-cloud replica pair



1 **Create Replica Pair**
Select a region and AZ for the disaster recovery site.

2 **Deploy Disaster Recovery Gateway**
Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

3 **Install Proxy Client**
Download the proxy client and install it on the servers you want to protect.

4 **Create Protected Instance**
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Type: **IDC-to-cloud** | Cross-region | Cross-AZ

Name: Site-replication-001

Production Site: Configure disaster recovery site information only for IDC-to-cloud replication.

Disaster Recovery Site

Region: CN Southwest-Guiyan...

AZ: **AZ1**

Network: vpc-29b1

If no desired VPCs are available, go to the VPC console and create one. Create VPC

Table 2-1 Parameter description

Parameter		Description	Example Value
Type		Type of the replica pair **NOTE** **IDC-to-cloud** will be supported later.	Cross-AZ
Name		Name of the replica pair The name can contain letters, digits, underscores (_), hyphens (-), or periods (.), can be no more than 64 characters long, and cannot contain spaces.	Site-replication-001
Production Site **NOTE** You only need to configure the production site when creating a cross-region or cross-AZ replica pair.	Region	Region where the production site resides **NOTE** You only need to select a region when creating a cross-region replica pair.	-
	AZ	AZ where the production site servers reside **NOTE** You only need to select an AZ when creating a cross-region or cross-AZ replica pair.	AZ1
	Network	VPC where the production site servers reside	VPC01
Disaster Recovery Site	Region	Region where the disaster recovery site resides Select the region you selected when you set up the disaster recovery network. For details, see **Preparation: Set Up a Disaster Recovery Network on the Cloud**. **NOTE** You only need to select a region when creating an IDC-to-cloud or a cross-region replica pair.	-
	AZ	AZ where the disaster recovery site servers reside	AZ2
	Network	VPC where the disaster recovery site servers reside	VPC02

----End

2.1.2 Changing the Name of a Replica Pair

Scenarios

You can change the name of an existing replica pair.

Procedure

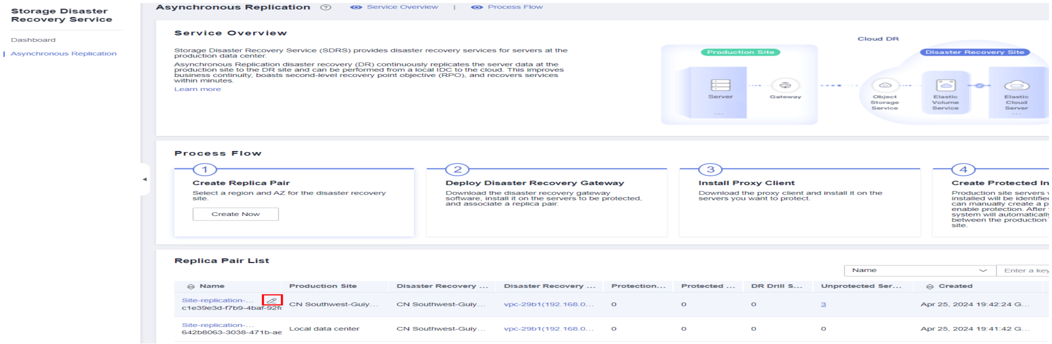
Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the replica pair list, locate the replica pair you want to change its name, and hover over its name.

Figure 2-5 Replica Pair List



Storage Disaster Recovery Service

Dashboard

Asynchronous Replication

Asynchronous Replication ⓘ Service Overview | Process Flow

Service Overview

Storage Disaster Recovery Service (SDRS) provides disaster recovery services for servers at the production data center.

Asynchronous Replication disaster recovery (DR) continuously replicates the server data at the production site to the DR site and can be performed from a local IDC to the cloud. This improves business continuity, boasts second-level recovery point objective (RPO), and recovers services within minutes.

Learn more

Process Flow

1 Create Replica Pair
Select a region and AZ for the disaster recovery site.
Create Now

2 Deploy Disaster Recovery Gateway
Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

3 Install Proxy Client
Download the proxy client and install it on the servers you want to protect.

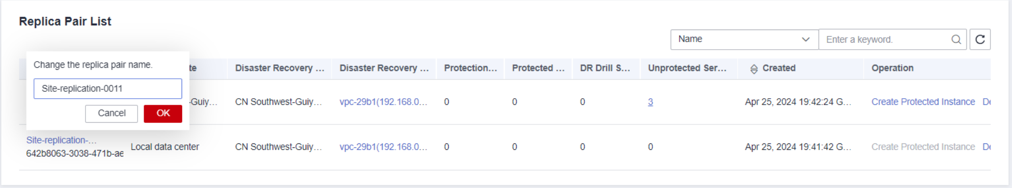
4 Create Protected In
Production site servers v installed will be identifiec can manually create a p enable protection. After system will automaticall between the production site.

Replica Pair List

Name | Enter a key

Name	Production Site	Disaster Recovery ...	Disaster Recovery ...	Protection...	Protected ...	DR Drill S...	Unprotected Ser...	Created
Site-replication-... c1e39e3d-f7b9-4baf-92fc	CN Southwest-Guiy...	CN Southwest-Guiy...	vpc-29b1(192.168.0...	0	0	0	3	Apr 25, 2024 19:42:24 G...
Site-replication-... 642b8063-3038-471b-ae	Local data center	CN Southwest-Guiy...	vpc-29b1(192.168.0...	0	0	0	0	Apr 25, 2024 19:41:42 G...

Step 4 Click the pencil icon. In the displayed dialog box, enter a new name.



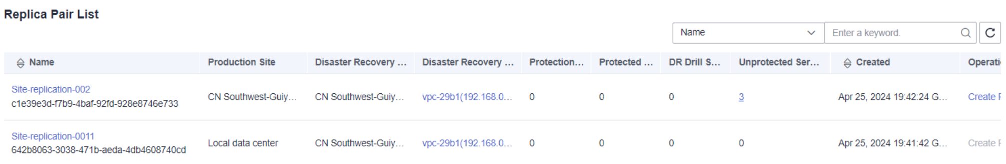
Replica Pair List

Name | Enter a keyword.

Change the replica pair name.
Site-replication-0011
Cancel OK

...te	Disaster Recovery ...	Disaster Recovery ...	Protection...	Protected ...	DR Drill S...	Unprotected Ser...	Created	Operation
-Guiy...	CN Southwest-Guiy...	vpc-29b1(192.168.0...	0	0	0	3	Apr 25, 2024 19:42:24 G...	Create Protected Instance De
Site-replication-... 642b8063-3038-471b-ae Local data center	CN Southwest-Guiy...	vpc-29b1(192.168.0...	0	0	0	0	Apr 25, 2024 19:41:42 G...	Create Protected Instance De

Step 5 Click **OK**.



Replica Pair List

Name | Enter a keyword.

Name	Production Site	Disaster Recovery ...	Disaster Recovery ...	Protection...	Protected ...	DR Drill S...	Unprotected Ser...	Created	Operati
Site-replication-002 c1e39e3d-f7b9-4baf-92fd-928e8746e733	CN Southwest-Guiy...	CN Southwest-Guiy...	vpc-29b1(192.168.0...	0	0	0	3	Apr 25, 2024 19:42:24 G...	Create F
Site-replication-0011 642b8063-3038-471b-aeda-4db4608740cd	Local data center	CN Southwest-Guiy...	vpc-29b1(192.168.0...	0	0	0	0	Apr 25, 2024 19:41:42 G...	Create F

----End

2.1.3 Deleting a Replica Pair

Scenarios

You can delete replica pairs that are no longer required to release resources.

Prerequisites

The replica pair does not contain any drill resource, protection group or protected instance.

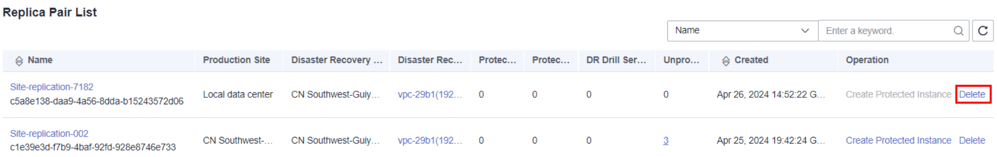
Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

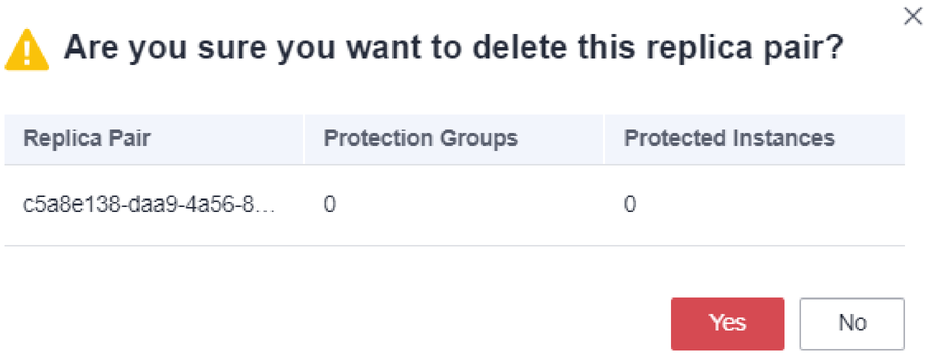
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair you want to delete and click **Delete** in the **Operation** column.



Replica Pair List

Name	Production Site	Disaster Recovery ...	Disaster Rec...	Protec...	Protec...	DR Drill Ser...	Unpro...	Created	Operation
Site-replication-7182 c5a8e138-daa9-4a56-8dda-b15243572d06	Local data center	CN Southwest-Guiy...	vpc-29b1(192...	0	0	0	0	Apr 26, 2024 14:52:22 G...	Create Protected Instance Delete
Site-replication-002 c1e39e3d-f7b9-4baf-92fd-928e8746e733	CN Southwest-...	CN Southwest-Guiy...	vpc-29b1(192...	0	0	0	3	Apr 25, 2024 19:42:24 G...	Create Protected Instance Delete

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



Are you sure you want to delete this replica pair?

Replica Pair	Protection Groups	Protected Instances
c5a8e138-daa9-4a56-8...	0	0

----End

2.2 Managing a Protection Group

2.2.1 Creating a Protection Group

Scenarios

In a replica pair, you can create a protection group and create protected instances in this group.

Procedure

Step 1 Log in to the management console.

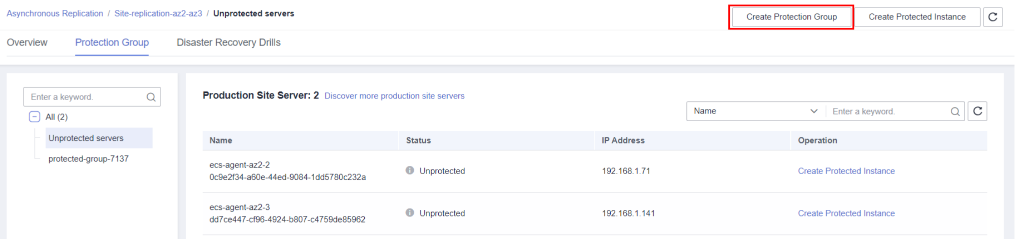
Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair in which you want to create protection groups and click the number in the **Protection Groups** column.

The **Protection Groups** tab page is displayed.

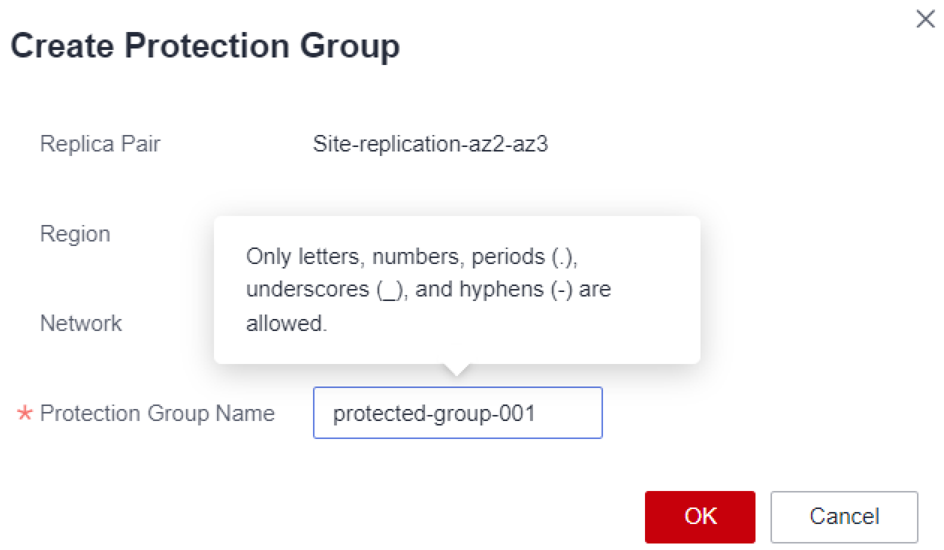
Step 4 In the upper right corner of the page, click **Create Protection Group**.



Production Site Server: 2 Discover more production site servers

Name	Status	IP Address	Operation
ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd5780c232a	Unprotected	192.168.1.71	Create Protected Instance
ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759de85962	Unprotected	192.168.1.141	Create Protected Instance

Step 5 On the displayed **Create Protection Group** page, enter a protection group name and click **OK**.



Replica Pair Site-replication-az2-az3

Region

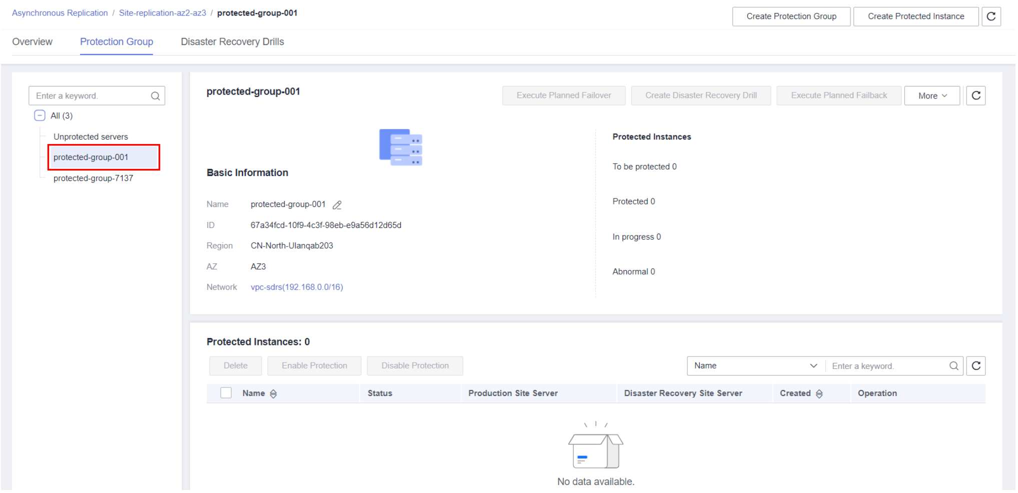
Network

Only letters, numbers, periods (.), underscores (_), and hyphens (-) are allowed.

* Protection Group Name protected-group-001

The name can contain letters, digits, underscores (_), hyphens (-), or periods (.), can be no more than 64 characters long, and cannot contain spaces.

Step 6 Manage the protection group on the **Protection Groups** tab page.



protected-group-001

Basic Information

Name	protected-group-001
ID	67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region	CN-North-Ulanqab203
AZ	AZ3
Network	vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 0

Protected 0

In progress 0

Abnormal 0

Protected Instances: 0

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation

----End

2.2.2 Enabling Protection

Scenarios

You can enable protection for all resources in a protection group.

After protection is enabled, data synchronization starts for all protected instances that meet the prerequisites in this group.

Prerequisites

- The protection group contains protected instances.
- The status of protected instances in the protection group is **Pending protection** or **Enabling protection failed**.

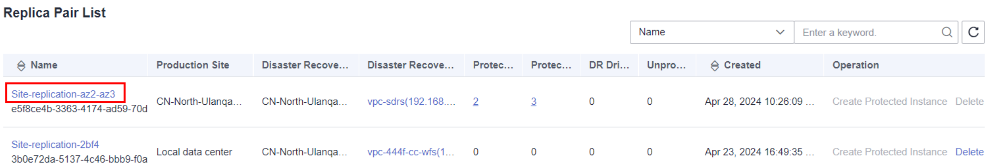
Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the replica pair list, locate the replica pair you want to operate and click its name to go to the **Overview** page.

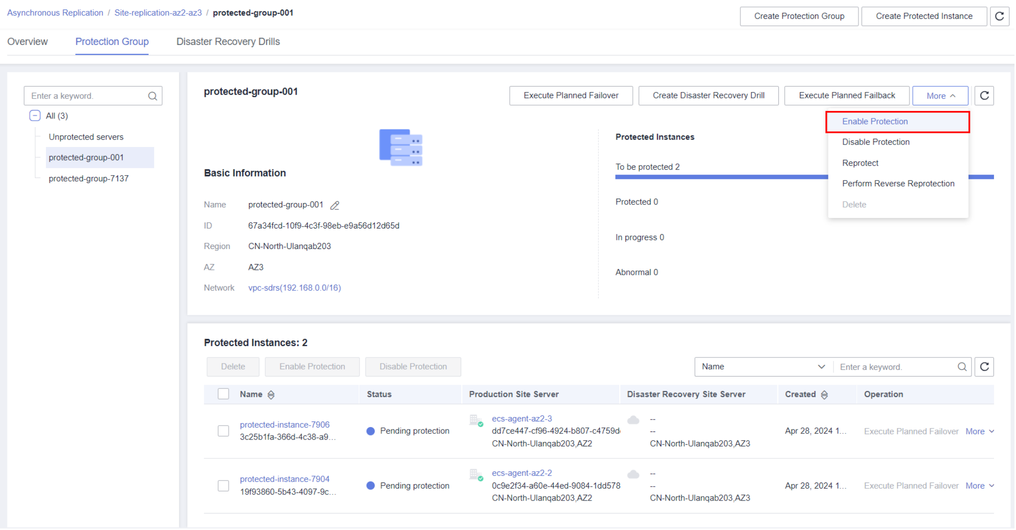


Replica Pair List

Name	Production Site	Disaster Recove...	Disaster Recove...	Protec...	Protec...	DR Dri...	Unpro...	Created	Operation
Site-replication-az2-az3 e5f8ce4b-3363-4174-ad59-70d	CN-North-Ulanqa...	CN-North-Ulanqa...	vpc-sdrs(192.168....	2	3	0	0	Apr 28, 2024 10:26:09 ...	Create Protected Instance Delete
Site-replication-2bf4 3b0e72da-5137-4c46-bbb9-f0a	Local data center	CN-North-Ulanqa...	vpc-444f-cc-wfs(1...	0	0	0	0	Apr 23, 2024 16:49:35 ...	Create Protected Instance Delete

Step 4 Click the **Protection Groups** tab and then select the desired protection group on the left to view the protection group details.

Step 5 In the upper right corner of the basic information area, choose **More** > **Enable Protection**.



protected-group-001

Basic Information

Name	protected-group-001
ID	67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region	CN-North-Ulanqab203
AZ	AZ3
Network	vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 2

Protected 0

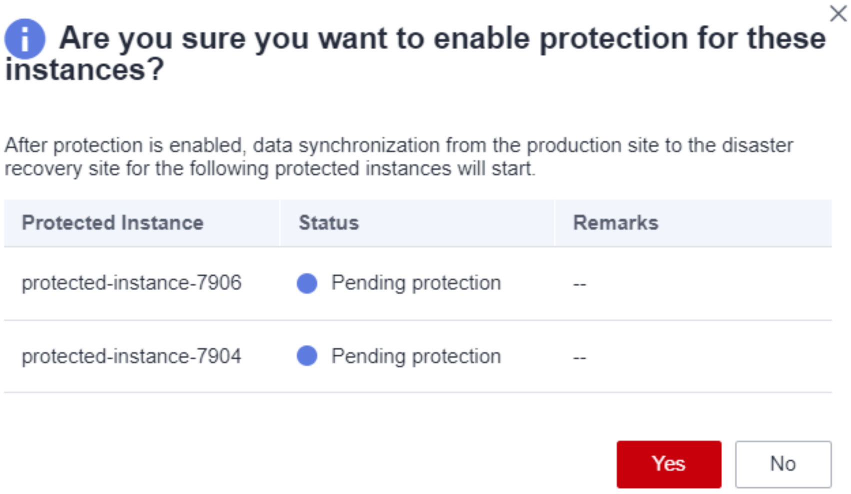
In progress 0

Abnormal 0

Protected Instances: 2

	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Pending protection	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
□	protected-instance-7904 19f93860-5b43-4097-9c...	● Pending protection	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

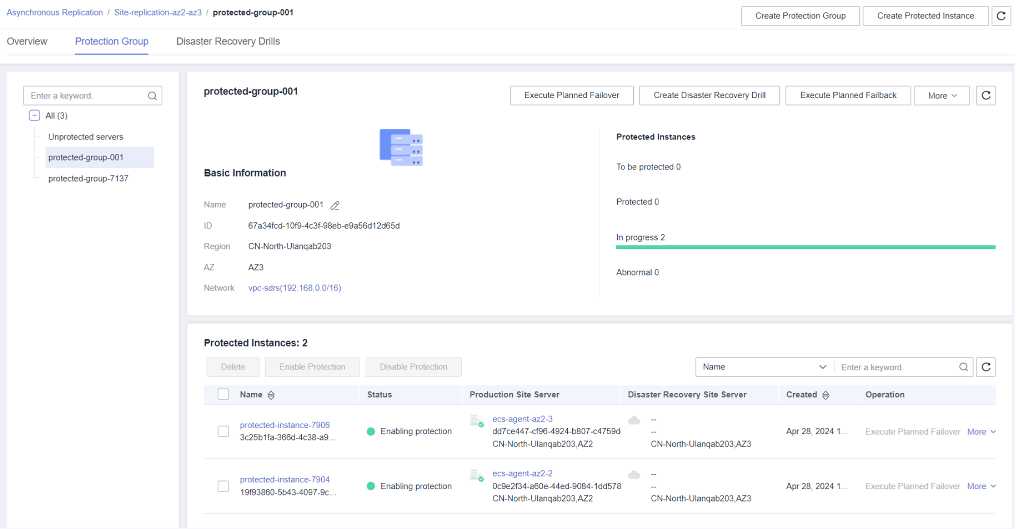
Step 6 In the displayed dialog box, confirm the protected instance information and click **Yes** to enable protection. The protected instance status changes to **Enabling protection**.



Are you sure you want to enable protection for these instances?

After protection is enabled, data synchronization from the production site to the disaster recovery site for the following protected instances will start.

Protected Instance	Status	Remarks
protected-instance-7906	● Pending protection	--
protected-instance-7904	● Pending protection	--



protected-group-001

Basic Information

Name	protected-group-001
ID	67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region	CN-North-Ulanqab203
AZ	AZ3
Network	vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 0

Protected 0

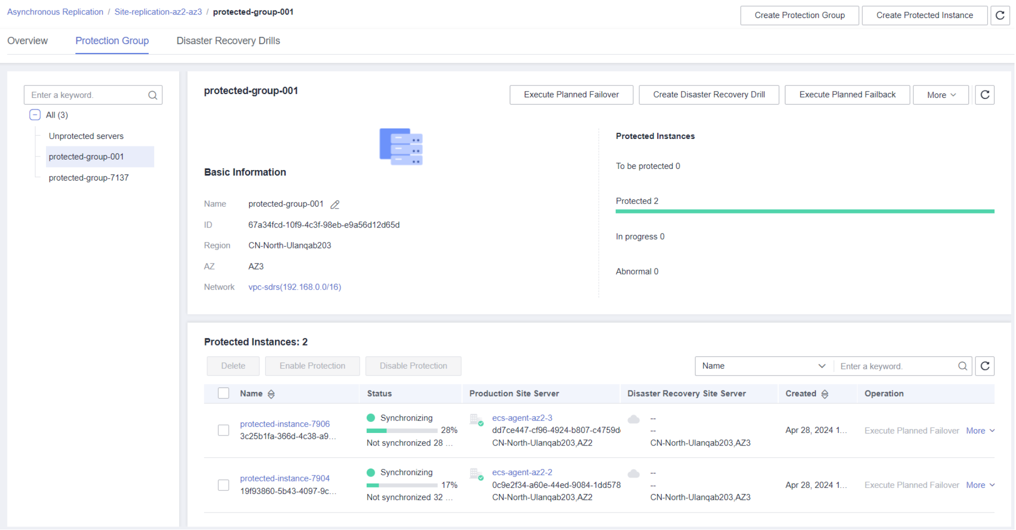
In progress 2

Abnormal 0

Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	Enabling protection	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	Enabling protection	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 7 After protection is enabled, the protected instance status changes to **Synchronizing**, indicating that differential data is being synchronized.



protected-group-001

Basic Information

Name	protected-group-001
ID	67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region	CN-North-Ulanqab203
AZ	AZ3
Network	vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 0

Protected 2

In progress 0

Abnormal 0

Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	Synchronizing 28% Not synchronized 28 ...	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	Synchronizing 17% Not synchronized 32 ...	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

NOTE

After protection is enabled, differential data is read from disks and synchronized to the disaster recovery site. During this period, the disk read bandwidth increases, and services may be affected, so you are advised to enable protection during off-peak hours.

----End

2.2.3 Disabling Protection

Scenarios

You can disable protection for all resources in a protection group.

After protection is disabled, data synchronization stops for all protected instances that meet the prerequisites in this group.

As data synchronization uses service resources (disk, CPU, and memory) and may affect production services, you can disable protection to stop data synchronization.

Prerequisites

- The protection group contains protected instances.
- The status of protected instances in the protection group is **Synchronization finished**, **Synchronizing**, or **Disabling protection failed**.
- Protected instance services are running at the production site.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

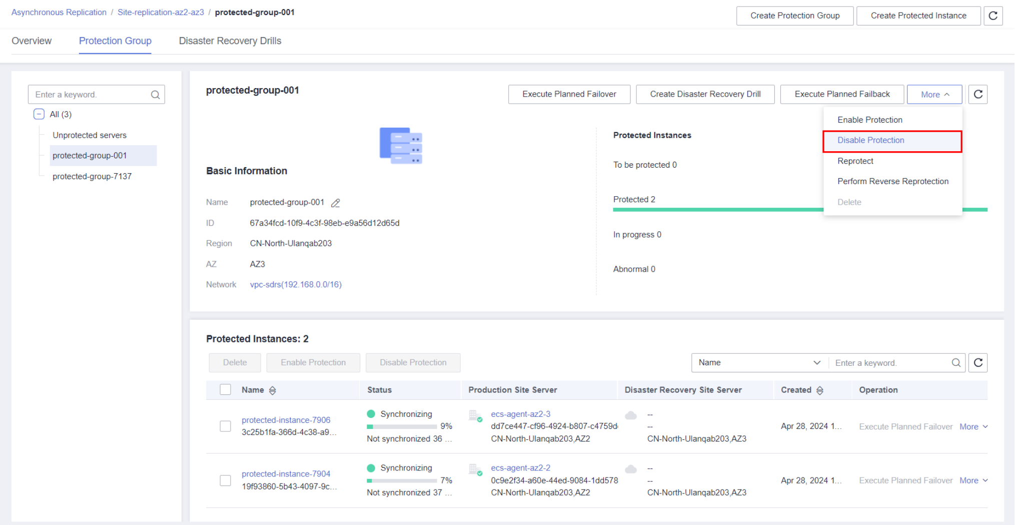
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protection group you want to disable protection and click the number in the **Protection Groups** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the upper right corner of the basic information area, choose **More** > **Disable Protection**.



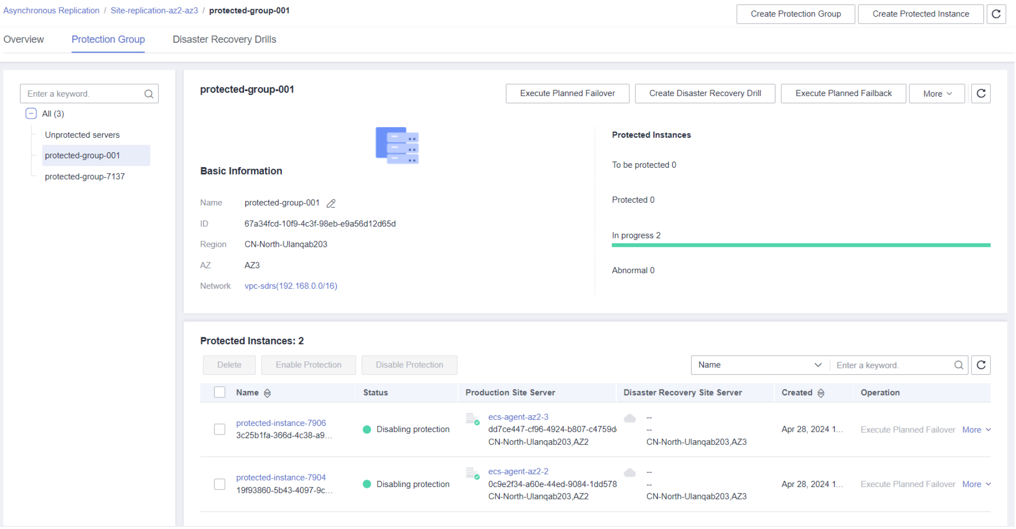
Name protected-group-001
ID 67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region CN-North-Ulanqab203
AZ AZ3
Network vpc-sdrs(192.168.0.0/16)

To be protected 0
Protected 2
In progress 0
Abnormal 0

Protected Instances: 2

☐ Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☐ protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Synchronizing 9% Not synchronized 36 ...	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
☐ protected-instance-7904 19f93860-5b43-4097-9c...	● Synchronizing 7% Not synchronized 37 ...	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 6 In the displayed dialog box, confirm the protected instance information and click **Yes** to disable protection. The protected instance status changes to **Disabling protection**.



protected-group-001

Basic Information

Name	protected-group-001
ID	67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region	CN-North-Ulanqab203
AZ	AZ3
Network	vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 0

Protected 0

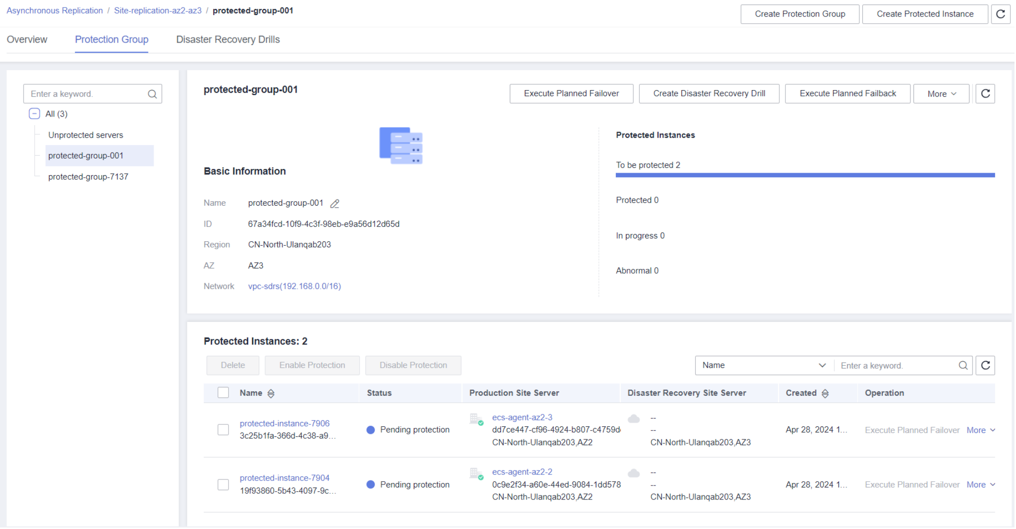
In progress 2

Abnormal 0

Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Disabling protection	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	● Disabling protection	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 7 After protection is disabled, the protected instance status changes to **Pending protection**.



protected-group-001

Basic Information

Name	protected-group-001
ID	67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region	CN-North-Ulanqab203
AZ	AZ3
Network	vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 2

Protected 0

In progress 0

Abnormal 0

Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Pending protection	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	● Pending protection	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

NOTE

After protection is disabled, the agent still records differential data.

----End

2.2.4 Performing a Failover

Scenarios

Disaster recovery site servers are created using the most current data and billed based on the server billing standards. If servers are still running during a failover, the system synchronizes all the server data before failover is performed to the disaster recovery site servers. Data written to the servers during the failover may not be synchronized to the disaster recovery site. If one of the servers to be failed over fails, data on the server may fail to be synchronized and some data may be lost.

After a failover, data is not automatically synchronized from the disaster recovery site to the production site, and protection is disabled for protected instances. To start data synchronization from the disaster recovery site to the production site, perform a reverse reprotection.

Failover is a high-risk operation. After a failover, services are started at the disaster recovery site. At this time, you must ensure that production site services are stopped. Otherwise, services may be conflicted or interrupted and data may be damaged because both sites are providing services. If you just want to verify and analyze the disaster recovery site data, perform disaster recovery drills instead.

Prerequisites

- The protection group contains protected instances.
- Initial synchronization is completed for all the protected instances in the protection group, and the status of protected instances is **Synchronization finished** or **Failover failed**.
- Protected instance services are running at the production site.
- All services on production site servers are stopped, and all data has been flushed to disks.

Precautions

During a failover, a primary NIC is configured for each disaster recovery site server. If a production site server uses a secondary NIC, you need to manually bind a secondary NIC for the corresponding disaster recovery site server on the server details page.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protection group you want to perform a failover and click the number in the **Protection Groups** column.

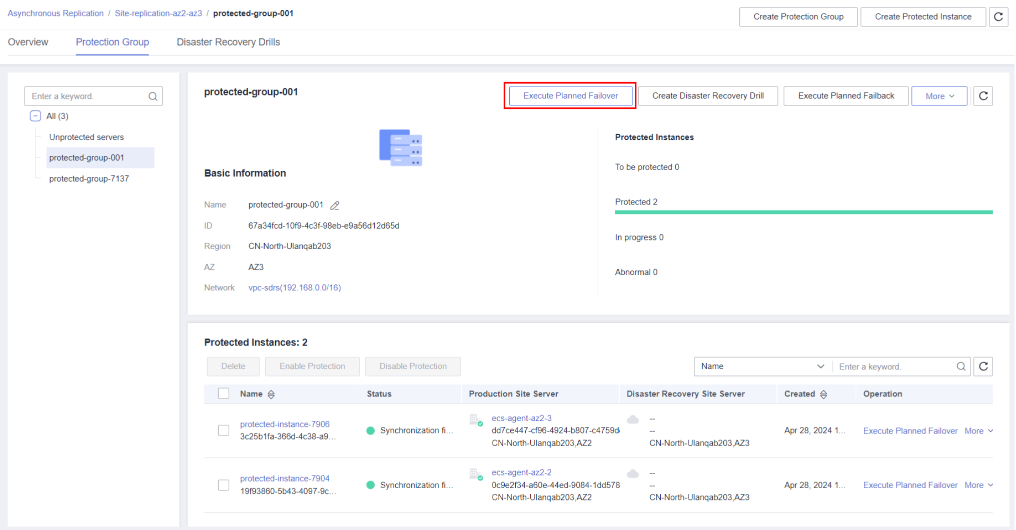
The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the upper right corner of the basic information area, click **Execute Failover**.

The **Execute Failover** page is displayed.



protected-group-001

Basic Information

Name protected-group-001
ID 67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region CN-North-Ulanqab203
AZ AZ3
Network vpc-sdrs(192.168.0.0/16)

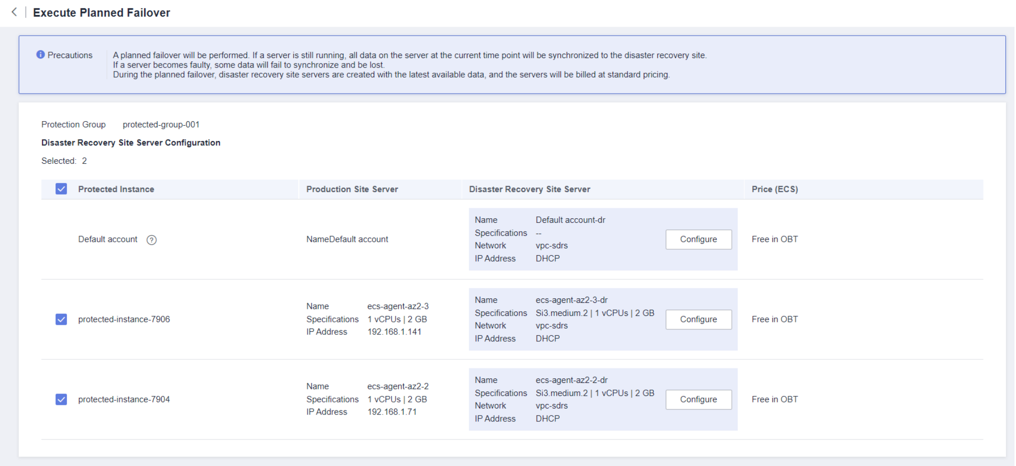
Protected Instances

To be protected 0
Protected 2
In progress 0
Abnormal 0

Protected Instances: 2

	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Synchronization fi...	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
□	protected-instance-7904 19f93860-5b43-4097-9c...	● Synchronization fi...	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 6 Configure disaster recovery site servers.



Execute Planned Failover

Precautions A planned failover will be performed. If a server is still running, all data on the server at the current time point will be synchronized to the disaster recovery site.
If a server becomes faulty, some data will fail to synchronize and be lost.
During the planned failover, disaster recovery site servers are created with the latest available data, and the servers will be billed at standard pricing.

Protection Group protected-group-001

Disaster Recovery Site Server Configuration

Selected: 2

☑ Protected Instance	Production Site Server	Disaster Recovery Site Server	Price (ECS)
Default account	NameDefault account	Name Default account-dr Specifications -- Network vpc-sdrs IP Address DHCP	Free in OBT
☑ protected-instance-7906	Name ecs-agent-az2-3 Specifications 1 vCPUs | 2 GB IP Address 192.168.1.141	Name ecs-agent-az2-3-dr Specifications Si3.medium.2 | 1 vCPUs | 2 GB Network vpc-sdrs IP Address DHCP	Free in OBT
☑ protected-instance-7904	Name ecs-agent-az2-2 Specifications 1 vCPUs | 2 GB IP Address 192.168.1.71	Name ecs-agent-az2-2-dr Specifications Si3.medium.2 | 1 vCPUs | 2 GB Network vpc-sdrs IP Address DHCP	Free in OBT

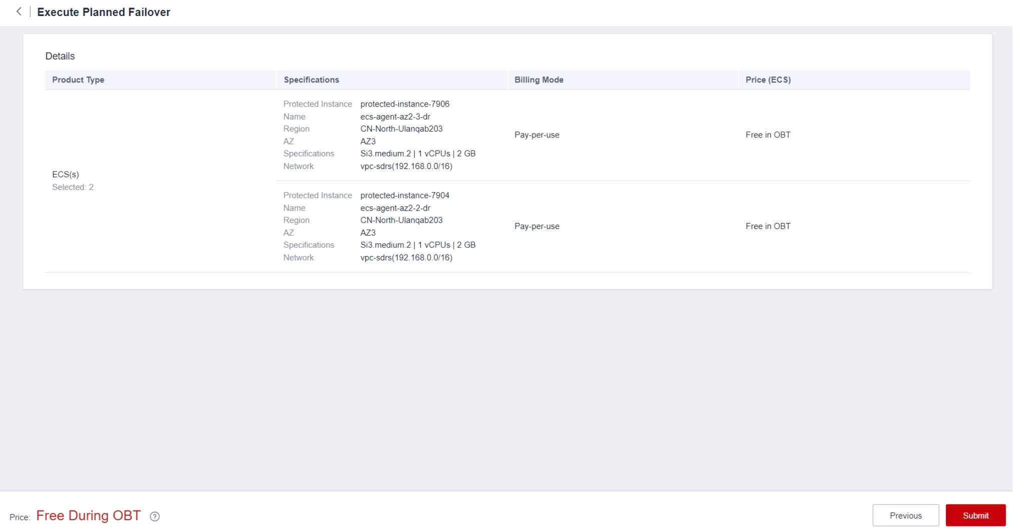
Table 2-2 Parameter description

Parameter	Description	Example Value
Protected Instance	Select the protected instances you want to execute a failover.	-

Parameter	Description	Example Value
Disaster Recovery Site Server	Configure the disaster recovery site server information. ● **Specifications**: Select the server specifications. ● **Name**: Enter a server name. The name can contain letters, digits, underscores (_), hyphens (-), or periods (.), can be no more than 64 characters long, and cannot contain spaces. ● **Subnet**: Select the subnet where the server resides. ● **IP Address**: Select how the server obtains an IP address. – **Use existing**: Select this option if the subnet selected is in the same CIDR Block as the production site server. This setting keeps the IP addresses on both servers consistent. – **DHCP**: IP addresses are automatically assigned by the system. – **Manually Assign**: Manually specify an IP address. NOTE If disaster recovery site servers are configured in a batch, only **DHCP** is available. If disaster recovery site servers are configured individually, all options are available.	-

Step 7 Click **Next**.

Step 8 Confirm the disaster recovery site server information and click **Submit**.



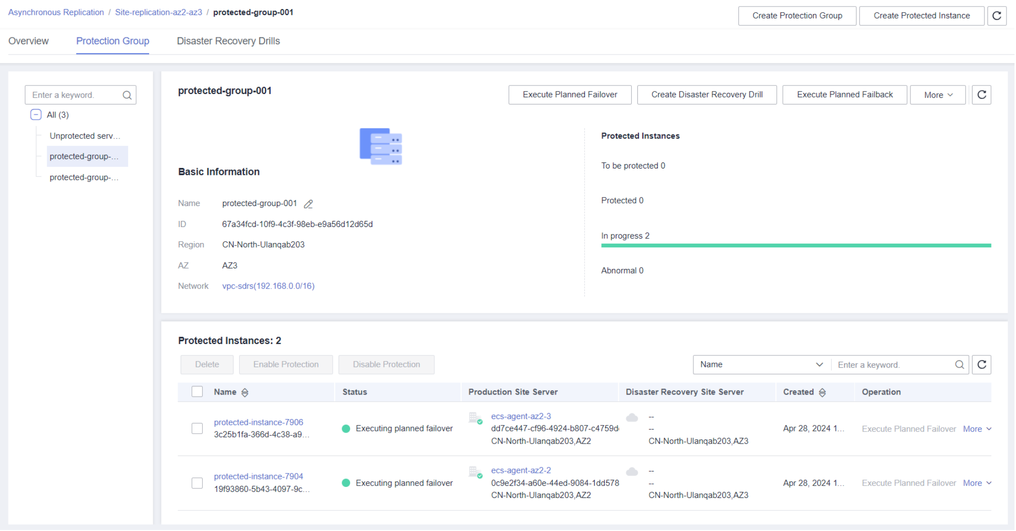
Execute Planned Failover

Details

Product Type	Specifications	Billing Mode	Price (ECS)
ECS(s) Selected: 2	Protected Instance protected-instance-7906 Name ecs-agent-az2-3-dr Region CN-North-Ulanqab203 AZ AZ3 Specifications Si3.medium.2 | 1 vCPUs | 2 GB Network vpc-sdrs(192.168.0.0/16)	Pay-per-use	Free in OBT
	Protected Instance protected-instance-7904 Name ecs-agent-az2-2-dr Region CN-North-Ulanqab203 AZ AZ3 Specifications Si3.medium.2 | 1 vCPUs | 2 GB Network vpc-sdrs(192.168.0.0/16)	Pay-per-use	Free in OBT

Price: Free During OBT

Step 9 The protected instance status changes to **Executing failover**. After the failover is complete, the status changes to **Failover completed**.



Asynchronous Replication / Site-replication-az2-az3 / protected-group-001

Overview | Protection Group | Disaster Recovery Drills

protected-group-001

Basic Information

Name	protected-group-001
ID	67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region	CN-North-Ulanqab203
AZ	AZ3
Network	vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 0

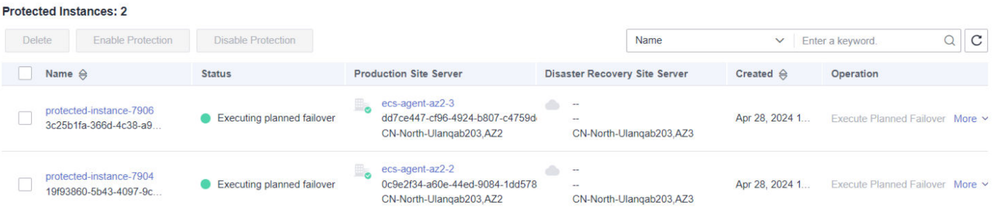
Protected 0

In progress 2

Abnormal 0

Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	Executing planned failover	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	Executing planned failover	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More



Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	Executing planned failover	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	Executing planned failover	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

----End

2.2.5 Performing a Reverse Reprotection

Scenarios

After a failover, data is not automatically synchronized from the disaster recovery site to the production site, and protection is disabled for protected instances. To start data synchronization from the disaster recovery site to the production site, perform a reverse reprotection.

NOTE

- After you perform a reverse reprotection, the initial data synchronization starts. During this process, if disaster recovery site servers are restarted, data will be resynchronized until the synchronization is complete.
- During a reverse reprotection, production site servers are stopped.
- Reverse reprotection overwrites data of production site servers with data of disaster recovery site servers. If there is data written to production site servers after the failover is performed, such data will be overwritten.

Prerequisites

- Disaster recovery site servers have been preconfigured according to **Configuring Disaster Recovery Site Servers**.
- The status of protected instances in the protection group is **Failover completed** or **Reverse reprotection failed**.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protection group you want to perform reverse reprotection and click the number in the **Protection Groups** column.

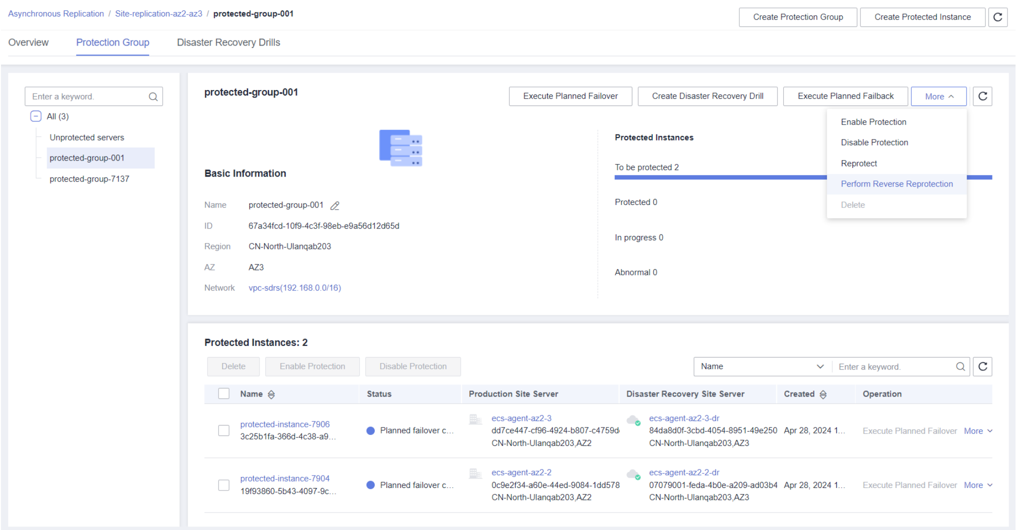
The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the upper right corner of the basic information area, choose **More** > **Perform Reverse Reprotection**.

The **Perform Reverse Reprotection** page is displayed.



Asynchronous Replication / Site-replication-az2-az3 / protected-group-001

protected-group-001

Basic Information

Name protected-group-001

ID 67a34fcd-10f9-4c3f-98eb-e9a56d12d65d

Region CN-North-Ulanqab203

AZ AZ3

Network vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 2

Protected 0

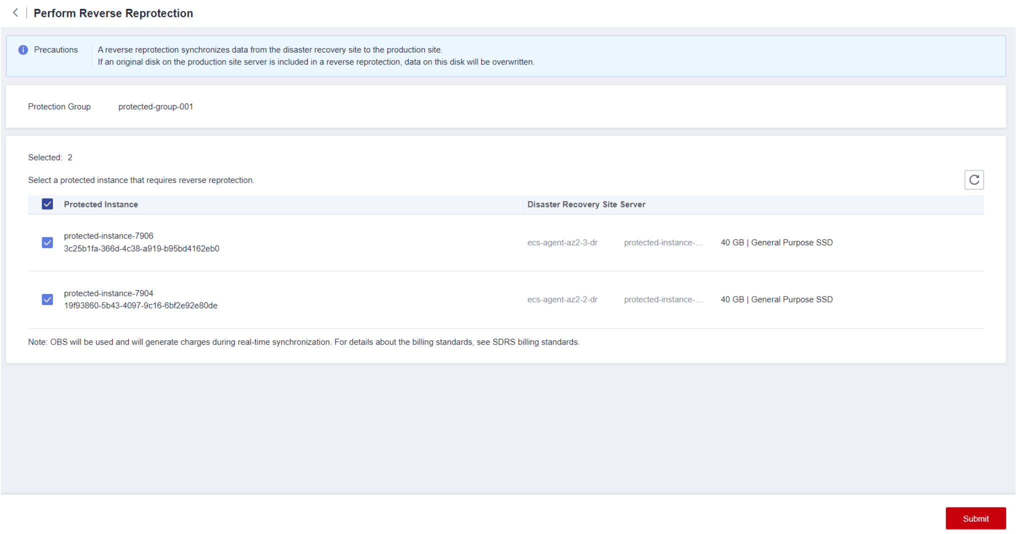
In progress 0

Abnormal 0

Protected Instances: 2

☐	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☐	protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Planned failover c...	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	ecs-agent-az2-3-dr 84da8d0f-3cbd-4054-8951-49e250 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
☐	protected-instance-7904 19f93860-5b43-4097-9c...	● Planned failover c...	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	ecs-agent-az2-2-dr 07079001-feda-4b0e-a209-ad03b4 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 6 Select the protected instances to be reprotected.



Perform Reverse Reprotection

Precautions A reverse reprotection synchronizes data from the disaster recovery site to the production site.
If an original disk on the production site server is included in a reverse reprotection, data on this disk will be overwritten.

Protection Group protected-group-001

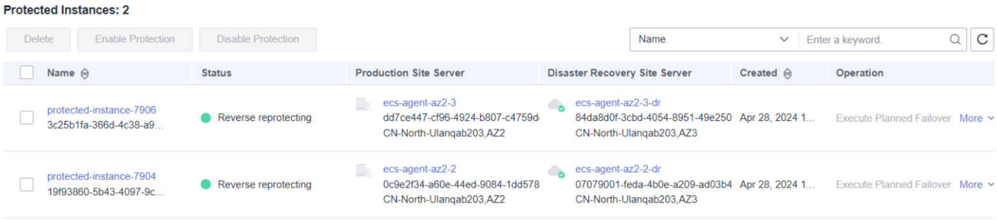
Selected: 2

Select a protected instance that requires reverse reprotection.

☑	Protected Instance	Disaster Recovery Site Server		
☑	protected-instance-7906 3c25b1fa-366d-4c38-a919-b95bd4162eb0	ecs-agent-az2-3-dr	protected-instance-...	40 GB | General Purpose SSD
☑	protected-instance-7904 19f93860-5b43-4097-9c16-6bf2e92e80de	ecs-agent-az2-2-dr	protected-instance-...	40 GB | General Purpose SSD

Note: OBS will be used and will generate charges during real-time synchronization. For details about the billing standards, see SDRS billing standards.

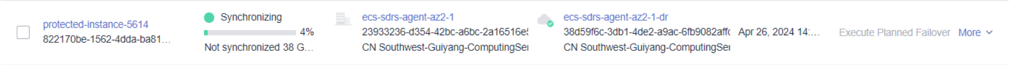
Step 7 Click **Submit**. The protected instance status changes to **Reverse reprotecting**.



Protected Instances: 2

□	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Reverse reprotecting	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	ecs-agent-az2-3-dr 84da8d0f-3cbd-4054-8951-49e250 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
□	protected-instance-7904 19f93860-5b43-4097-9c...	● Reverse reprotecting	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	ecs-agent-az2-2-dr 07079001-feda-4b0e-a209-ad03b4 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 8 After 1 to 2 minutes, the protected instance status changes to **Synchronizing**, and the amount of data to be synchronized and estimated remaining time are displayed.



□	protected-instance-5614 822170be-1562-4dda-ba81...	● Synchronizing 4% Not synchronized 38 G...	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

----End

2.2.6 Performing a Failback

Scenarios

After a failover, services are running at the disaster recovery site. You can fail back to your production site with a failback.

Failback is a high-risk operation. After a failback, services are started at the production site. At this time, you must ensure that disaster recovery site services are stopped. Otherwise, services may be conflicted or interrupted and data may be damaged because both sites are providing services.

Prerequisites

- Reverse reprotection is completed for all the protected instances in the protection group, and the status of protected instances is **Synchronization finished** or **Failback failed**.
- Protected instance services are running at the disaster recovery site.
- All services on disaster recovery site servers are stopped, and all data has been flushed to disks.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protection group you want to perform a failback and click the number in the **Protection Groups** column.

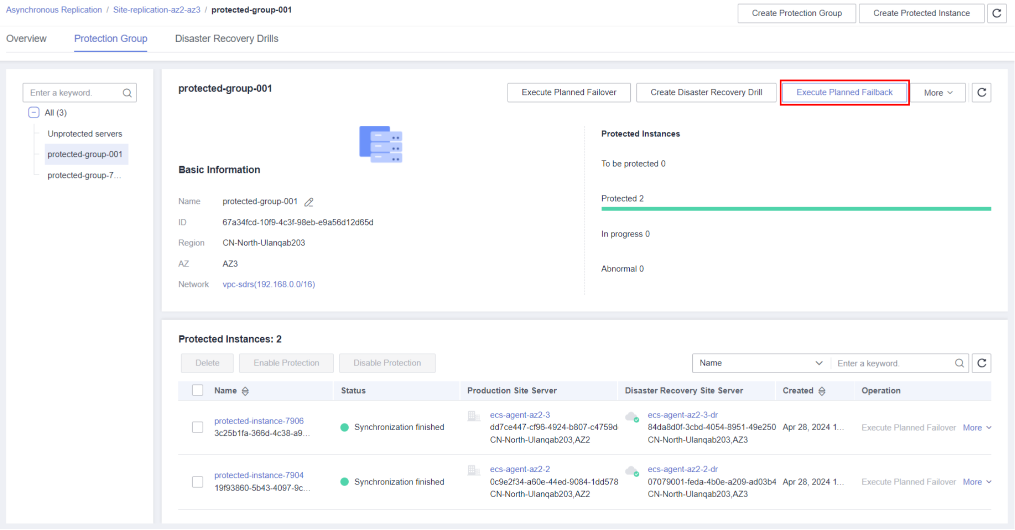
The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the upper right corner of the basic information area, click **Execute Failback**.

The **Execute Failback** page is displayed.



protected-group-001

Basic Information

Name	protected-group-001
ID	67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region	CN-North-Ulanqab203
AZ	AZ3
Network	vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 0

Protected 2

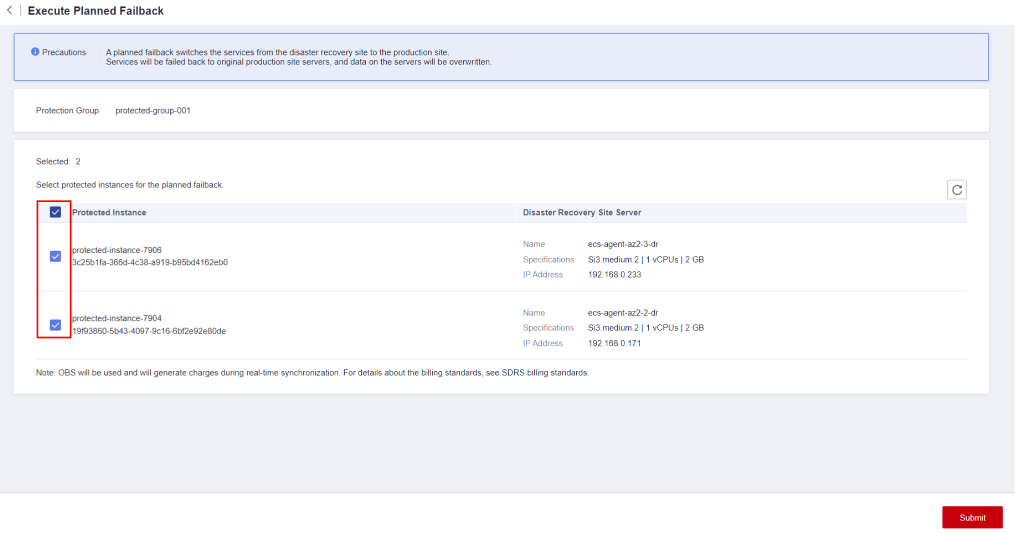
In progress 0

Abnormal 0

Protected Instances: 2

☐	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☐	protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Synchronization finished	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	ecs-agent-az2-3-dr 84da8d0f-3cbd-4054-8951-49e250 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
☐	protected-instance-7904 19f93860-5b43-4097-9c...	● Synchronization finished	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	ecs-agent-az2-2-dr 07079001-feda-4b0e-a209-ad03b4 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 6 Select protected instances and click **Submit**.



Execute Planned Failback

Precautions A planned failback switches the services from the disaster recovery site to the production site.
Services will be failed back to original production site servers, and data on the servers will be overwritten.

Protection Group protected-group-001

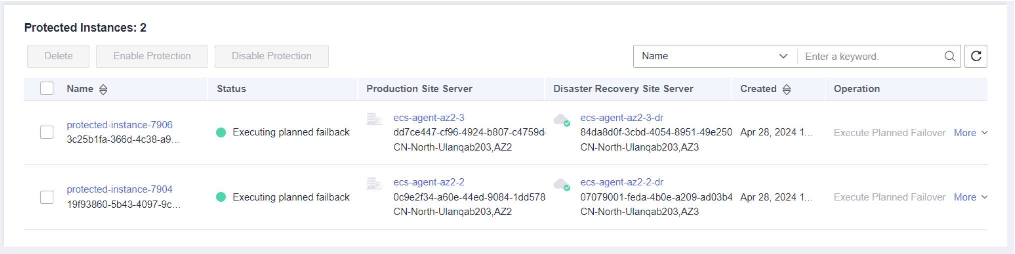
Selected: 2

Select protected instances for the planned failback.

☑	Protected Instance	Disaster Recovery Site Server
☑	protected-instance-7906 3c25b1fa-366d-4c38-a919-b95bd4162eb0	Name ecs-agent-az2-3-dr Specifications Si3.medium.2 | 1 vCPUs | 2 GB IP Address 192.168.0.233
☑	protected-instance-7904 19f93860-5b43-4097-9c16-6bf2e92e80de	Name ecs-agent-az2-2-dr Specifications Si3.medium.2 | 1 vCPUs | 2 GB IP Address 192.168.0.171

Note: OBS will be used and will generate charges during real-time synchronization. For details about the billing standards, see SDRS billing standards.

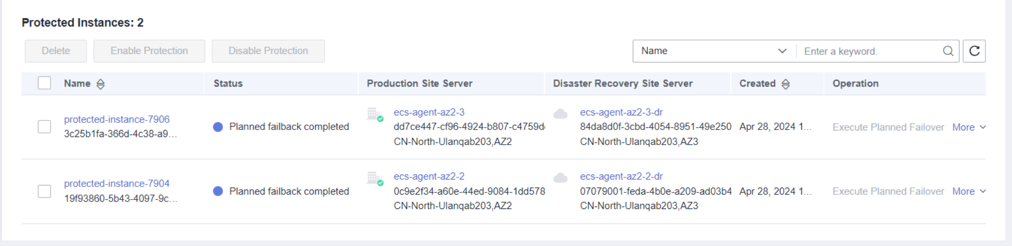
Step 7 The protected instance status changes to **Executing failback**.



Protected Instances: 2

☐	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☐	protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Executing planned failback	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	ecs-agent-az2-3-dr 84da8d0f-3cbd-4054-8951-49e250 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
☐	protected-instance-7904 19f93860-5b43-4097-9c...	● Executing planned failback	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	ecs-agent-az2-2-dr 07079001-feda-4b0e-a209-ad03b4 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 8 After the protected instance status changes to **Failback completed**, the operation is successful.



Protected Instances: 2

☐ Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☐ protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Planned failback completed	ecs-agent-az2-3 dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	ecs-agent-az2-3-dr 84da8d0f-3cbd-4054-8951-49e250 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
☐ protected-instance-7904 19f93860-5b43-4097-9c...	● Planned failback completed	ecs-agent-az2-2 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	ecs-agent-az2-2-dr 07079001-feda-4b0e-a209-ad03b4 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

----End

2.2.7 Reprotecting a Protection Group

Scenarios

After a failback, data is not automatically synchronized from the production site to the disaster recovery site, and protection is disabled for protected instances. To start data synchronization from the production site to the disaster recovery site, reprotect the protection group.

Prerequisites

- Production site servers have been preconfigured according to **Configuring Production Site Servers**.
- The status of protected instances in the protection group is **Failback completed** or **Reprotection failed**.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

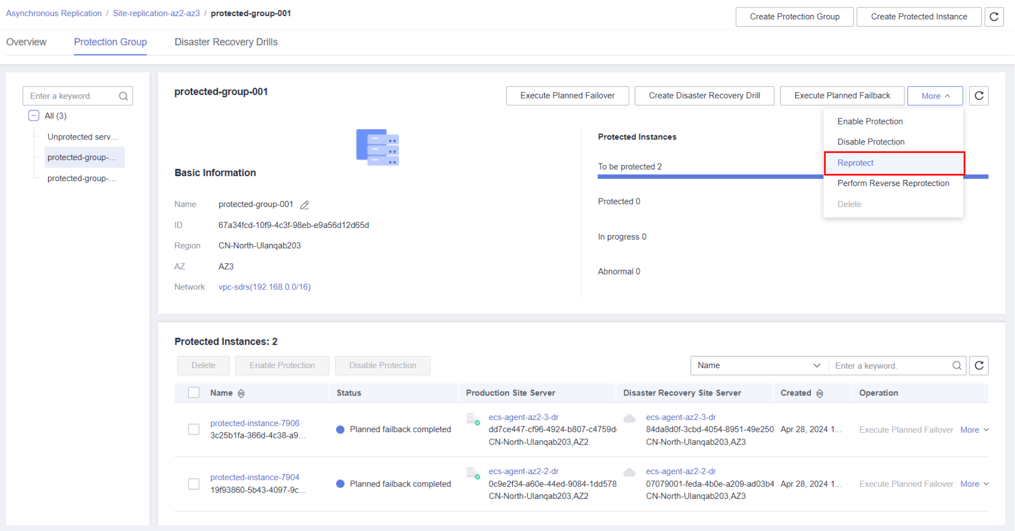
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protection group you want to reprotect and click the number in the **Protection Groups** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the upper right corner of the basic information area, choose **More** > **Reprotect**.



Asynchronous Replication / Site-replication-az2-az3 / protected-group-001

protected-group-001

Basic Information

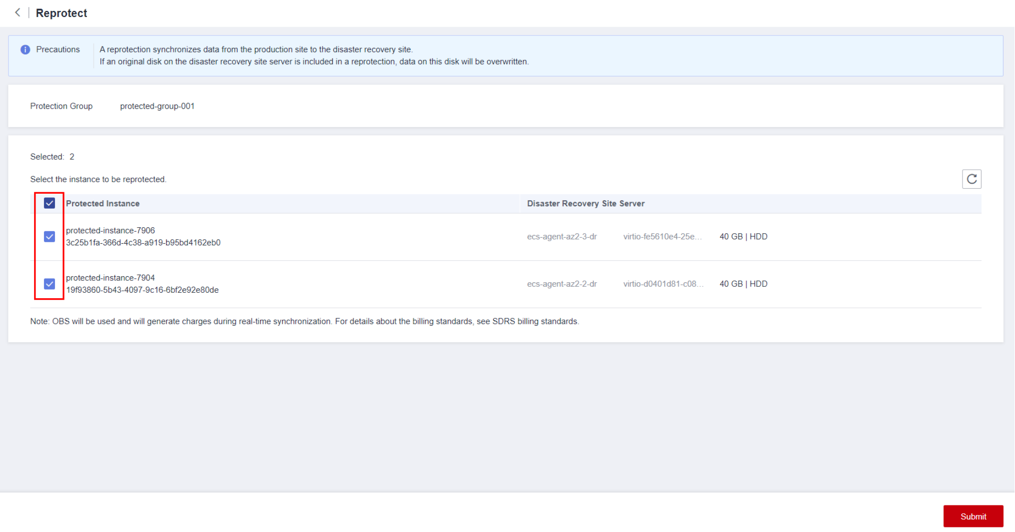
Name protected-group-001
ID 67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region CN-North-Ulanqab203
AZ AZ3
Network vpc-sdrs(192.168.0.0/16)

Protected Instances
To be protected 2
Protected 0
In progress 0
Abnormal 0

Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Planned failback completed	ecs-agent-az2-3-dr dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	ecs-agent-az2-3-dr 84da8d0f-3cbd-4054-8951-49e250 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	● Planned failback completed	ecs-agent-az2-2-dr 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	ecs-agent-az2-2-dr 07079001-feda-4b0e-a209-ad03b4 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 6 Select protected instances and click **Submit**.



Reprotect

Precautions A reprotection synchronizes data from the production site to the disaster recovery site.
If an original disk on the disaster recovery site server is included in a reprotection, data on this disk will be overwritten.

Protection Group protected-group-001

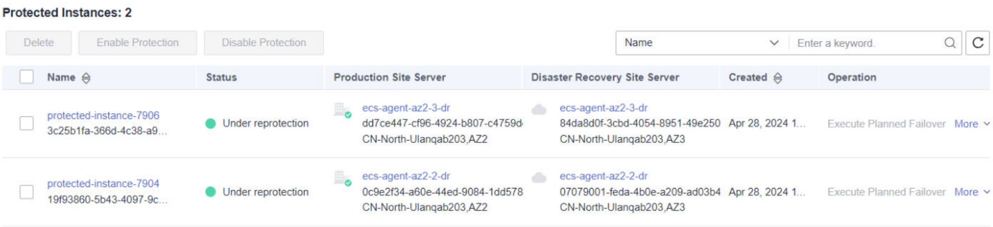
Selected: 2

Select the instance to be reprotected.

☑ Protected Instance	Disaster Recovery Site Server		
☑ protected-instance-7906 3c25b1fa-366d-4c38-a919-b95bd4162eb0	ecs-agent-az2-3-dr	virtio-fe5610e4-25e...	40 GB | HDD
☑ protected-instance-7904 19f93860-5b43-4097-9c16-6bf2e92e80de	ecs-agent-az2-2-dr	virtio-d0401d81-c08...	40 GB | HDD

Note: OBS will be used and will generate charges during real-time synchronization. For details about the billing standards, see SDRS billing standards.

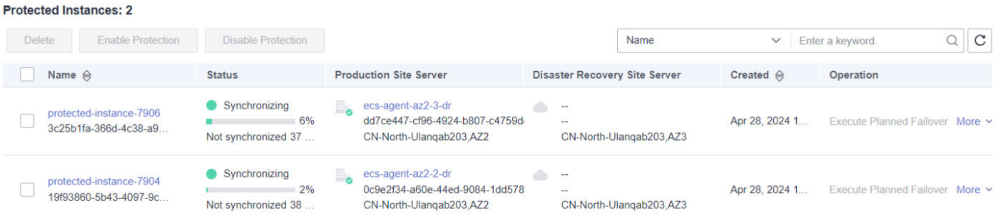
Step 7 The protected instance status changes to **Under reprotection**. Wait until the operation is complete.



Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Under reprotection	ecs-agent-az2-3-dr dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	ecs-agent-az2-3-dr 84da8d0f-3cbd-4054-8951-49e250 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	● Under reprotection	ecs-agent-az2-2-dr 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	ecs-agent-az2-2-dr 07079001-feda-4b0e-a209-ad03b4 CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 8 After the operation is complete, the protected instance status changes to **Synchronizing**, and the amount of data to be synchronized and estimated remaining time are displayed.



Protected Instances: 2

□ Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□ protected-instance-7906 3c25b1fa-366d-4c38-a9...	● Synchronizing 6% Not synchronized 37 ...	ecs-agent-az2-3-dr dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
□ protected-instance-7904 19f93860-5b43-4097-9c...	● Synchronizing 2% Not synchronized 38 ...	ecs-agent-az2-2-dr 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

NOTE

After the failback is successful, disaster recovery site servers will be automatically deleted.

----End

2.2.8 Creating a Disaster Recovery Drill

Scenarios

Disaster recovery drills are used to simulate fault scenarios, formulate recovery plans, and verify whether the plans are applicable and effective. Services are not affected during disaster recovery drills. When a fault occurs, you can use the plans to quickly recover services, thus improving service continuity.

SDRS allows you to run disaster recovery drills in isolated VPCs (different from the disaster recovery site VPC). During a disaster recovery drill, drill servers can be quickly created based on the disk snapshot data.

NOTE

After drill servers are created, production site servers and drill servers will independently run at the same time, and data will not be synchronized between these servers.

To guarantee that services can be switched to the disaster recovery site when an outage occurs, it is recommended that you run disaster recovery drills regularly.

Precautions

- If the production site servers of a protection group are added to an enterprise project, the drill servers created will not be automatically added to the enterprise project. Manually add them to the project as needed.
- If the production site servers run Linux and use key pairs for login, the key pair information will not be displayed on the server details page, but login using the key pairs is not affected.
- After a disaster recovery drill is created, modifications made to **Hostname**, **Name**, **Agency**, **ECS Group**, **Security Group**, **Tags**, and **Auto Recovery** of production site servers will not be synchronized to drill servers. Log in to the console and manually make the modifications for the drill servers.
- During a disaster recovery drill, a primary NIC is configured for each disaster recovery site server. If a production site server uses a secondary NIC, you need to manually bind a secondary NIC for the corresponding disaster recovery site server on the server details page.

Prerequisites

- Initial synchronization is completed for all the protected instances in the protection group, and the status of protected instances is **Synchronization finished** or **Disaster recovery drill failed**.
- Protected instance services are running at the production site.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protection group you want to run a disaster recovery drill and click the number in the **Protection Groups** column.

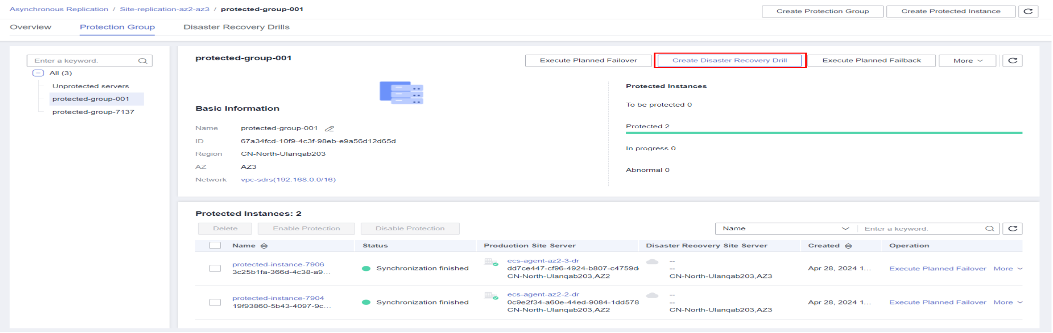
The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the upper right corner of the basic information area, click **Create Disaster Recover Drill**.

Figure 2-6 Protection group drill entry



protected-group-001

Basic Information

Name protected-group-001
ID 67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region CN-North-Ulanqab203
AZ AZ3
Network vpc-sdrs(192.168.0.0/16)

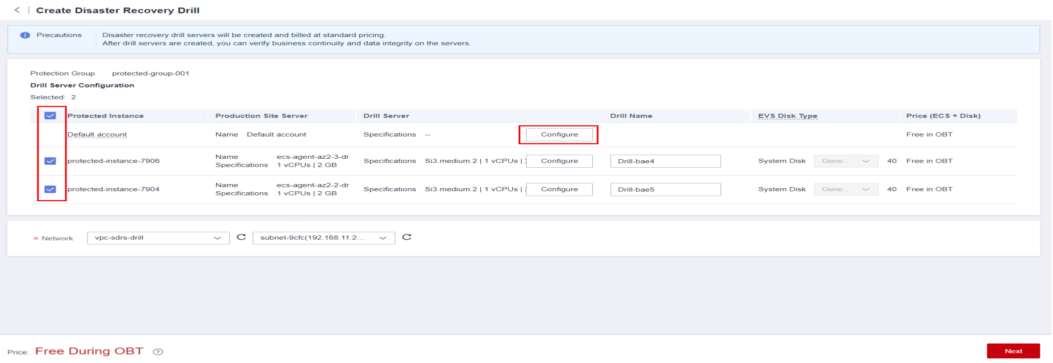
Protected Instances
To be protected 0
Protected 2
In progress 0
Abnormal 0

Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	Synchronization finished	ecs-agent-az2-3-dr dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	Synchronization finished	ecs-agent-az2-2-dr 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

Step 6 Configure drill servers.

Figure 2-7 Configuring drill server specifications in a batch



Create Disaster Recovery Drill

Precautions Disaster recovery drill servers will be created and billed at standard pricing.
After drill servers are created, you can verify business continuity and data integrity on the servers.

Protection Group protected-group-001

Drill Server Configuration

Selected: 2

☑	Protected Instance	Production Site Server	Drill Server	Drill Name	EVS Disk Type	Price (ECS + Disk)
	Default account	Name Default account	Specifications --			Free in OBT
☑	protected-instance-7906	Name ecs-agent-az2-3-dr Specifications 1 vCPUs | 2 GB	Specifications Si3.medium.2 | 1 vCPUs |	Drill-bae4	System Disk Gene... 40	Free in OBT
☑	protected-instance-7904	Name ecs-agent-az2-2-dr Specifications 1 vCPUs | 2 GB	Specifications Si3.medium.2 | 1 vCPUs |	Drill-bae5	System Disk Gene... 40	Free in OBT

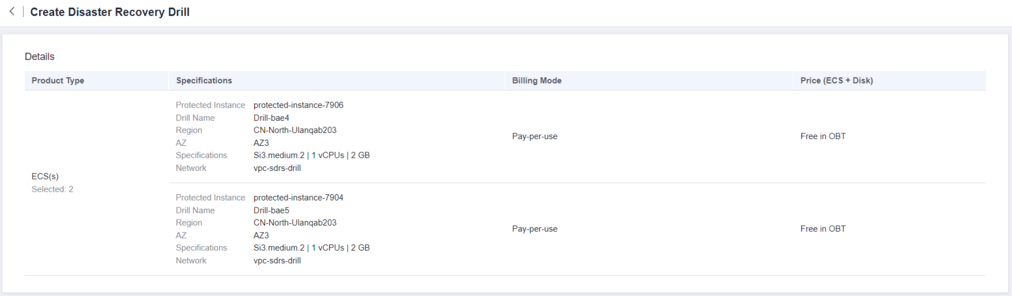
* Network vpc-sdrs-drill subnet-9cfc(192.168.11.2...

Price: Free During OBT

Table 2-3 Parameter description

Parameter	Description	Example Value
Protected Instance	Select all the protected instances you want to perform a disaster recovery drill.	-
Drill Server	Select the drill server specifications. To configure drill server specifications in a batch, select protected instances and click **Configure** in the first row, as shown in **Figure 2-7**.	-
Drill Name	Enter a drill name for each protected instance. The name can contain letters, digits, underscores (_), hyphens (-), or periods (.), can be no more than 64 characters long, and cannot contain spaces.	Drill-ECS02
Network	Select a VPC and subnet for the drill. The drill VPC and the VPC of disaster recovery site servers must be different.	-

Step 7 Click **Next**. On the displayed page, confirm drill information and click **Submit**.



Create Disaster Recovery Drill

Details

Product Type	Specifications	Billing Mode	Price (ECS + Disk)
ECS(s) Selected: 2	Protected Instance protected-instance-7906 Drill Name Drill-bae4 Region CN-North-Ulanqab203 AZ AZ3 Specifications Si3.medium.2 | 1 vCPUs | 2 GB Network vpc-sdrs-drill	Pay-per-use	Free in OBT
	Protected Instance protected-instance-7904 Drill Name Drill-bae5 Region CN-North-Ulanqab203 AZ AZ3 Specifications Si3.medium.2 | 1 vCPUs | 2 GB Network vpc-sdrs-drill	Pay-per-use	Free in OBT

Step 8 After the disaster recovery drill is created, log in to drill servers and check whether services are running properly.

----End

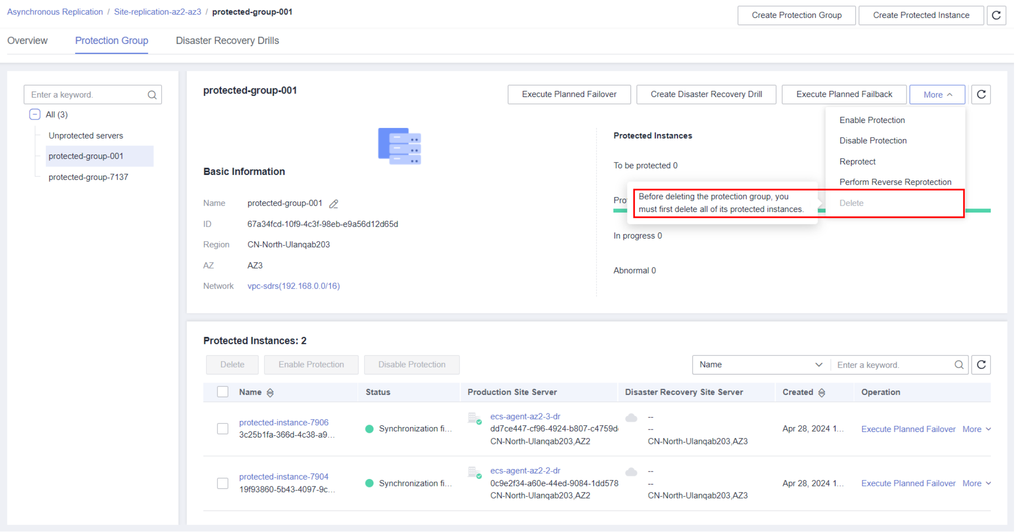
2.2.9 Deleting a Protection Group

Scenarios

You can delete protection groups that are no longer needed to release resources.

Prerequisites

- The protection group contains no protected instances.



protected-group-001

Basic Information

Name protected-group-001
ID 67a34fcd-10f9-4c3f-98eb-e9a56d12d65d
Region CN-North-Ulanqab203
AZ AZ3
Network vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 0

Pro

In progress 0

Abnormal 0

Before deleting the protection group, you must first delete all of its protected instances.

Protected Instances: 2

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-7906 3c25b1fa-366d-4c38-a9...	Synchronization fi...	ecs-agent-az2-3-dr dd7ce447-cf96-4924-b807-c4759d CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More
protected-instance-7904 19f93860-5b43-4097-9c...	Synchronization fi...	ecs-agent-az2-2-dr 0c9e2f34-a60e-44ed-9084-1dd578 CN-North-Ulanqab203,AZ2	-- -- CN-North-Ulanqab203,AZ3	Apr 28, 2024 1...	Execute Planned Failover More

- Disaster recovery drills in the protection group have been deleted.

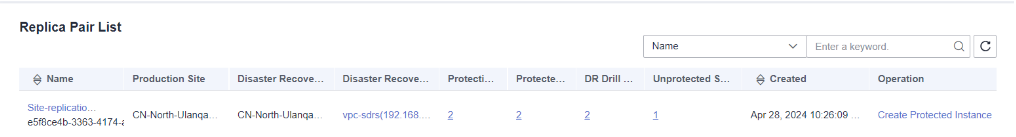
Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair in which you want to delete protection groups and click the number in the **Protection Groups** column.

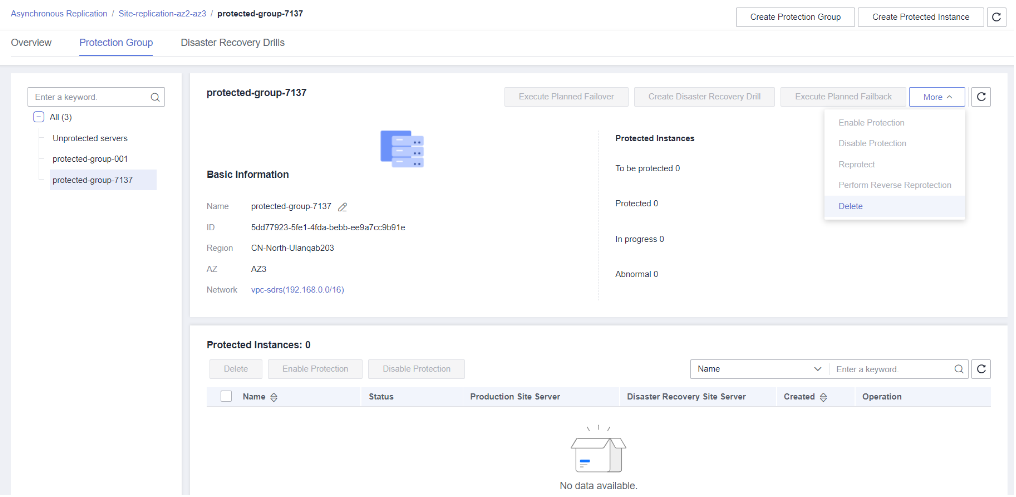


Replica Pair List

Name	Production Site	Disaster Recove...	Disaster Recove...	Protecti...	Protecte...	DR Drill ...	Unprotected S...	Created	Operation
Site-replicatio... e5f8ce4b-3363-4174-a	CN-North-Ulanqa...	CN-North-Ulanqa...	vpc-sdrs(192.168....	2	2	2	1	Apr 28, 2024 10:26:09 ...	Create Protected Instance

Step 4 In the navigation tree, select the target protection group to view its details.

In the upper right corner of the basic information area, choose **More** > **Delete**.



protected-group-7137

Basic Information

Name protected-group-7137
ID 5dd77923-5fe1-4fda-bebb-ee9a7cc9b91e
Region CN-North-Ulanqab203
AZ AZ3
Network vpc-sdrs(192.168.0.0/16)

Protected Instances

To be protected 0

Protected 0

In progress 0

Abnormal 0

Protected Instances: 0

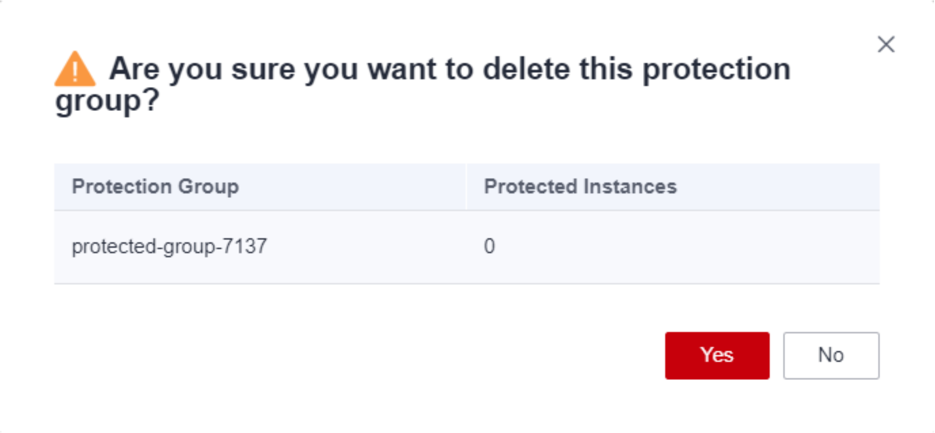
Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation

No data available.

NOTE

A protection group cannot be deleted if it contains protected instances or disaster recovery drills.

Step 5 In the displayed dialog box, confirm information and click **Yes**.



Are you sure you want to delete this protection group?

Protection Group	Protected Instances
protected-group-7137	0

----End

2.3 Managing Protected Instances

2.3.1 Creating Protected Instances

Scenarios

You can create protected instances for ECSs that require disaster recovery in a specific protection group. If a lot of production site servers become faulty due to force majeure, you can execute a failover to switch services from the production site to disaster recovery site to ensure service continuity.

When you create a protected instance, only disks are created at the disaster recovery site. The disk type can be different, but disk sizes must be the same as those of the production site server disks. After a protected instance is created, protection is automatically enabled until data has been synchronized.

NOTE

1. When you create a protected instance, the background system automatically creates replication pairs for all disks on the server, creates disks of the same specifications at the disaster recovery site, and then starts the initial data synchronization. Initial synchronization occupies the read bandwidth, CPU, and memory of the production disks, so you are advised to create protected instances at off-peak hours, or disable protection when services are affected and then enable protection at off-peak hours.

Prerequisites

- Production site servers are not used to create protected instances.
- Production site servers are in the same AZ and VPC as the cloud disaster recovery gateway.

NOTE

- If you have installed the proxy client on production site servers and then attach and detach disks on them, restart the servers before creating protected instances for them.

Procedure

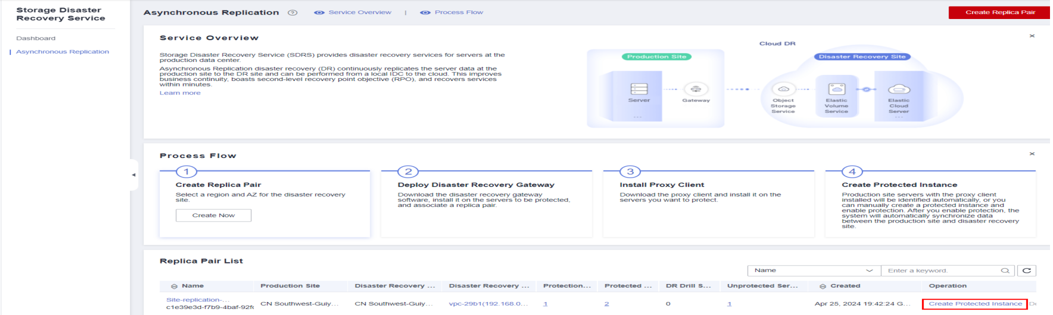
Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair in which you want to create protected instances and click **Create Protected Instance** in the **Operation** column.

The **Create Protected Instance** page is displayed.



Service Overview

Storage Disaster Recovery Service (SDRS) provides disaster recovery services for servers at the production data center.

Asynchronous Replication disaster recovery (DR) continuously replicates the server data at the production site to the DR site and can be performed from a local IDC to the cloud. This improves business continuity, boasts second-level recovery point objective (RPO), and recovers services within minutes.

Learn more

Process Flow

1 Create Replica Pair: Select a region and AZ for the disaster recovery site.

2 Deploy Disaster Recovery Gateway: Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

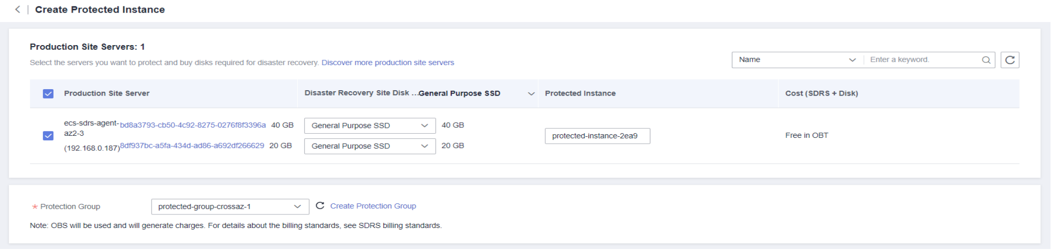
3 Install Proxy Client: Download the proxy client and install it on the servers you want to protect.

4 Create Protected Instance: Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Replica Pair List

Name	Production Site	Disaster Recovery ...	Disaster Recovery ...	Protection...	Protected ...	DR Drill S...	Unprotected Ser...	Created	Operation
Site-replication-... c1e39e3d-f7b9-4baf-92f	CN Southwest-Guiy...	CN Southwest-Guiy...	vpc-29b1(192.168.0...	1	2	0	1	Apr 25, 2024 19:42:24 G...	Create Protected Instance

Step 4 Configure the protected instance information.



Production Site Servers: 1

Select the servers you want to protect and buy disks required for disaster recovery. Discover more production site servers

☑ Production Site Server		Disaster Recovery Site Disk ...General Purpose SSD		Protected Instance	Cost (SDRS + Disk)
☑ ecs-sdrs-agent-az2-3 (192.168.0.187)	bd8a3793-cb50-4c92-8275-0276f8f3396a 40 GB	General Purpose SSD	40 GB	protected-instance-2ea9	Free in OBT
	8df937bc-a5fa-434d-ad86-a692df266629 20 GB	General Purpose SSD	20 GB		

* Protection Group: protected-group-crossaz-1

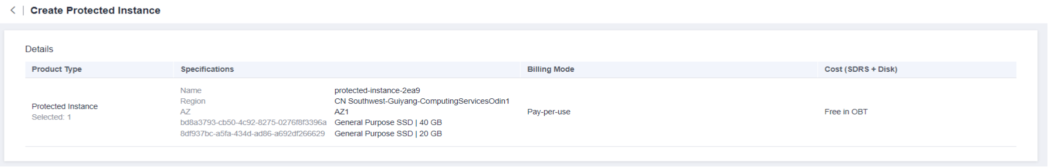
Note: OBS will be used and will generate charges. For details about the billing standards, see SDRS billing standards.

Table 2-4 Parameter description

Parameter	Description	Example Value
Production Site Server	Select production site servers you want to protect.	-
Disaster Recovery Site Disk	Select the disk type for each disaster recovery site disk. **NOTE** For the disaster recovery site servers created, the device type of system disks is VBD, and that of data disks is SCSI.	-

Parameter	Description	Example Value
Protected Instance	Enter a name for each protected instance. The name can contain letters, digits, underscores (_), hyphens (-), or periods (.), can be no more than 64 characters long, and cannot contain spaces.	protected-instance-01
Protection Group	Select a protection group for the protected instances. If you create protected instances first time ever or the current protection group does not meet your requirements, click **Create Protection Group** to create a new one. It is recommended that you add servers of a specific business to the same protection group. In this case, you can start protection, perform failovers, and run disaster recovery drills for the entire group.	protected-group-01

Step 5 Click **Next**. On the displayed page, confirm the configuration information and click **Submit**.

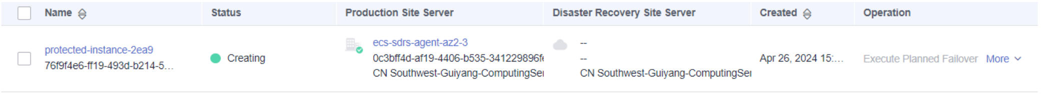


< | Create Protected Instance

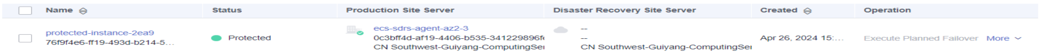
Details

Product Type	Specifications		Billing Mode	Cost (SDRS + Disk)
Protected Instance Selected: 1	Name Region AZ bd8a3793-cb50-4c92-8275-0276f8f3396a 8df937bc-a5fa-434d-ad86-a692df266629	protected-instance-2ea9 CN Southwest-Guiyang-ComputingServicesOdin1 AZ1 General Purpose SSD | 40 GB General Purpose SSD | 20 GB	Pay-per-use	Free in OBT

Step 6 When the protected instance status changes from **Creating** to **Protected**, the protected instance is created successfully created, and the initial data synchronization starts.

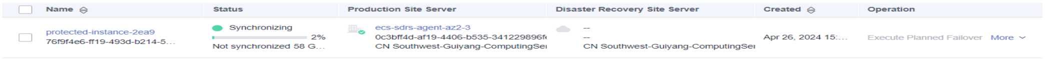


□	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Creating	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More ˅



□	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Protected	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More ˅

Step 7 After 1 to 2 minutes, the protected instance status changes to **Synchronizing**, and the amount of data to be synchronized and estimated remaining time are displayed.



□	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Synchronizing 2% Not synchronized 58 G...	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More ˅

NOTE

1. An initial synchronization synchronizes all disk data on the servers to disaster recovery site disks. The time required for synchronization varies with the amount of the disk data. The larger the amount of data, the longer the time.
2. The initial synchronization speed is affected by multiple factors, including the service loads, network quality, and network bandwidth on the servers. Normally, the synchronization speed is faster when servers have light loads and high network quality. The synchronization bandwidth of a single instance can reach up to 60 MB/s.
3. The data upload bandwidth displayed on the protected instance page is the bandwidth after data is compressed. This bandwidth is usually smaller than the actual bandwidth.
4. The synchronization progress displayed may restart from 0% if the synchronization is interrupted by a fault or manually disabled and then enabled. This is because the progress of the previous synchronization is not accumulated.

Step 8 When the protected instance status changes from **Synchronization finished** and the **Execute Failover** button is available, the initial synchronization is complete.

----End

2.3.2 Enabling Protection

Scenarios

You can enable protection for a protected instance in a protection group.

After protection is enabled, data synchronization starts for the protected instance.

Prerequisites

The status of the protected instance is **Pending protection** or **Enabling protection failed**.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

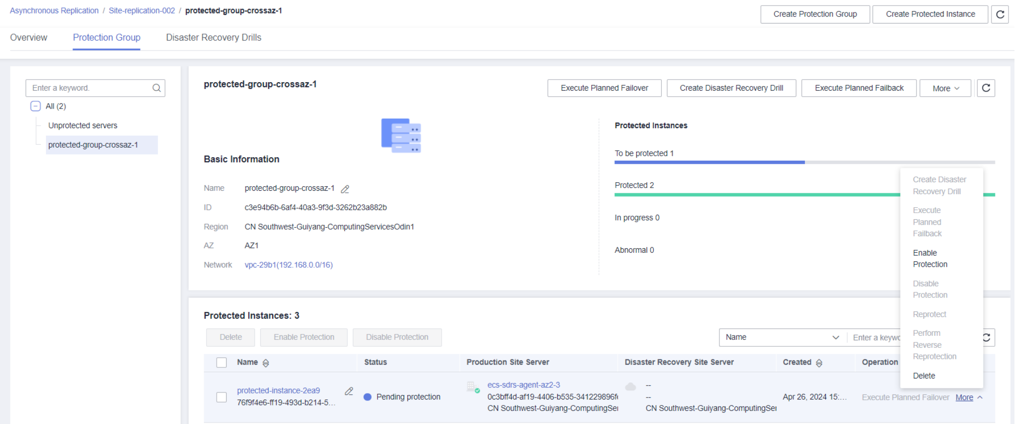
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protected instance you want to enable protection and click the number in the **Protected Instances** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the **Protected Instances** area, locate the target protected instance, choose **More** > **Enable Protection** in the **Operation** column.



protected-group-crossaz-1

Basic Information

Name	protected-group-crossaz-1
ID	c3e94b6b-6af4-40a3-9f3d-3262b23a882b
Region	CN Southwest-Guiyang-ComputingServicesOdin1
AZ	AZ1
Network	vpc-29b1(192.168.0.0/16)

Protected Instances

To be protected 1

Protected 2

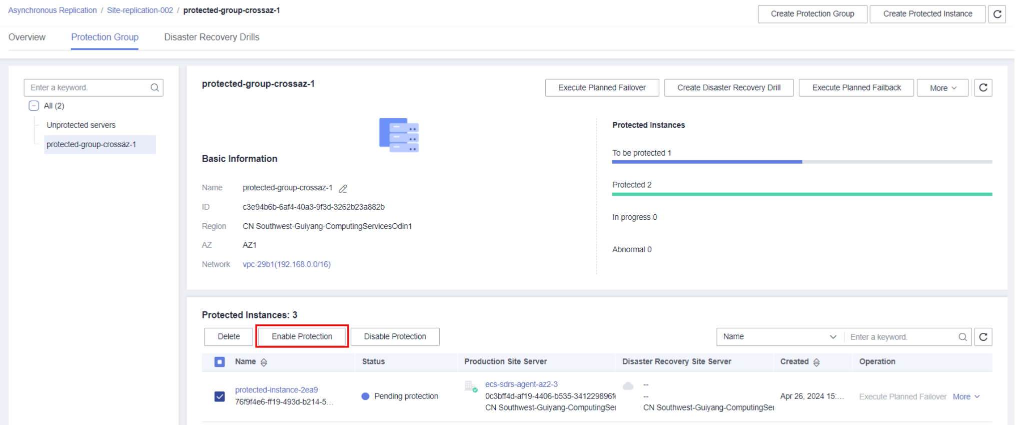
In progress 0

Abnormal 0

Protected Instances: 3

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	Pending protection	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More

If you want to enable protection for multiple protected instances, select the desired instances and click **Enable Protection** above the instance list.



protected-group-crossaz-1

Basic Information

Name	protected-group-crossaz-1
ID	c3e94b6b-6af4-40a3-9f3d-3262b23a882b
Region	CN Southwest-Guiyang-ComputingServicesOdin1
AZ	AZ1
Network	vpc-29b1(192.168.0.0/16)

Protected Instances

To be protected 1

Protected 2

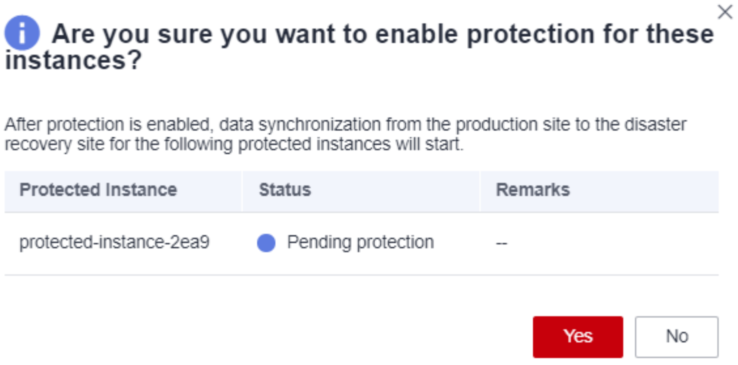
In progress 0

Abnormal 0

Protected Instances: 3

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☑ protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	Pending protection	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More

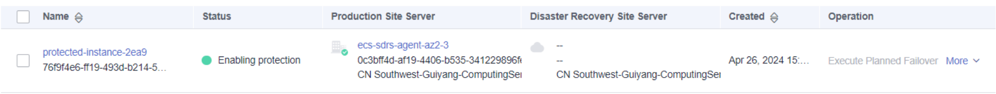
Step 6 In the displayed dialog box, confirm the protected instance information and click **Yes** to enable protection. The protected instance status changes to **Enabling protection**.



Are you sure you want to enable protection for these instances?

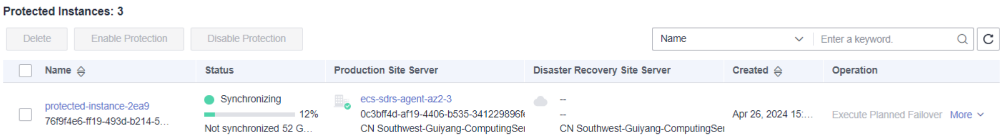
After protection is enabled, data synchronization from the production site to the disaster recovery site for the following protected instances will start.

Protected Instance	Status	Remarks
protected-instance-2ea9	● Pending protection	--



Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Enabling protection	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More

Step 7 After protection is enabled, the protected instance status changes to **Synchronizing**, indicating that differential data is being synchronized.



☐	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☐	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5…	● Synchronizing 12% Not synchronized 52 G…	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:…	Execute Planned Failover More

NOTE

After protection is enabled, differential data is read from disks and synchronized to the disaster recovery site. During this period, the disk read bandwidth increases, and services may be affected, so you are advised to enable protection during off-peak hours.

----End

2.3.3 Disabling Protection

Scenarios

You can disable protection for a protected instance in a protection group.

After protection is disabled, data synchronization stops for the protected instance.

Prerequisites

- The status of the protected instance is **Synchronization finished**, **Synchronizing**, or **Disabling protection failed**.
- Protected instance services are running at the production site.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

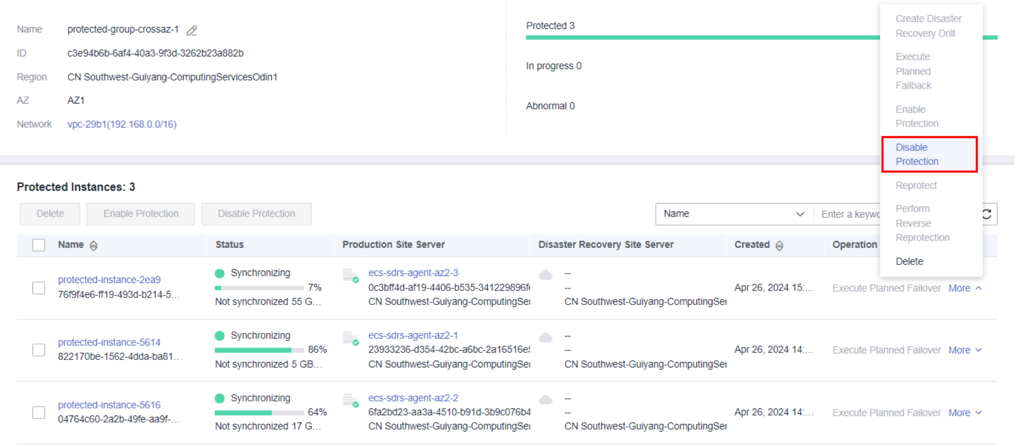
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protected instance you want to disable protection and click the number in the **Protection Groups** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the **Protected Instances** area, locate the target protected instance, choose **More** > **Disable Protection** in the **Operation** column.



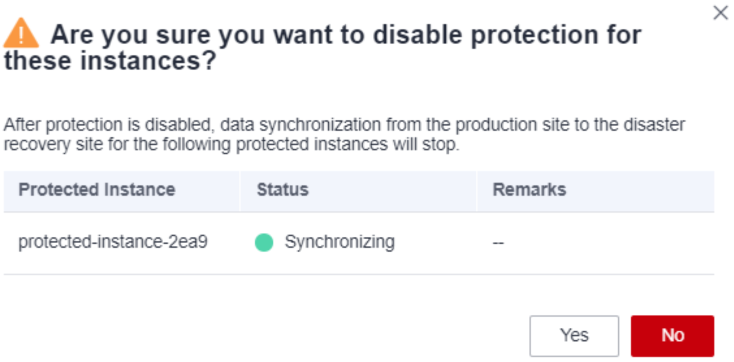
Name protected-group-crossaz-1
ID c3e94b6b-6af4-40a3-9f3d-3262b23a882b
Region CN Southwest-Guiyang-ComputingServicesOdin1
AZ AZ1
Network vpc-29b1(192.168.0.0/16)

Protected 3
In progress 0
Abnormal 0

Protected Instances: 3

	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Synchronizing 7% Not synchronized 55 G...	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More
□	protected-instance-5614 822170be-1562-4dda-ba81...	● Synchronizing 86% Not synchronized 5 GB...	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More
□	protected-instance-5616 04764c60-2a2b-49fe-aa9f-...	● Synchronizing 64% Not synchronized 17 G...	ecs-sdrs-agent-az2-2 6fa2bd23-aa3a-4510-b91d-3b9c076b4 CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

If you want to disable protection for multiple protected instances, select the desired instances and click **Disable Protection** above the instance list.

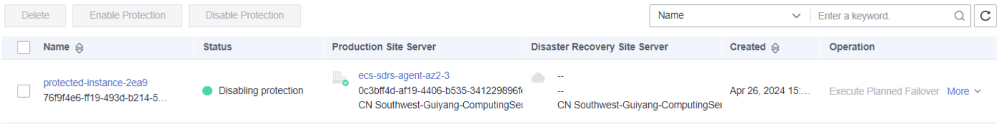


Are you sure you want to disable protection for these instances?

After protection is disabled, data synchronization from the production site to the disaster recovery site for the following protected instances will stop.

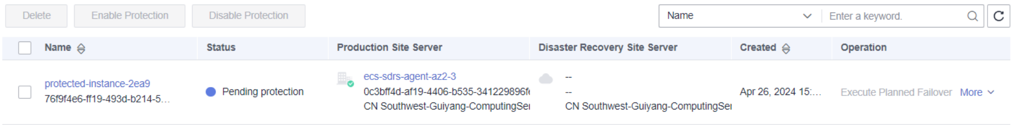
Protected Instance	Status	Remarks
protected-instance-2ea9	● Synchronizing	--

Step 6 In the displayed dialog box, confirm the protected instance information and click **Yes** to disable protection. The protected instance status changes to **Disabling protection**.



	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Disabling protection	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More

Step 7 After protection is disabled, the protected instance status changes to **Pending protection**.



	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Pending protection	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More

----End

2.3.4 Performing a Failover

Scenarios

Disaster recovery site servers are created using the most current data and billed based on the server billing standards. If servers are still running during a failover, the system synchronizes all the server data before failover is performed to the disaster recovery site servers. Data written to the servers during the failover may not be synchronized to the disaster recovery site. If one of the servers to be failed over fails, data on the server may fail to be synchronized and some data may be lost.

After a failover, data is not automatically synchronized from the disaster recovery site to the production site, and protection is disabled for protected instances. To start data synchronization from the disaster recovery site to the production site, perform a reverse reprotection.

Failover is a high-risk operation. After a failover, services are started at the disaster recovery site. At this time, you must ensure that production site services are stopped. Otherwise, services may be conflicted or interrupted and data may be damaged because both sites are providing services. If you just want to verify and analyze the disaster recovery site data, perform disaster recovery drills instead.

Prerequisites

- Initial synchronization is completed for the protected instance, and the status of the protected instance is **Synchronization finished** or **Failover failed**.
- Protected instance services are running at the production site.
- All services on production site server are stopped, and all data has been flushed to disks.

Precautions

During a failover, a primary NIC is configured for each disaster recovery site server. If a production site server uses a secondary NIC, you need to manually bind a secondary NIC for the corresponding disaster recovery site server on the server details page.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

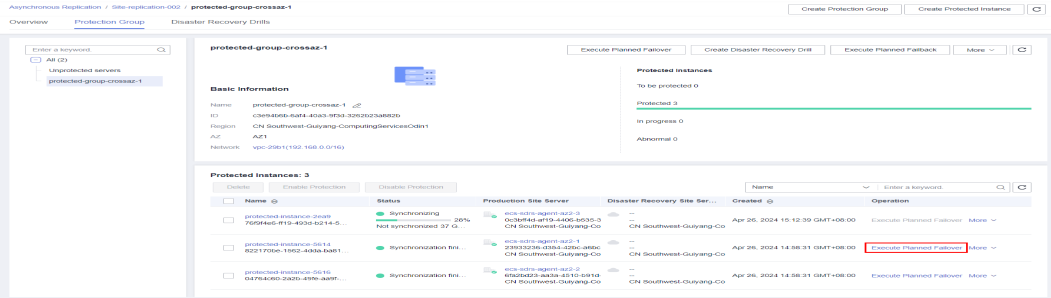
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protected instance you want to perform a failover and click the number in the **Protected Instances** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the **Protected Instances** area, locate the target protected instance, and click **Execute Failover** in the **Operation** column.



Asynchronous Replication / Site-replication-002 / **protected-group-crossaz-1**

protected-group-crossaz-1

Basic Information

Name	protected-group-crossaz-1
ID	c3e94b6b-6af4-40a3-9f3d-3262b23a882b
Region	CN Southwest-Guiyang-ComputingServicesOdin1
AZ	AZ1
Network	vpc-29b1(192.168.0.0/16)

Protected Instances

To be protected 0

Protected 3

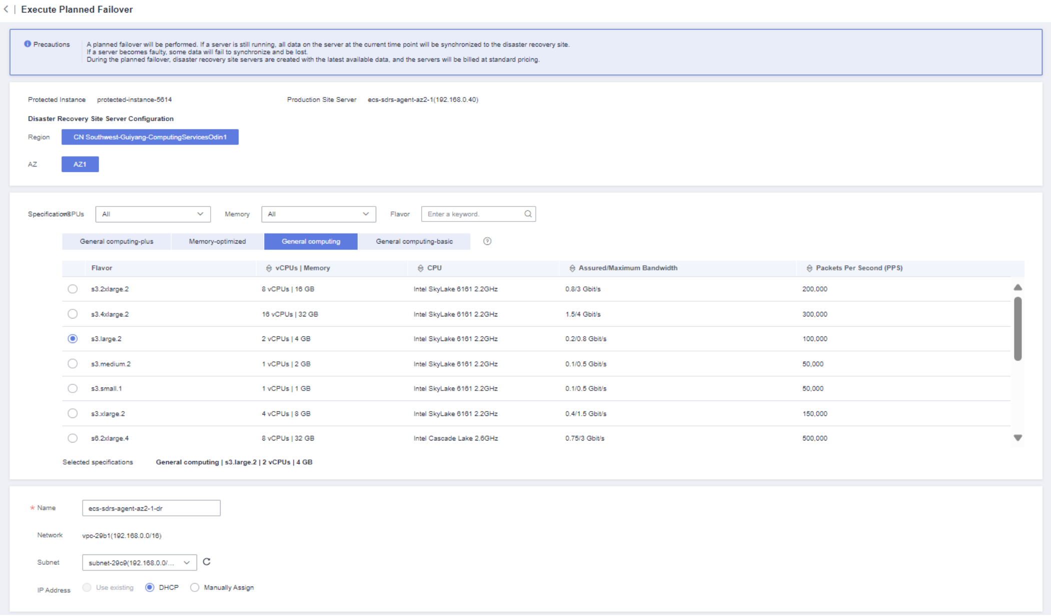
In progress 0

Abnormal 0

Protected Instances: 3

Name	Status	Production Site Server	Disaster Recovery Site Ser...	Created	Operation
protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	Synchronizing 28% Not synchronized 37 G...	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-3 CN Southwest-Guiyang-Co	-- -- CN Southwest-Guiyang-Co	Apr 26, 2024 15:12:39 GMT+08:00	Execute Planned Failover More
protected-instance-5614 822170be-1562-4dda-ba81...	Synchronization fini...	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc CN Southwest-Guiyang-Co	-- -- CN Southwest-Guiyang-Co	Apr 26, 2024 14:58:31 GMT+08:00	Execute Planned Failover More
protected-instance-5616 04764c60-2a2b-49fe-aa9f-...	Synchronization fini...	ecs-sdrs-agent-az2-2 6fa2bd23-aa3a-4510-b91d- CN Southwest-Guiyang-Co	-- -- CN Southwest-Guiyang-Co	Apr 26, 2024 14:58:31 GMT+08:00	Execute Planned Failover More

Step 6 Configure the disaster recovery site server.



Execute Planned Failover

Precautions A planned failover will be performed. If a server is still running, all data on the server at the current time point will be synchronized to the disaster recovery site.
If a server becomes faulty, some data will fail to synchronize and be lost.
During the planned failover, disaster recovery site servers are created with the latest available data, and the servers will be billed at standard pricing.

Protected Instance protected-instance-5614 Production Site Server ecs-sdrs-agent-az2-1(192.168.0.40)

Disaster Recovery Site Server Configuration

Region: CN Southwest-Guiyang-ComputingServicesOdin1

AZ: AZ1

SpecificationsCPUs: All Memory: All Flavor: Enter a keyword.

	Flavor	vCPUs | Memory	CPU	Assured/Maximum Bandwidth	Packets Per Second (PPS)
○	s3.2xlarge.2	8 vCPUs | 16 GB	Intel SkyLake 6161 2.2GHz	0.8/3 Gbit/s	200,000
○	s3.4xlarge.2	16 vCPUs | 32 GB	Intel SkyLake 6161 2.2GHz	1.5/4 Gbit/s	300,000
●	s3.large.2	2 vCPUs | 4 GB	Intel SkyLake 6161 2.2GHz	0.2/0.8 Gbit/s	100,000
○	s3.medium.2	1 vCPUs | 2 GB	Intel SkyLake 6161 2.2GHz	0.1/0.5 Gbit/s	50,000
○	s3.small.1	1 vCPUs | 1 GB	Intel SkyLake 6161 2.2GHz	0.1/0.5 Gbit/s	50,000
○	s3.xlarge.2	4 vCPUs | 8 GB	Intel SkyLake 6161 2.2GHz	0.4/1.5 Gbit/s	150,000
○	s6.2xlarge.4	8 vCPUs | 32 GB	Intel Cascade Lake 2.6GHz	0.75/3 Gbit/s	500,000

Selected specifications **General computing | s3.large.2 | 2 vCPUs | 4 GB**

* Name: ecs-sdrs-agent-az2-1-dr

Network: vpc-29b1(192.168.0.0/16)

Subnet: subnet-29c9(192.168.0.0/...

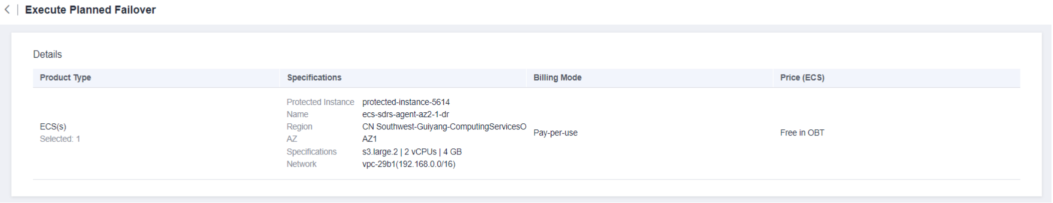
IP Address: ○ Use existing ● DHCP ○ Manually Assign

Table 2-5 Parameter description

Parameter	Description	Example Value
Specifications	Select the specifications for the disaster recovery site server.	-
Name	Enter a disaster recovery server name. The name can contain letters, digits, underscores (_), hyphens (-), or periods (.), can be no more than 64 characters long, and cannot contain spaces.	ECS02-DR
Subnet	Select the subnet where the disaster recovery server resides.	-

Parameter	Description	Example Value
IP Address	Select how the server obtains an IP address. - **Use existing**: Select this option if the subnet selected is in the same CIDR Block as the production site server. This setting keeps the IP addresses on both servers consistent. - **DHCP**: IP addresses are automatically assigned by the system. - **Manually Assign**: Manually specify an IP address.	-

Step 7 Click **Next**. On the displayed page, confirm the disaster recovery server information and click **Submit**.

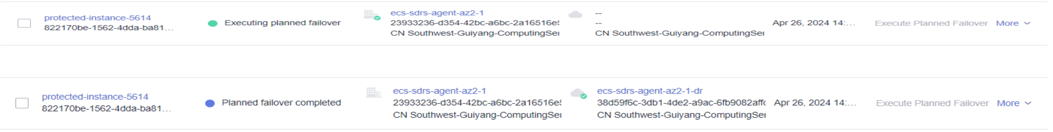


< | Execute Planned Failover

Details

Product Type	Specifications	Billing Mode	Price (ECS)
ECS(s) Selected: 1	Protected Instance protected-instance-5614 Name ecs-sdrs-agent-az2-1-dr Region CN Southwest-Guiyang-ComputingServicesO AZ AZ1 Specifications s3.large.2 | 2 vCPUs | 4 GB Network vpc-29b1(192.168.0.0/16)	Pay-per-use	Free in OBT

Step 8 The protected instance status changes to **Executing failover**. After the failover is complete, the status changes to **Failover completed**.



□	protected-instance-5614 822170be-1562-4dda-ba81...	● Executing planned failover	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e5 CN Southwest-Guiyang-ComputingSei	-- -- CN Southwest-Guiyang-ComputingSei	Apr 26, 2024 14:...	Execute Planned Failover More ⌄
□	protected-instance-5614 822170be-1562-4dda-ba81...	● Planned failover completed	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e5 CN Southwest-Guiyang-ComputingSei	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082affc CN Southwest-Guiyang-ComputingSei	Apr 26, 2024 14:...	Execute Planned Failover More ⌄

----End

2.3.5 Performing a Reverse Reprotection

Scenarios

After a failover, data is not automatically synchronized from the disaster recovery site to the production site, and protection is disabled for protected instances. To start data synchronization from the disaster recovery site to the production site, perform a reverse reprotection.

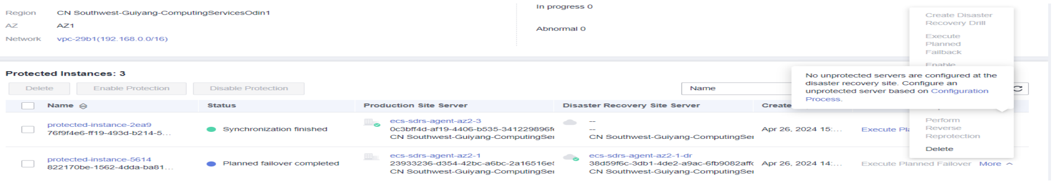
NOTE

- After you perform a reverse reprotection, the initial data synchronization starts. During the data synchronization, if disaster recovery site servers are restarted, data will be resynchronized until the synchronization is complete.
- If disaster recovery site servers are restarted after the initial synchronization is complete, data will not be resynchronized. If there is data written to the disaster recovery server later, incremental data synchronization will be performed.
- Reverse reprotection overwrites data of the production site server with data of the disaster recovery site server. If there is data written to the production site server after the failover is performed, such data will be overwritten.

Prerequisites

- The disaster recovery site server has been preconfigured according to **Configuring Disaster Recovery Site Servers**. Otherwise, the button is grayed out, as shown in the following figure.

  Figure 2-8 Disaster recovery site server not configured

  Region CN Southwest-Guiyang-ComputingServicesOdin1
  AZ AZ1
  Network vpc-29b1(192.168.0.0/16)

  In progress 0
  Abnormal 0

  Protected Instances: 3

  Delete | Enable Protection | Disable Protection | Name

  No unprotected servers are configured at the disaster recovery site. Configure an unprotected server based on Configuration Process.

□	Name	Status	Production Site Server	Disaster Recovery Site Server	Create	
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Synchronization finished	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSer	-- -- CN Southwest-Guiyang-ComputingSer	Apr 26, 2024 15:...	Execute Pl
□	protected-instance-5614 822170be-1562-4dda-ba81...	● Planned failover completed	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSer	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSer	Apr 26, 2024 14:...	Execute Planned Failover More ^

- The status of the protected instance is **Failover completed** or **Reverse reprotection failed**.

Procedure

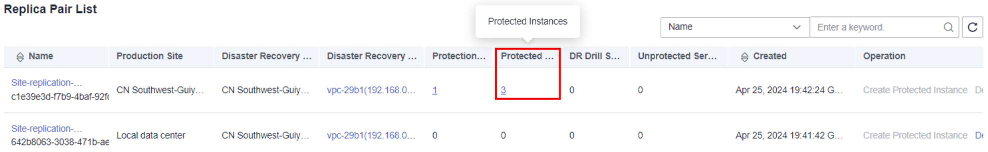
Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protected instance you want to perform reverse reprotection and click the number in the **Protected Instances** column.

The **Protection Groups** tab page is displayed.



Replica Pair List

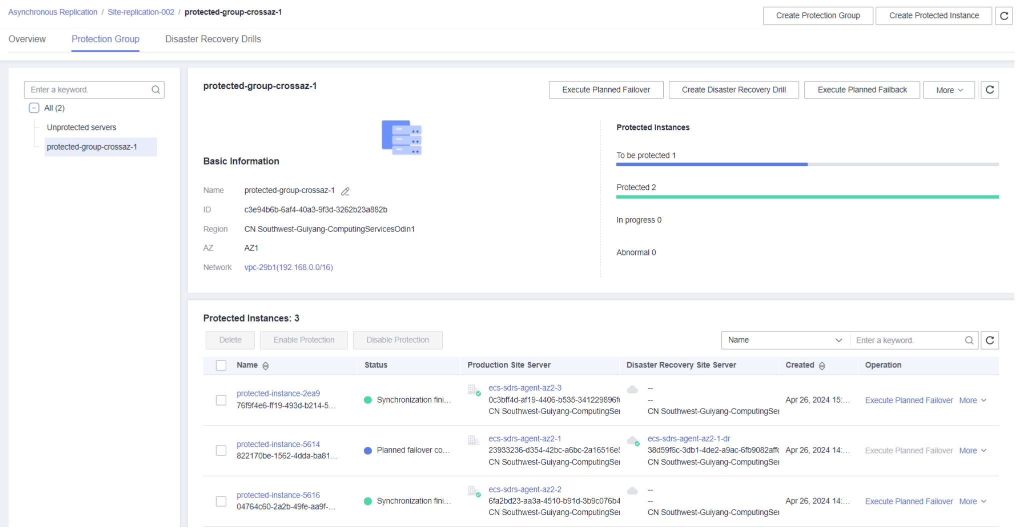
Protected Instances

Name | Enter a keyword.

Name	Production Site	Disaster Recovery ...	Disaster Recovery ...	Protection...	Protected ...	DR Drill S...	Unprotected Ser...	Created	Operation
Site-replication-... c1e39e3d-f7b9-4baf-92f	CN Southwest-Guiy...	CN Southwest-Guiy...	vpc-29b1(192.168.0...	1	3	0	0	Apr 25, 2024 19:42:24 G...	Create Protected Instance De
Site-replication-... 642b8063-3038-471b-ae	Local data center	CN Southwest-Guiy...	vpc-29b1(192.168.0...	0	0	0	0	Apr 25, 2024 19:41:42 G...	Create Protected Instance De

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.



Asynchronous Replication / Site-replication-002 / protected-group-crossaz-1

Overview | Protection Group | Disaster Recovery Drills

protected-group-crossaz-1

Basic Information

Name	protected-group-crossaz-1
ID	c3e94b6b-6af4-40a3-9f3d-3262b23a882b
Region	CN Southwest-Guiyang-ComputingServicesOdin1
AZ	AZ1
Network	vpc-29b1(192.168.0.0/16)

Protected Instances

To be protected 1

Protected 2

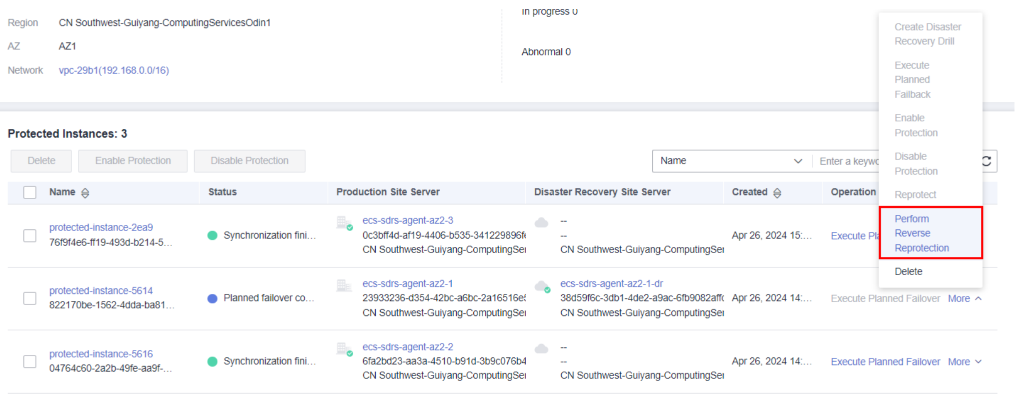
In progress 0

Abnormal 0

Protected Instances: 3

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	Synchronization fini...	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More
protected-instance-5614 822170be-1562-4dda-ba81...	Planned failover co...	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More
protected-instance-5616 04764c60-2a2b-49fe-aa9f-...	Synchronization fini...	ecs-sdrs-agent-az2-2 6fa2bd23-aa3a-4510-b91d-3b9c076b4 CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

Step 5 In the **Protected Instances** area, locate the target protected instance, choose **More** > **Perform Reverse Reprotection** in the **Operation** column.



Region	CN Southwest-Guiyang-ComputingServicesOdin1
AZ	AZ1
Network	vpc-29b1(192.168.0.0/16)

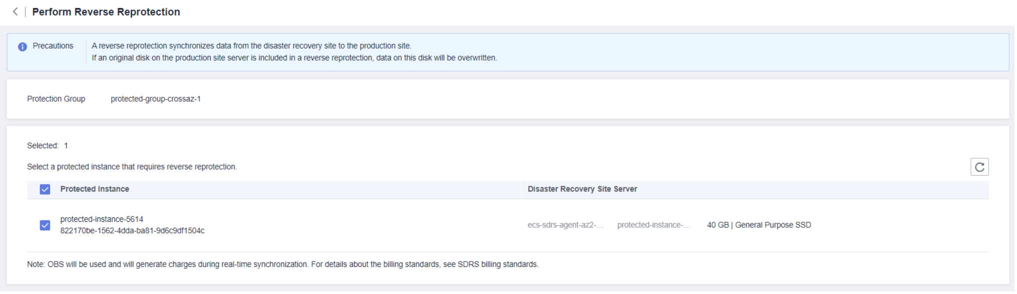
In progress 0

Abnormal 0

Protected Instances: 3

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	Synchronization fini...	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Pl
protected-instance-5614 822170be-1562-4dda-ba81...	Planned failover co...	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More
protected-instance-5616 04764c60-2a2b-49fe-aa9f-...	Synchronization fini...	ecs-sdrs-agent-az2-2 6fa2bd23-aa3a-4510-b91d-3b9c076b4 CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

Step 6 Confirm information on the **Perform Reverse Reprotection** page.



Perform Reverse Reprotection

Precautions: A reverse reprotection synchronizes data from the disaster recovery site to the production site.
If an original disk on the production site server is included in a reverse reprotection, data on this disk will be overwritten.

Protection Group: protected-group-crossaz-1

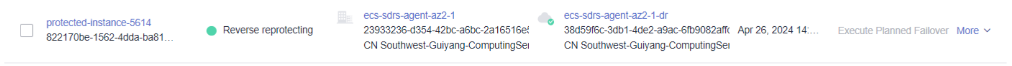
Selected: 1

Select a protected instance that requires reverse reprotection.

☑ Protected Instance	Disaster Recovery Site Server
☑ protected-instance-5614 822170be-1562-4dda-ba81-9d6c9df1504c	ecs-sdrs-agent-az2-... protected-instance-... 40 GB | General Purpose SSD

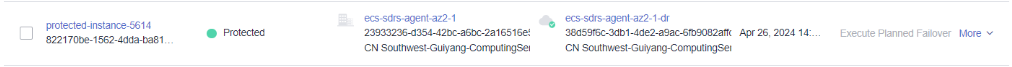
Note: OBS will be used and will generate charges during real-time synchronization. For details about the billing standards, see SDRS billing standards.

Step 7 Click **Submit**. The protected instance status changes to **Reverse reprotecting**.



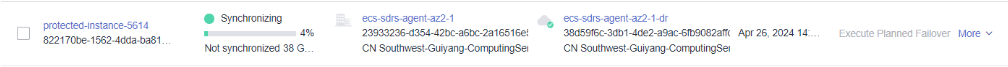
protected-instance-5614 822170be-1562-4dda-ba81...	Reverse reprotecting	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

Step 8 When the protected instance status changes to **Protected**, reverse reprotection is executed successfully. At this time, a full data comparison is performed and incremental data synchronization is started.



protected-instance-5614 822170be-1562-4dda-ba81...	Protected	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

Step 9 After 1 to 2 minutes, the protected instance status changes to **Synchronizing**, and the amount of data to be synchronized and estimated remaining time are displayed.



□	protected-instance-5614 822170be-1562-4dda-ba81…	● Synchronizing 4% Not synchronized 38 G…	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e! CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff(CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:…	Execute Planned Failover More ⌄

----End

2.3.6 Performing a Failback

Scenarios

After a failover, services are running at the disaster recovery site. You can fail back to your production site with a failback.

Failback is a high-risk operation. After a failback, services are started at the production site. At this time, you must ensure that disaster recovery site services are stopped. Otherwise, services may be conflicted or interrupted and data may be damaged because both sites are providing services.

Prerequisites

- Initial synchronization is completed for the protected instance, and the status of the protected instance is **Synchronization finished** or **Failback failed**.
- Protected instance services are running at the disaster recovery site.
- All services on the disaster recovery site server are stopped, and all data has been flushed to disks.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

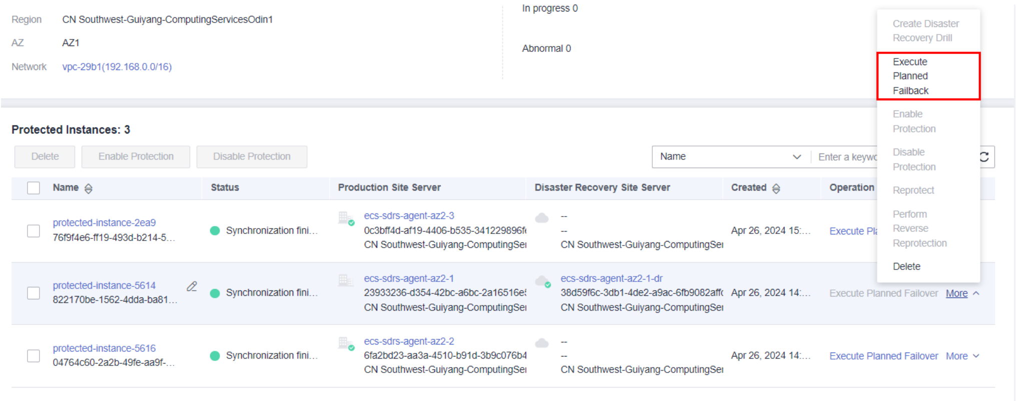
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protected instance you want to perform a failback and click the number in the **Protected Instances** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the **Protected Instances** area, locate the target protected instance and choose **More** > **Execute Failback** in the **Operation** column.



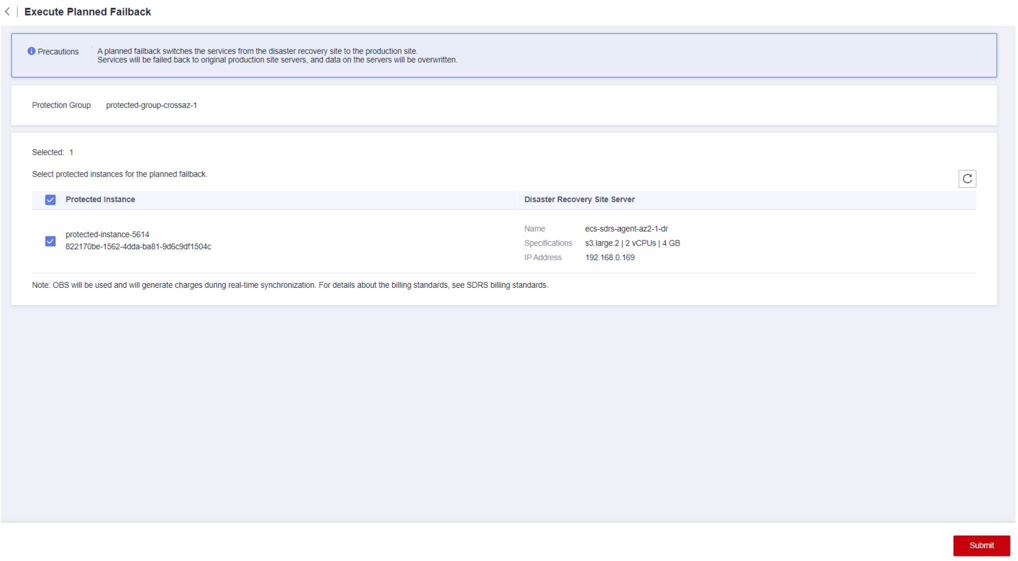
Region CN Southwest-Guiyang-ComputingServicesOdin1
AZ AZ1
Network vpc-29b1(192.168.0.0/16)

In progress 0
Abnormal 0

Protected Instances: 3

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	Synchronization fini...	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Pl
protected-instance-5614 822170be-1562-4dda-ba81...	Synchronization fini...	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More
protected-instance-5616 04764c60-2a2b-49fe-aa9f-...	Synchronization fini...	ecs-sdrs-agent-az2-2 6fa2bd23-aa3a-4510-b91d-3b9c076b4 CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

Step 6 On the displayed page, click **Submit**.



Execute Planned Failback

Precautions A planned failback switches the services from the disaster recovery site to the production site.
Services will be failed back to original production site servers, and data on the servers will be overwritten.

Protection Group protected-group-crossaz-1

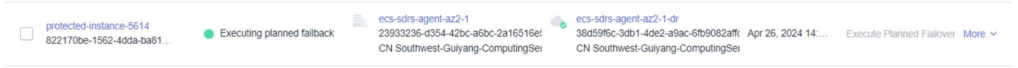
Selected: 1

Select protected instances for the planned failback.

☑ Protected Instance	Disaster Recovery Site Server
☑ protected-instance-5614 822170be-1562-4dda-ba81-9d6c9df1504c	Name ecs-sdrs-agent-az2-1-dr Specifications s3.large.2 | 2 vCPUs | 4 GB IP Address 192.168.0.169

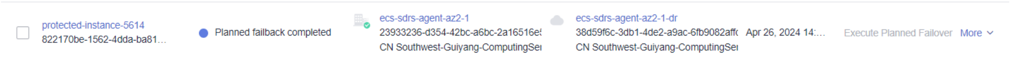
Note: OBS will be used and will generate charges during real-time synchronization. For details about the billing standards, see SDRS billing standards.

Step 7 The protected instance status changes to **Executing failback**. Wait until the operation is complete.



protected-instance-5614 822170be-1562-4dda-ba81...	Executing planned failback	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

Step 8 After the protected instance status changes to **Failback completed**, the operation is successful.



protected-instance-5614 822170be-1562-4dda-ba81...	Planned failback completed	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

----End

2.3.7 Reprotecting a Protected Instance

Scenarios

After a failback, data is not automatically synchronized from the production site to the disaster recovery site, and protection is disabled for protected instances. To start data synchronization from the production site to the disaster recovery site, reprotect the protection group.

Prerequisites

- The production site server has been preconfigured according to **Configuring Production Site Servers**.
- The status of the protected instance is **Failback completed** or **Reprotection failed**.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

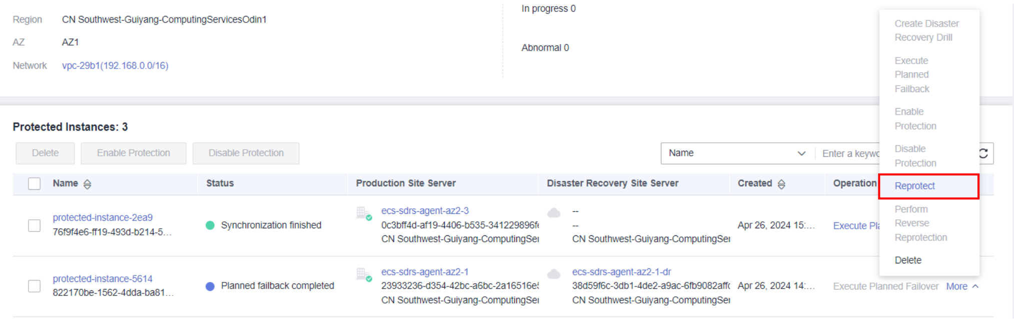
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protected instance you want to reprotect and click the number in the **Protected Instances** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

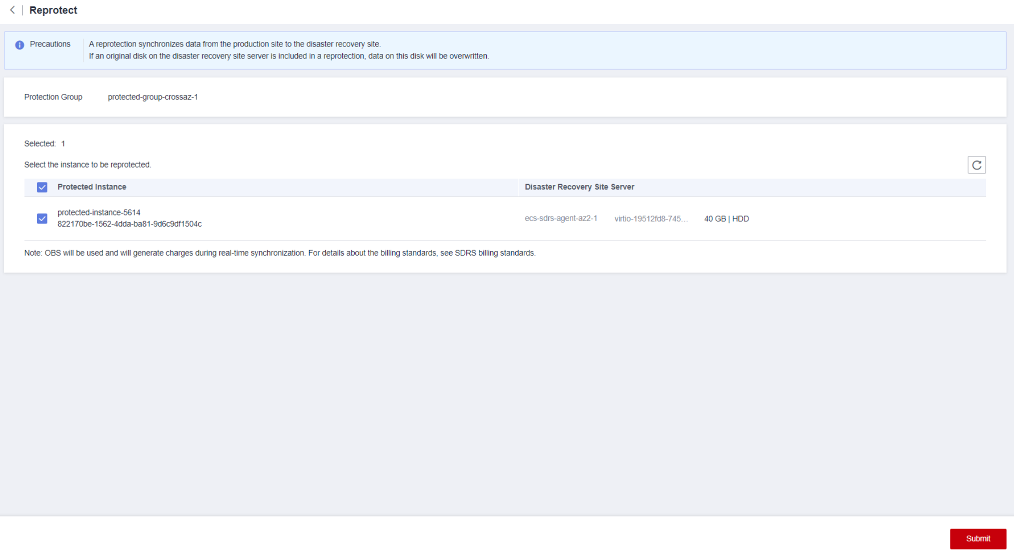
Step 5 In the **Protected Instances** area, locate the target protected instance, choose **More** > **Reprotect** in the **Operation** column.


Region CN Southwest-Guiyang-ComputingServicesOdin1
AZ AZ1
Network vpc-29b1(192.168.0.0/16)
In progress 0
Abnormal 0

Protected Instances: 3

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	Synchronization finished	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Pl
protected-instance-5614 822170be-1562-4dda-ba81...	Planned failback completed	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:...	Execute Planned Failover More

Step 6 On the displayed page, click **Submit**.


Reprotect

Precautions A reprotection synchronizes data from the production site to the disaster recovery site.
If an original disk on the disaster recovery site server is included in a reprotection, data on this disk will be overwritten.

Protection Group protected-group-crossaz-1

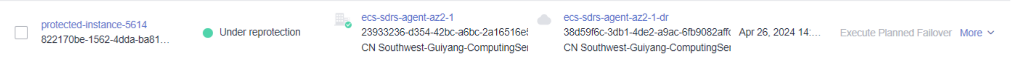
Selected: 1

Select the instance to be reprotected.

☑ Protected Instance	Disaster Recovery Site Server
☑ protected-instance-5614 822170be-1562-4dda-ba81-9d6c9df1504c	ecs-sdrs-agent-az2-1 virtio-19512fd8-745... 40 GB | HDD

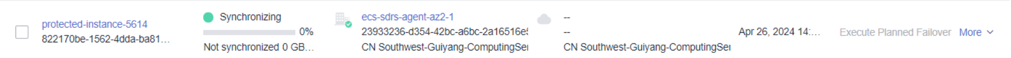
Note: OBS will be used and will generate charges during real-time synchronization. For details about the billing standards, see SDRS billing standards.

Step 7 The protected instance status changes to **Under reprotection**. Wait until the operation is complete.



□	protected-instance-5614 822170be-1562-4dda-ba81...	● Under reprotection	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e‹ CN Southwest-Guiyang-ComputingSe‹	ecs-sdrs-agent-az2-1-dr 38d59f6c-3db1-4de2-a9ac-6fb9082aff‹ CN Southwest-Guiyang-ComputingSe‹	Apr 26, 2024 14:...	Execute Planned Failover More ⌄

Step 8 After the operation is complete, the protected instance status changes to **Synchronizing**, and the amount of data to be synchronized and estimated remaining time are displayed.



□	protected-instance-5614 822170be-1562-4dda-ba81...	● Synchronizing 0% Not synchronized 0 GB...	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e‹ CN Southwest-Guiyang-ComputingSe‹	-- -- CN Southwest-Guiyang-ComputingSe‹	Apr 26, 2024 14:...	Execute Planned Failover More ⌄

NOTE

After the failback is successful, the disaster recovery site server will be automatically deleted.

----End

2.3.8 Creating a Disaster Recovery Drill

Scenarios

Disaster recovery drills are used to simulate fault scenarios, formulate recovery plans, and verify whether the plans are applicable and effective. Services are not affected during disaster recovery drills. When a fault occurs, you can use the plans to quickly recover services, thus improving service continuity.

SDRS allows you to run disaster recovery drills in isolated VPCs (different from the disaster recovery site VPC). During a disaster recovery drill, drill servers can be quickly created based on the disk snapshot data.

NOTE

After drill servers are created, production site servers and drill servers will independently run at the same time, and data will not be synchronized between these servers.

To guarantee that services can be switched to the disaster recovery site when an outage occurs, it is recommended that you run disaster recovery drills regularly.

Precautions

- If the production site servers of a protection group are added to an enterprise project, the drill servers created will not be automatically added to the enterprise project. Manually add them to the project as needed.
- If the production site servers run Linux and use key pairs for login, the key pair information will not be displayed on the server details page, but login using the key pairs is not affected.
- After a disaster recovery drill is created, modifications made to **Hostname**, **Name**, **Agency**, **ECS Group**, **Security Group**, **Tags**, and **Auto Recovery** of production site servers will not be synchronized to drill servers. Log in to the console and manually make the modifications for the drill servers.
- During a disaster recovery drill, a primary NIC is configured for each disaster recovery site server. If a production site server uses a secondary NIC, you need

to manually bind a secondary NIC for the corresponding disaster recovery site server on the server details page.

Prerequisites

- Initial synchronization is completed for the protected instance, and the status of the protected instance is **Synchronization finished** or **Disaster recovery drill failed**.
- Protected instance services are running at the production site.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

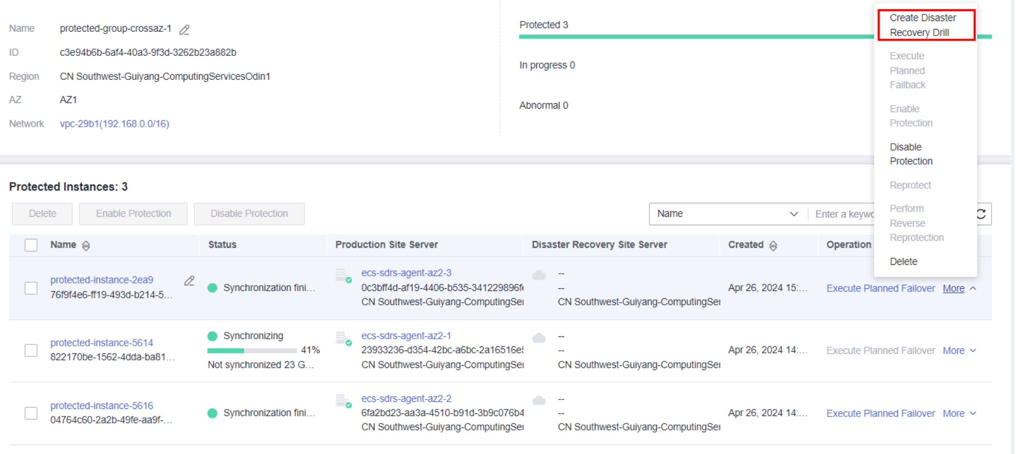
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protected instance you want to run a disaster recovery drill and click the number in the **Protection Groups** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation tree, choose the target protection group.

The protection group details page is displayed.

Step 5 In the **Protected Instances** area, locate the target protected instance and choose **More** > **Create Disaster Recovery Drill** in the **Operation** column.



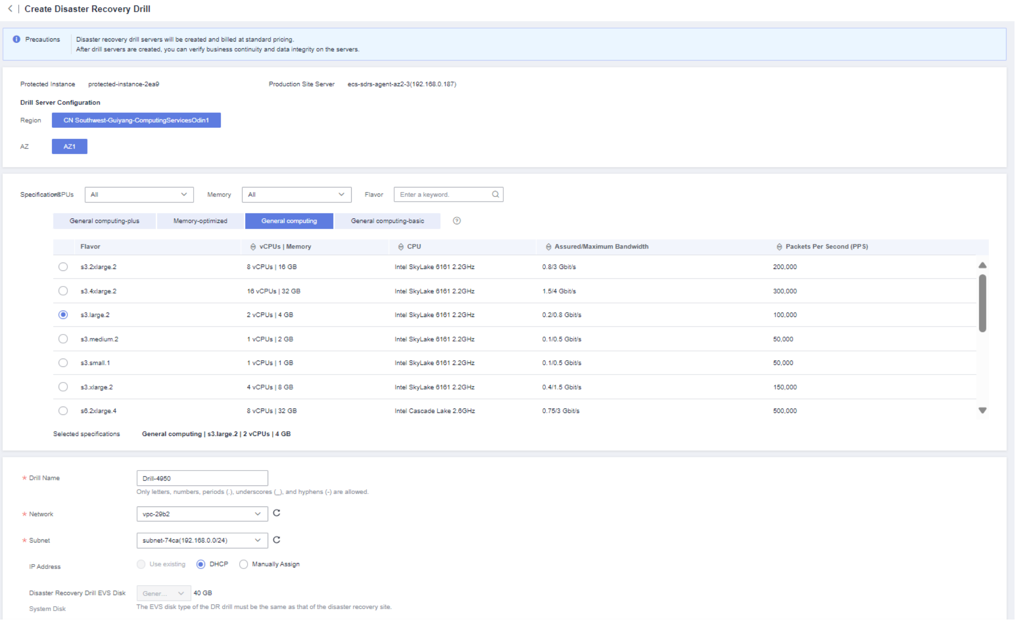
Name protected-group-crossaz-1
ID c3e94b6b-6af4-40a3-9f3d-3262b23a882b
Region CN Southwest-Guiyang-ComputingServicesOdin1
AZ AZ1
Network vpc-29b1(192.168.0.0/16)

Protected 3
In progress 0
Abnormal 0

Protected Instances: 3

Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5…	Synchronization fini…	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:…	Execute Planned Failover More
protected-instance-5614 822170be-1562-4dda-ba81…	Synchronizing 41% Not synchronized 23 G…	ecs-sdrs-agent-az2-1 23933236-d354-42bc-a6bc-2a16516e CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:…	Execute Planned Failover More
protected-instance-5616 04764c60-2a2b-49fe-aa9f-…	Synchronization fini…	ecs-sdrs-agent-az2-2 6fa2bd23-aa3a-4510-b91d-3b9c076b4 CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 14:…	Execute Planned Failover More

Step 6 Configure the drill server information.



Precautions: Disaster recovery drill servers will be created and billed at standard pricing.
After drill servers are created, you can verify business continuity and data integrity on the servers.

Protected Instance: protected-instance-2ea9

Production Site Server: ecs-sdrs-agent-az2-3(192.168.0.187)

Drill Server Configuration

Region: CN Southwest-Guiyang-ComputingServicesOdin1

AZ: AZ1

SpecificationsvCPUs: All | Memory: All | Flavor: Enter a keyword.

	Flavor	vCPUs | Memory	CPU	Assured/Maximum Bandwidth	Packets Per Second (PPS)
○	s3.2xlarge.2	8 vCPUs | 16 GB	Intel SkyLake 6161 2.2GHz	0.8/3 Gbit/s	200,000
○	s3.4xlarge.2	16 vCPUs | 32 GB	Intel SkyLake 6161 2.2GHz	1.5/4 Gbit/s	300,000
●	s3.large.2	2 vCPUs | 4 GB	Intel SkyLake 6161 2.2GHz	0.2/0.8 Gbit/s	100,000
○	s3.medium.2	1 vCPUs | 2 GB	Intel SkyLake 6161 2.2GHz	0.1/0.5 Gbit/s	50,000
○	s3.small.1	1 vCPUs | 1 GB	Intel SkyLake 6161 2.2GHz	0.1/0.5 Gbit/s	50,000
○	s3.xlarge.2	4 vCPUs | 8 GB	Intel SkyLake 6161 2.2GHz	0.4/1.5 Gbit/s	150,000
○	s6.2xlarge.4	8 vCPUs | 32 GB	Intel Cascade Lake 2.6GHz	0.75/3 Gbit/s	500,000

Selected specifications: **General computing | s3.large.2 | 2 vCPUs | 4 GB**

* Drill Name: Drill-4950
Only letters, numbers, periods (.), underscores (_), and hyphens (-) are allowed.

* Network: vpc-29b2

* Subnet: subnet-74ca(192.168.0.0/24)

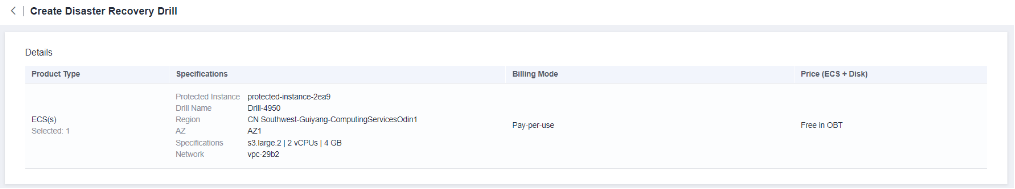
IP Address: ○ Use existing ● DHCP ○ Manually Assign

Disaster Recovery Drill EVS Disk System Disk: Gener... 40 GB
The EVS disk type of the DR drill must be the same as that of the disaster recovery site.

Table 2-6 Parameter description

Parameter	Description	Example Value
Specifications	Select the drill server specifications.	-
Drill Name	Enter a drill name. The name can contain letters, digits, underscores (_), hyphens (-), or periods (.), can be no more than 64 characters long, and cannot contain spaces.	Drill-ECS02
Network	Select a VPC for the drill. The drill VPC and the VPC of disaster recovery site server must be different.	-
Subnet	Select a subnet for the drill.	-
IP Address	Select how the server obtains an IP address. ● **Use existing**: Select this option if the subnet selected is in the same CIDR Block as the production site server. This setting keeps the IP addresses on both servers consistent. ● **DHCP**: IP addresses are automatically assigned by the system. ● **Manually Assign**: Manually specify an IP address.	-

Step 7 Click **Next**. On the displayed page, confirm drill information and click **Submit**.

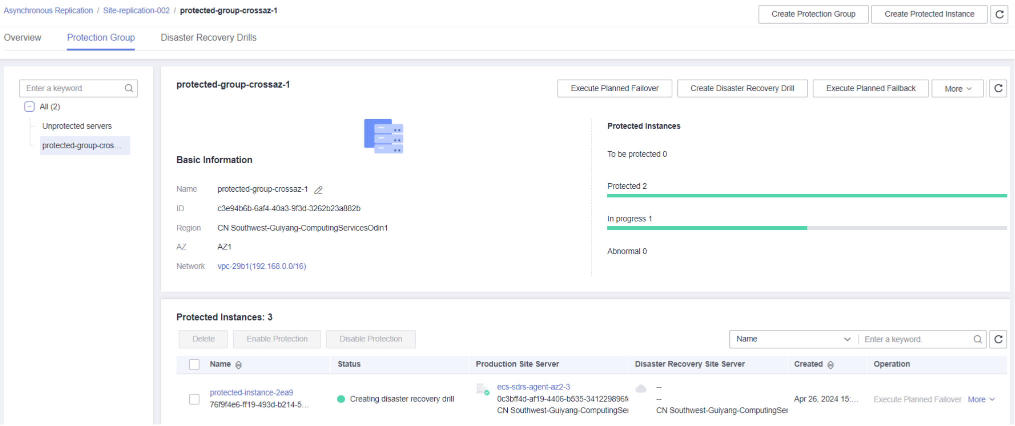


Create Disaster Recovery Drill

Details

Product Type	Specifications	Billing Mode	Price (ECS + Disk)
ECS(s) Selected: 1	Protected Instance protected-instance-2ea9 Drill Name Drill-4950 Region CN Southwest-Guiyang-ComputingServicesOdin1 AZ AZ1 Specifications s3.large.2 | 2 vCPUs | 4 GB Network vpc-29b2	Pay-per-use	Free in OBT

Step 8 The protected instance status changes to **Creating disaster recovery drill**. After the drill is created, the instance status changes back to **Synchronization finished**.



Asynchronous Replication / Site-replication-002 / protected-group-crossaz-1

protected-group-crossaz-1

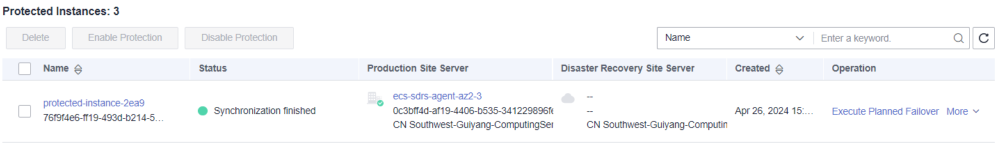
Basic Information

Name protected-group-crossaz-1
ID c3e94b6b-6af4-40a3-9f3d-3262b23a882b
Region CN Southwest-Guiyang-ComputingServicesOdin1
AZ AZ1
Network vpc-29b1(192.168.0.0/16)

Protected Instances
To be protected 0
Protected 2
In progress 1
Abnormal 0

Protected Instances: 3

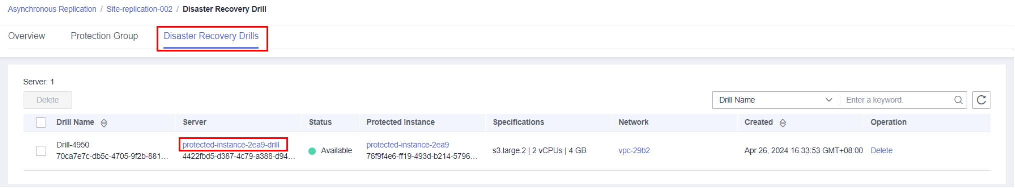
	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Creating disaster recovery drill	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More



Protected Instances: 3

	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Synchronization finished	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-Computin	Apr 26, 2024 15:...	Execute Planned Failover More

Step 9 After the drill is created, view the drill information on the **Disaster Recovery Drills** tab page. Alternatively, log in to the drill server and check whether services are running properly.



Asynchronous Replication / Site-replication-002 / Disaster Recovery Drill

Server: 1

	Drill Name	Server	Status	Protected Instance	Specifications	Network	Created	Operation
□	Drill-4950 70ca7e7c-db5c-4705-9f2b-881...	protected-instance-2ea9-drill 4422fbd5-d387-4c79-a388-d94...	● Available	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5796...	s3.large.2 | 2 vCPUs | 4 GB	vpc-29b2	Apr 26, 2024 16:33:53 GMT+08:00	Delete

----End

2.3.9 Deleting a Protected Instance

Scenarios

You can delete protected instances no longer needed to cancel the replication relationship between production site servers and disaster recovery site servers.

Deleting protected instances does not delete production site servers and has no impact on production site services.

Precautions

- In the scenario that a reverse reprotection is performed for a protected instance, you are advised to delete the instance after the initial data synchronization is complete.

Prerequisites

No operations are being performed on the protected instance.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

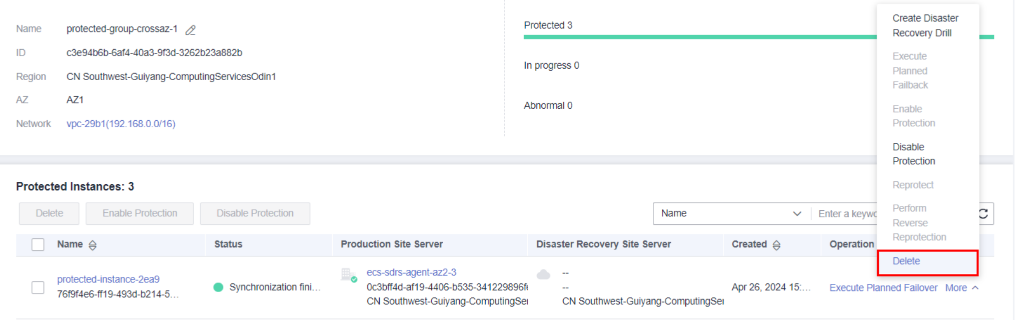
Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the protected instance you want to delete and click the number in the **Protected Instances** column.

The **Protection Groups** tab page is displayed.

Step 4 In the navigation pane, choose the protection group housing the target protected instance.

The protection group details page is displayed.

Step 5 In the **Protected Instances** area, locate the target protected instance, and choose **More** > **Delete** in the **Operation** column.



Name	protected-group-crossaz-1
ID	c3e94b6b-6af4-40a3-9f3d-3262b23a882b
Region	CN Southwest-Guiyang-ComputingServicesOdin1
AZ	AZ1
Network	vpc-29b1(192.168.0.0/16)

Protected 3

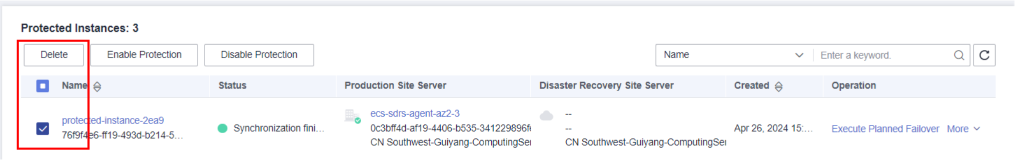
In progress 0

Abnormal 0

Protected Instances: 3

☐ Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☐ protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Synchronization fini...	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More

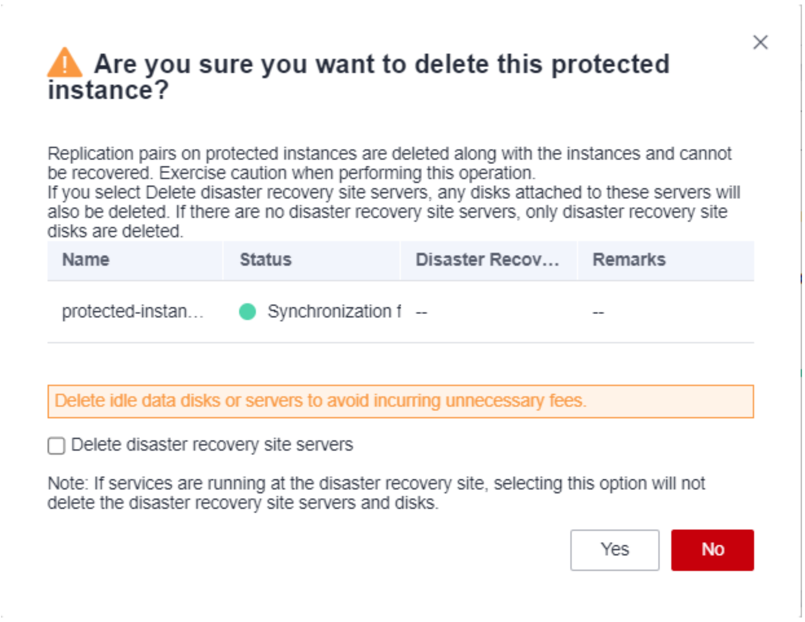
To delete protected instances in a batch, select the target protected instances and click **Delete** above the protected instance list.



Protected Instances: 3

■ Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
☑ protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Synchronization fini...	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More

Step 6 In the displayed dialog box, select the following option as required:



Are you sure you want to delete this protected instance?

Replication pairs on protected instances are deleted along with the instances and cannot be recovered. Exercise caution when performing this operation.
If you select Delete disaster recovery site servers, any disks attached to these servers will also be deleted. If there are no disaster recovery site servers, only disaster recovery site disks are deleted.

Name	Status	Disaster Recov...	Remarks
protected-instan...	● Synchronization f	--	--

Delete idle data disks or servers to avoid incurring unnecessary fees.

□ Delete disaster recovery site servers

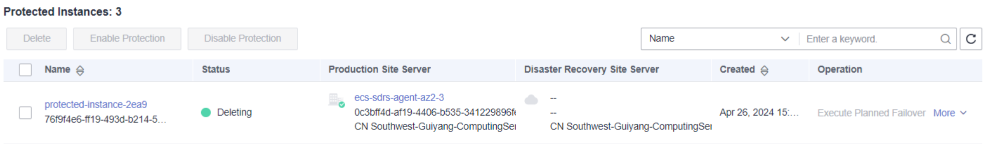
Note: If services are running at the disaster recovery site, selecting this option will not delete the disaster recovery site servers and disks.

Delete disaster recovery site servers

- If you do not select this option, the replication relationship between the production site server and disaster recovery site server is canceled, but the disaster recovery site server and disks are retained.
- If you select this option, the replication relationship between the production site server and disaster recovery site server is canceled, and the disaster recovery site server and disks are deleted. If there are no disaster recovery site servers, EVS disks will be deleted.

> NOTE
>
> If the protected instance is in the **Failover completed** or **Reverse reprotecting** state, meaning that services are running at the disaster recovery site, resources at the disaster recovery site will not be deleted regardless of whether you select this option or not.

Step 7 Click **Yes**. The protected instance status changes to **Deleting**.

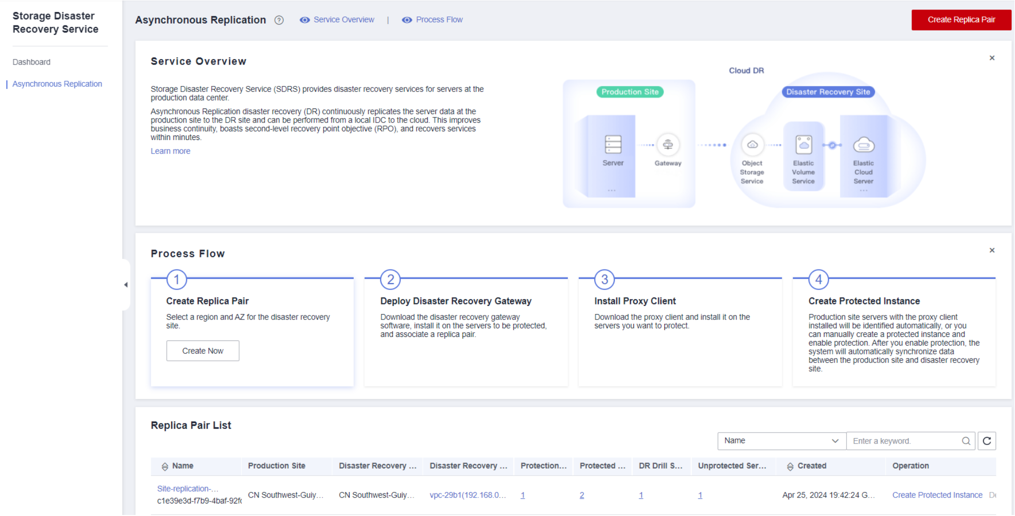


Protected Instances: 3

□	Name	Status	Production Site Server	Disaster Recovery Site Server	Created	Operation
□	protected-instance-2ea9 76f9f4e6-ff19-493d-b214-5...	● Deleting	ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896f CN Southwest-Guiyang-ComputingSe	-- -- CN Southwest-Guiyang-ComputingSe	Apr 26, 2024 15:...	Execute Planned Failover More

Step 8 After the deletion is complete, the production site server is moved in the list of **Unprotected servers**.

Deleting a protected instance does not delete its disaster recovery drills. To delete its drills, go to the **Diaster Recovery Drills** tab page, as shown in **Deleting a Disaster Recovery Drill**.



Service Overview

Storage Disaster Recovery Service (SDRS) provides disaster recovery services for servers at the production data center.

Asynchronous Replication disaster recovery (DR) continuously replicates the server data at the production site to the DR site and can be performed from a local IDC to the cloud. This improves business continuity, boasts second-level recovery point objective (RPO), and recovers services within minutes.

Learn more

Process Flow

1 Create Replica Pair

Select a region and AZ for the disaster recovery site.

2 Deploy Disaster Recovery Gateway

Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

3 Install Proxy Client

Download the proxy client and install it on the servers you want to protect.

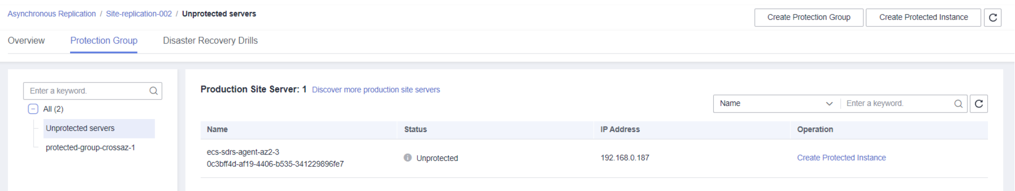
4 Create Protected Instance

Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Replica Pair List

Name | Enter a keyword.

Name	Production Site	Disaster Recovery ...	Disaster Recovery ...	Protection...	Protected ...	DR Drill S...	Unprotected Ser...	Created	Operation
Site-replication-... c1e39e3d-f7b9-4baf-92f(	CN Southwest-Guiy...	CN Southwest-Guiy...	vpc-29b1(192.168.0...	1	2	1	1	Apr 25, 2024 19:42:24 G...	Create Protected Instance De



Asynchronous Replication / Site-replication-002 / Unprotected servers

Production Site Server: 1 Discover more production site servers

Name | Enter a keyword.

Name	Status	IP Address	Operation
ecs-sdrs-agent-az2-3 0c3bff4d-af19-4406-b535-341229896fe7	Unprotected	192.168.0.187	Create Protected Instance

----End

2.4 Managing DR Drills

2.4.1 Deleting a Disaster Recovery Drill

Scenarios

Delete disaster recovery drills no longer needed to release the virtual resources. Drill servers are deleted along with drills.

Prerequisites

No operations are being performed on the disaster recovery drill.

Procedure

Step 1 Log in to the management console.

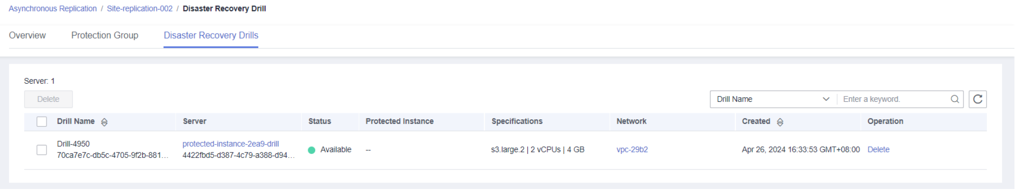
Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Choose **Asynchronous Replication**. In the right pane, locate the replica pair housing the disaster recovery drill you want to delete and click the replica pair name.

The **Overview** tab page is displayed.

Step 4 Click the **Disaster Recovery Drill** tab. In the drill list, locate the drill you want to delete and click **Delete** in the **Operation** column.



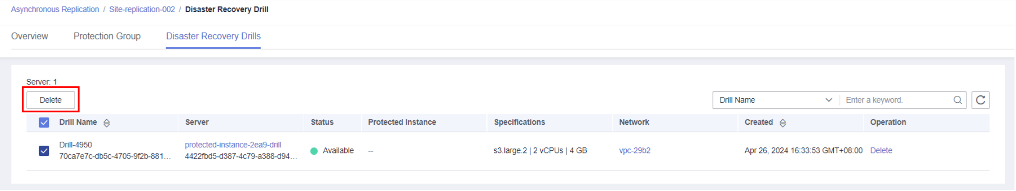
Asynchronous Replication / Site-replication-002 / Disaster Recovery Drill

Overview | Protection Group | Disaster Recovery Drills

Server: 1

	Drill Name	Server	Status	Protected Instance	Specifications	Network	Created	Operation
□	Drill-4950 70ca7e7c-db5c-4705-9f2b-881...	protected-instance-2ea9-drill 4422fbd5-d387-4c79-a388-d94...	● Available	--	s3.large.2 | 2 vCPUs | 4 GB	vpc-29b2	Apr 26, 2024 16:33:53 GMT+08:00	Delete

To delete drills in a batch, select the target drills and click **Delete** above the drill server list.



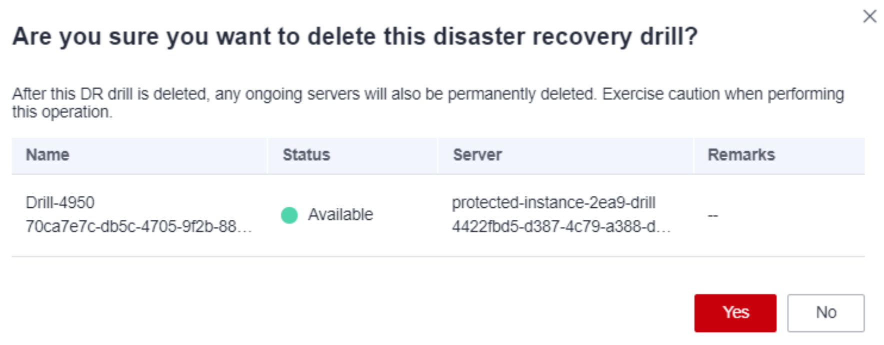
Asynchronous Replication / Site-replication-002 / Disaster Recovery Drill

Overview | Protection Group | Disaster Recovery Drills

Server: 1

☑	Drill Name	Server	Status	Protected Instance	Specifications	Network	Created	Operation
☑	Drill-4950 70ca7e7c-db5c-4705-9f2b-881...	protected-instance-2ea9-drill 4422fbd5-d387-4c79-a388-d94...	● Available	--	s3.large.2 | 2 vCPUs | 4 GB	vpc-29b2	Apr 26, 2024 16:33:53 GMT+08:00	Delete

Step 5 In the displayed dialog box, confirm drill information and click **Yes**.



Are you sure you want to delete this disaster recovery drill?

After this DR drill is deleted, any ongoing servers will also be permanently deleted. Exercise caution when performing this operation.

Name	Status	Server	Remarks
Drill-4950 70ca7e7c-db5c-4705-9f2b-88...	● Available	protected-instance-2ea9-drill 4422fbd5-d387-4c79-a388-d...	--

Step 6 The drill status changes to **Deleting**. After the drill is deleted, it disappears from the drill list.

The drill server is deleted along with the drill.

----End

2.5 Installing Clients

2.5.1 Installing a Disaster Recovery Gateway

Scenarios

To use SDRS, you need to deploy the cloud disaster recovery gateway at the production site.

The gateway aggregates and compresses I/Os received from production site servers and then transmits them to the disaster recovery site.

Prerequisites

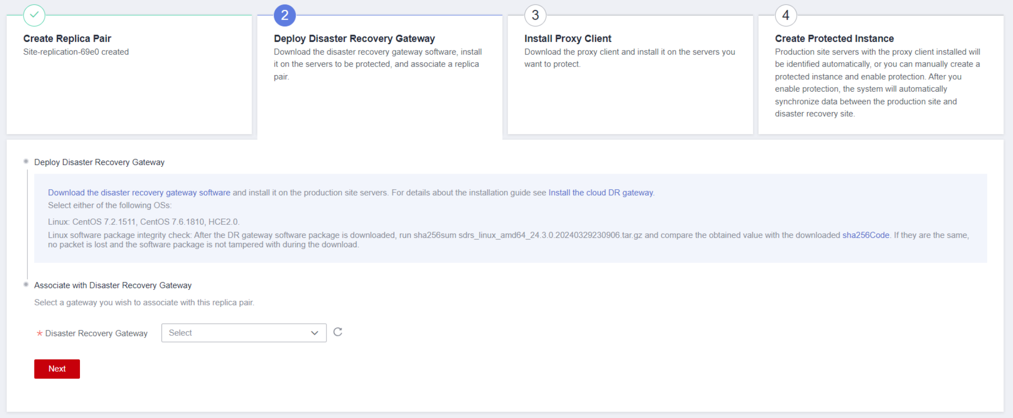
- The recommended ECS specifications to deploy the gateway are 8 vCPUs and 16 GB memory. Only Linux is supported, and Huawei Cloud EulerOS 2.0 and EulerOS 2.9/2.10 are recommended.
- The region, AZ, and VPC of the gateway ECS must be the same as those of the production site servers.
- It is recommended that you deploy the disaster recovery gateway and proxy client in the same security group and only allow ECSs within the security group to communication with each other. For details, see **Security Group Configuration Examples**.
- To ensure that the service can run properly, make sure that the ports described in section "Port Description (Asynchronous Replication)" are not used.

Procedure

In the following example, **sdrs_linux_amd64_24.3.0.20240329230906.tar.gz** is the package (24.3.0) used to install the gateway.

Step 1 Obtain the disaster recovery gateway package and upload it to a directory on the target ECS.

- **IDC-to-cloud**: Click the link on the console to download the package and upload it to the ECS where you want to deploy the gateway.



Create Replica Pair
Site-replication-69e0 created

Deploy Disaster Recovery Gateway
Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

Install Proxy Client
Download the proxy client and install it on the servers you want to protect.

Create Protected Instance
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

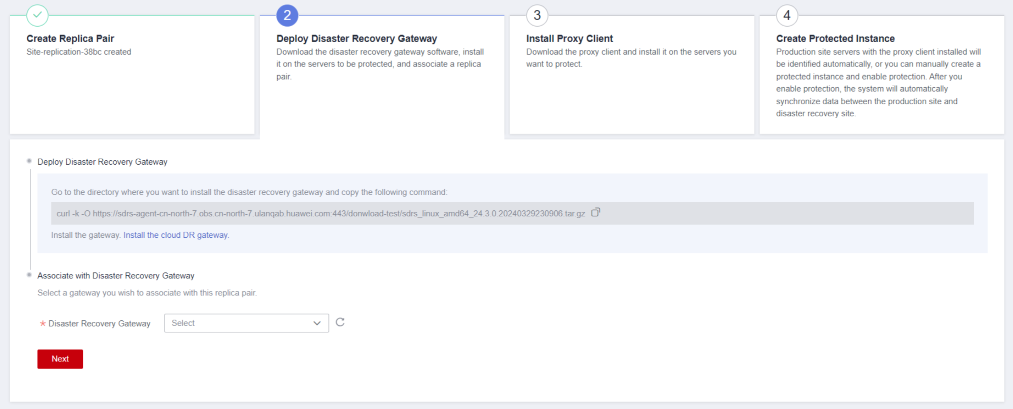
Deploy Disaster Recovery Gateway

Download the disaster recovery gateway software and install it on the production site servers. For details about the installation guide see Install the cloud DR gateway.
Select either of the following OSs:
Linux: CentOS 7.2.1511, CentOS 7.6.1810, HCE2.0.
Linux software package integrity check: After the DR gateway software package is downloaded, run sha256sum sdrs_linux_amd64_24.3.0.20240329230906.tar.gz and compare the obtained value with the downloaded sha256Code. If they are the same, no packet is lost and the software package is not tampered with during the download.

Associate with Disaster Recovery Gateway
Select a gateway you wish to associate with this replica pair.

* Disaster Recovery Gateway: Select

- **Cross-region** and **Cross-AZ**: Copy the command provided on the console, log in to the ECS where you want to deploy the gateway, go to the desired directory, and paste and run the command to obtain the package.



Create Replica Pair
Site-replication-38bc created

Deploy Disaster Recovery Gateway
Download the disaster recovery gateway software, install it on the servers to be protected, and associate a replica pair.

Install Proxy Client
Download the proxy client and install it on the servers you want to protect.

Create Protected Instance
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Deploy Disaster Recovery Gateway

Go to the directory where you want to install the disaster recovery gateway and copy the following command:

```
curl -k -O https://sdrs-agent-cn-north-7.obs.cn-north-7.ulanqab.huawei.com:443/donwload-test/sdrs_linux_amd64_24.3.0.20240329230906.tar.gz
```

Install the gateway. Install the cloud DR gateway.

Associate with Disaster Recovery Gateway
Select a gateway you wish to associate with this replica pair.

* Disaster Recovery Gateway: Select

Step 2 In the directory containing the package, and run the following command as user **root** to decompress the package:

tar -zxvf sdrs_linux_amd64_24.3.0.20240329230906.tar.gz

Step 3 Go to the directory containing the installation script.

cd sdrs_linux_amd64_24.3.0.20240329230906.tar.gz

Step 4 Install the gateway.

sh install.sh --drm-ip=*drm ip* **--dra-ip=***dra ip* **--role=gateway**

In the command, both *drm ip* and *dra ip* indicate the primary NIC IP address of ECS where the gateway is deployed.

If the command output contains the following information, the gateway has been installed:

```
...
Installed DRM successfully.
Installed SDRS successfully.
...
```

Step 5 Check whether the gateway is enabled.

ps -ef | grep java | grep drm

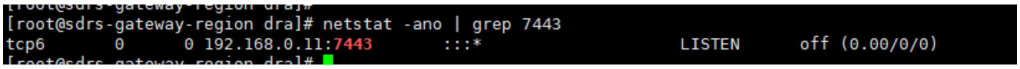
Information similar to the following is displayed:

```
service 2089 1 5 10:25 ? 00:01:12 /opt/cloud/sdrs/drm/tools/jre/bin/java -Djava.security.egd=file:/dev/
random -jar /opt/cloud/sdrs/drm/drm-24.3.0.jar --service.kernel.security.scc.config_path=file:/opt/cloud/
sdrs/drm/classes/scc --spring.config.location=/opt/cloud/sdrs/drm/classes/application.properties
```

If the command output contains the **drm** process, the gateway has been enabled.

Step 6 Check whether the gateway listening port is enabled.

netstat -ano | grep 7443



```
[root@sdrs-gateway-region dra]#
[root@sdrs-gateway-region dra]# netstat -ano | grep 7443
tcp6       0      0 192.168.0.11:7443       :::*                    LISTEN      off (0.00/0/0)
[root@sdrs-gateway-region dra]#
```

Step 7 After the installation is complete, delete the installation package and decompressed files.

----End

2.5.2 Configuring the Disaster Recovery Gateway

Scenarios

Before using the gateway and disaster recovery site servers for the first time, you need to configure the gateway.

Prerequisites

- The recommended ECS specifications to deploy the gateway are 8 vCPUs and 16 GB memory. Only Linux is supported, and Huawei Cloud EulerOS 2.0 and EulerOS 2.9/2.10 are recommended.
- The region, AZ, and VPC of the gateway ECS must be the same as those of the production site servers.

- It is recommended that you deploy the disaster recovery gateway and proxy client in the same security group and only allow ECSs within the security group to communication with each other. For details, see **Security Group Configuration Examples**.

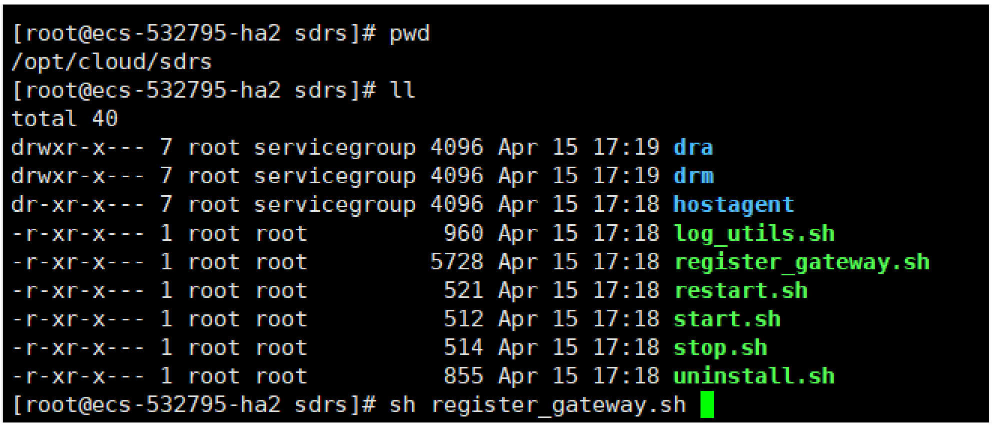
Procedure

In the following example, **sdrs_linux_amd64_24.3.0.20240329230906.tar.gz** is the package (24.3.0) used to configure the gateway.

Step 1 Run the following command in the **/opt/cloud/sdrs** directory to configure the gateway:

sh register_gateway.sh

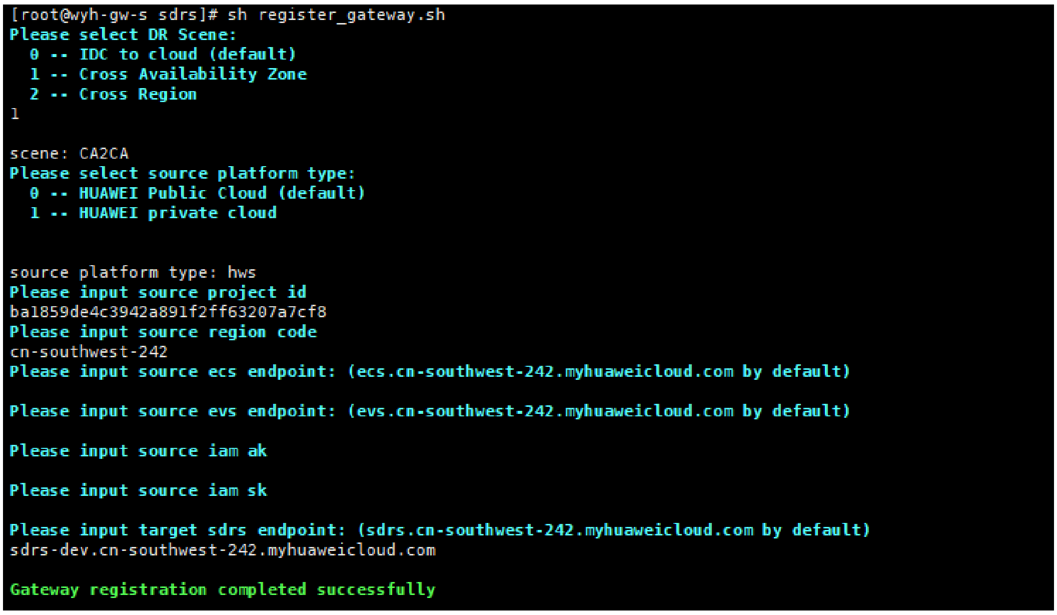
Figure 2-9 Executing the script



```
[root@ecs-532795-ha2 sdrs]# pwd
/opt/cloud/sdrs
[root@ecs-532795-ha2 sdrs]# ll
total 40
drwxr-x--- 7 root servicegroup 4096 Apr 15 17:19 dra
drwxr-x--- 7 root servicegroup 4096 Apr 15 17:19 drm
dr-xr-x--- 7 root servicegroup 4096 Apr 15 17:18 hostagent
-r-xr-x--- 1 root root          960 Apr 15 17:18 log_utils.sh
-r-xr-x--- 1 root root         5728 Apr 15 17:18 register_gateway.sh
-r-xr-x--- 1 root root          521 Apr 15 17:18 restart.sh
-r-xr-x--- 1 root root          512 Apr 15 17:18 start.sh
-r-xr-x--- 1 root root          514 Apr 15 17:18 stop.sh
-r-xr-x--- 1 root root          855 Apr 15 17:18 uninstall.sh
[root@ecs-532795-ha2 sdrs]# sh register_gateway.sh
```

1. In cross-AZ scenarios, configure the following parameters:

Figure 2-10 Script execution example in the cross-AZ scenario



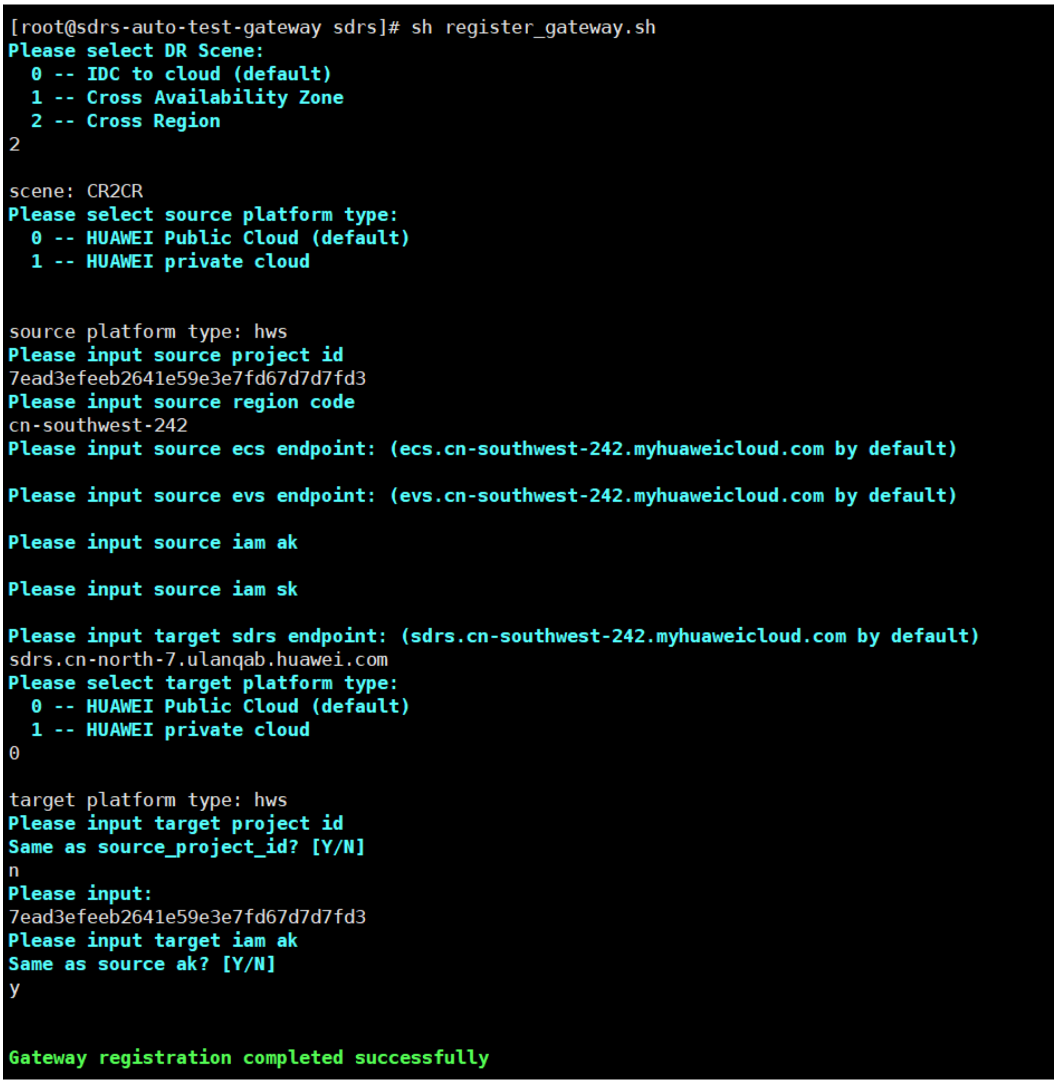
```
[root@wyh-gw-s sdrs]# sh register_gateway.sh
Please select DR Scene:
  0 -- IDC to cloud (default)
  1 -- Cross Availability Zone
  2 -- Cross Region
1

scene: CA2CA
Please select source platform type:
  0 -- HUAWEI Public Cloud (default)
  1 -- HUAWEI private cloud


source platform type: hws
Please input source project id
ba1859de4c3942a891f2ff63207a7cf8
Please input source region code
cn-southwest-242
Please input source ecs endpoint: (ecs.cn-southwest-242.myhuaweicloud.com by default)

Please input source evs endpoint: (evs.cn-southwest-242.myhuaweicloud.com by default)

Please input source iam ak

Please input source iam sk

Please input target sdrs endpoint: (sdrs.cn-southwest-242.myhuaweicloud.com by default)
sdrs-dev.cn-southwest-242.myhuaweicloud.com

Gateway registration completed successfully
```

Table 2-7 Parameter description

Parameter	Description	How to Obtain	Example Value
DR Scene	Replication	– **0**: IDC-to-cloud – **1**: Cross-AZ – **2**: Cross-region	1
source platform type	Type of the production site	– **0**: Huawei public cloud – **1**: Huawei private cloud	0
source project id	Project ID	Log in to the console and choose **My Credentials** > **API Credentials** to view the project ID.	51af777371904892a49a0c3e3e53de44
source region code	Destination region ID	Obtain the SDRS endpoint by referring to **SDRS Endpoints**.	cn-east-2
source ecs endpoint	ECS endpoint	Obtain the ECS endpoint by referring to **ECS Endpoints**.	-
source evs endpoint	EVS endpoint	Obtain the EVS endpoint by referring to **EVS Endpoints**.	-
source iam ak	Access key ID	Obtain AK/SK by referring to **How Do I Obtain an Access Key (AK/SK)?**	RZSAMHULWKKE71N0XHUT
source iam sk	Access key		K7bXplAT0pEpy4SAiN2fHUwEtxvgmK3IqyhqnMTA
target sdrs endpoint	SDRS endpoint	Obtain the SDRS endpoint by referring to **SDRS Endpoints**.	sdrs.cn-east-2.myhuaweicloud.com

2. In cross-region scenarios, configure the following parameters:

Figure 2-11 Script execution example in the cross-region scenario



```
[root@sdrs-auto-test-gateway sdrs]# sh register_gateway.sh
Please select DR Scene:
  0 -- IDC to cloud (default)
  1 -- Cross Availability Zone
  2 -- Cross Region
2

scene: CR2CR
Please select source platform type:
  0 -- HUAWEI Public Cloud (default)
  1 -- HUAWEI private cloud


source platform type: hws
Please input source project id
7ead3efeeb2641e59e3e7fd67d7d7fd3
Please input source region code
cn-southwest-242
Please input source ecs endpoint: (ecs.cn-southwest-242.myhuaweicloud.com by default)

Please input source evs endpoint: (evs.cn-southwest-242.myhuaweicloud.com by default)

Please input source iam ak

Please input source iam sk

Please input target sdrs endpoint: (sdrs.cn-southwest-242.myhuaweicloud.com by default)
sdrs.cn-north-7.ulanqab.huawei.com
Please select target platform type:
  0 -- HUAWEI Public Cloud (default)
  1 -- HUAWEI private cloud
0

target platform type: hws
Please input target project id
Same as source_project_id? [Y/N]
n
Please input:
7ead3efeeb2641e59e3e7fd67d7d7fd3
Please input target iam ak
Same as source ak? [Y/N]
y


Gateway registration completed successfully
```

Table 2-8 Parameter description

Parameter	Description	How to Obtain	Example Value
DR Scene	Replication	– **0**: IDC-to-cloud – **1**: Cross-AZ – **2**: Cross-region	2
source platform type	Type of the production site	– **0**: Huawei public cloud – **1**: Huawei private cloud	0

Parameter	Description	How to Obtain	Example Value
source project id	Project ID in the production region	Log in to the console and choose **My Credentials** > **API Credentials** to view the project ID.	51af777371904892a49a0c3e3e53de44
source region code	Destination region ID	Obtain the SDRS endpoint by referring to **SDRS Endpoints**.	cn-east-2
source ecs endpoint	ECS endpoint	Obtain the ECS endpoint by referring to **ECS Endpoints**.	-
source evs endpoint	EVS endpoint	Obtain the EVS endpoint by referring to **EVS Endpoints**.	-
source iam ak	Access key ID	Obtain AK/SK by referring to **How Do I Obtain an Access Key (AK/SK)?**	-
source iam sk	Access key		-
target sdrs endpoint	SDRS endpoint in the DR region	Obtain the SDRS endpoint by referring to **SDRS Endpoints**.	sdrs.cn-east-2.myhuaweicloud.com
target platform type	Type of the disaster recovery site	– **0**: Huawei public cloud – **1**: Huawei private cloud	0
target project id	Project ID in the disaster recovery region	Log in to the console and choose **My Credentials** > **API Credentials** to view the project ID.	51af777371904892a49a0c3e3e53de44
target iam ak	Access key ID	Obtain AK/SK by referring to **How Do I Obtain an Access Key (AK/SK)?**	-
target iam sk	Access key		-

----End

2.5.3 Installing the Proxy Client

Scenarios

Asynchronous replication provides server-level protection if production site applications cannot be recovered within a short period of time due to force majeure (fire and earthquake) or device faults (faulty software and hardware). You can quickly recover services at the disaster recovery site with simple configurations.

Prerequisites

- To ensure that the service can run properly, make sure that the ports described in section "Port Description (Asynchronous Replication)" are not used.
- If the firewall is enabled on the ECS where you want to deploy the proxy client, enable port 59526 on the firewall.
- It is recommended that you deploy the disaster recovery gateway and proxy client in the same security group and only allow ECSs within the security group to communication with each other. For details, see **Security Group Configuration Examples**.

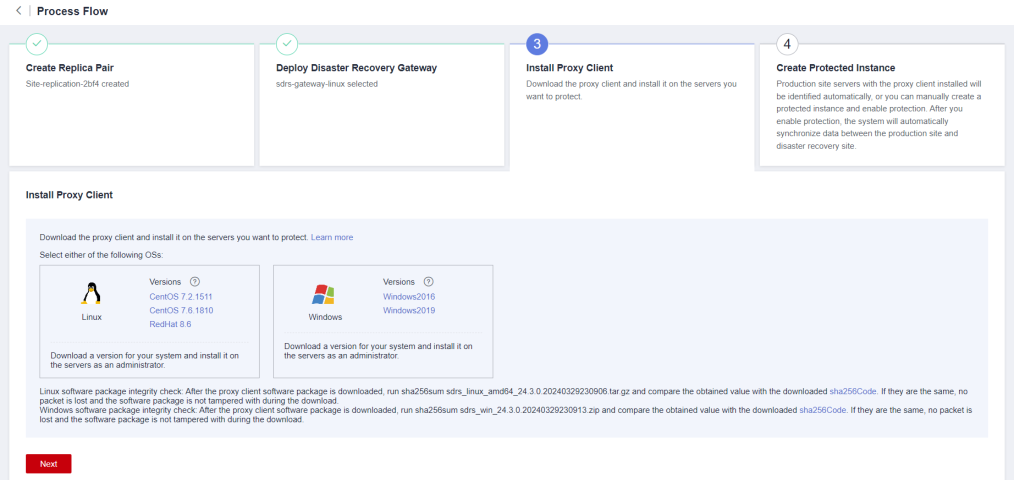
Procedure

Linux

In the following example, **sdrs_linux_amd64_24.3.0.20240329230906.tar.gz** is the package (24.3.0) used to install the proxy client on CentOS.

Step 1 Obtain the proxy client package and upload it to a directory on the target server. Ensure the package integrity by comparing the sha256 value in advance.

- **IDC-to-cloud**: Click the link on the console to download the package and upload it to the target server.



Download the proxy client and install it on the servers you want to protect.

Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Install Proxy Client

Download the proxy client and install it on the servers you want to protect. Learn more

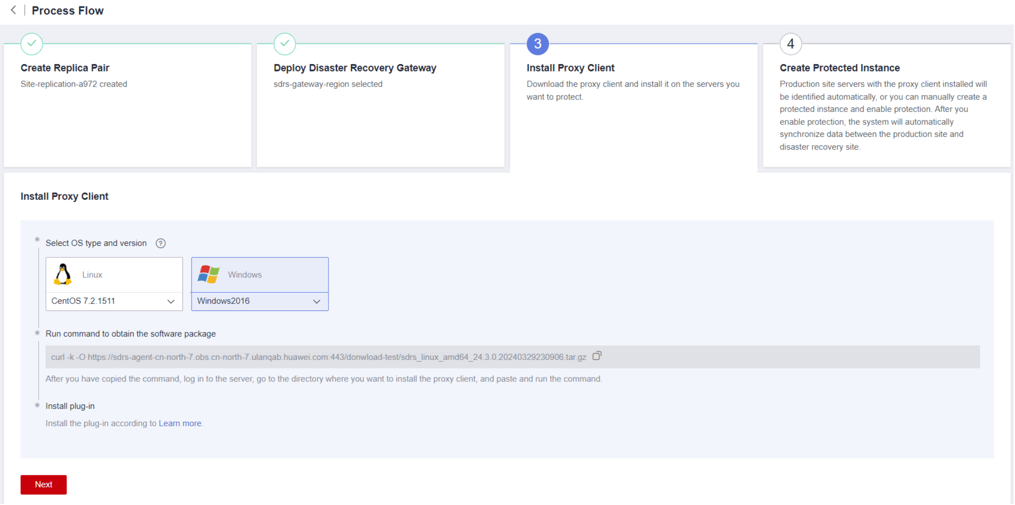
Select either of the following OSs:

Download a version for your system and install it on the servers as an administrator.

Download a version for your system and install it on the servers as an administrator.

Linux software package integrity check: After the proxy client software package is downloaded, run sha256sum sdrs_linux_amd64_24.3.0.20240329230906.tar.gz and compare the obtained value with the downloaded sha256Code. If they are the same, no packet is lost and the software package is not tampered with during the download.
Windows software package integrity check: After the proxy client software package is downloaded, run sha256sum sdrs_win_24.3.0.20240329230913.zip and compare the obtained value with the downloaded sha256Code. If they are the same, no packet is lost and the software package is not tampered with during the download.

- **Cross-region** and **Cross-AZ**: Select the OS type and version of your production server on the console and copy the command provided. Then, log in to the production server, go to the desired directory, and paste and run the command to obtain the package.



Process Flow

✓ **Create Replica Pair**
Site-replication-a972 created

✓ **Deploy Disaster Recovery Gateway**
sdrs-gateway-region selected

3 **Install Proxy Client**
Download the proxy client and install it on the servers you want to protect.

4 **Create Protected Instance**
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Install Proxy Client

Select OS type and version

Linux: CentOS 7.2.1511

Windows: Windows2016

Run command to obtain the software package

```
curl -k -O https://sdrs-agent-cn-north-7.obs.cn-north-7.ulanqab.huawei.com:443/donwload-test/sdrs_linux_amd64_24.3.0.20240329230906.tar.gz
```

After you have copied the command, log in to the server, go to the directory where you want to install the proxy client, and paste and run the command.

Install plug-in

Install the plug-in according to Learn more.

Step 2 In the directory containing the package, and run the following command as user **root** to decompress the package:

tar -zxvf sdrs_linux_amd64_24.3.0.20240329230906.tar.gz

Step 3 Go to the directory containing the installation script.

cd sdrs_linux_amd64_24.3.0.20240329230906

Step 4 Install the proxy client.

sh install.sh --hostagent-ip=*hostagent ip* **--drm-ip=***drm ip* **--role=all**

In the preceding command, *hostagent ip* indicates the IP address of the proxy client. Set it to the IP address of the primary NIC of the server you want to install the proxy client. *drm ip* indicates the IP address of the cloud disaster recovery gateway.

If the command output contains the following information, the proxy client has been installed:

```
...
Installed SDRS successfully.
...
```

Step 5 After the installation is complete, delete the installation package and decompressed files.

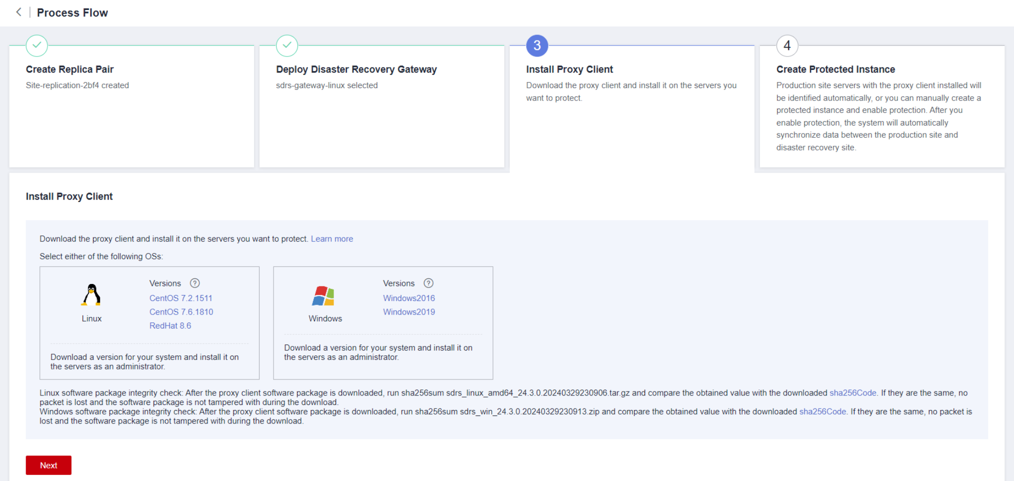
----End

Windows

In the following example, **sdrs_win_24.3.0.20240329230913.zip** is the package (24.3.0) used to install the proxy client on Windows Server 2019.

Step 1 Obtain the proxy client package and upload it to a directory on the target server. Ensure the package integrity by comparing the sha256 value in advance.

- **IDC-to-cloud**: Click the link on the console to download the package and upload it to the target server.



< | **Process Flow**

✓ **Create Replica Pair**
Site-replication-2bf4 created

✓ **Deploy Disaster Recovery Gateway**
sdrs-gateway-linux selected

3 **Install Proxy Client**
Download the proxy client and install it on the servers you want to protect.

4 **Create Protected Instance**
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Install Proxy Client

Download the proxy client and install it on the servers you want to protect. Learn more

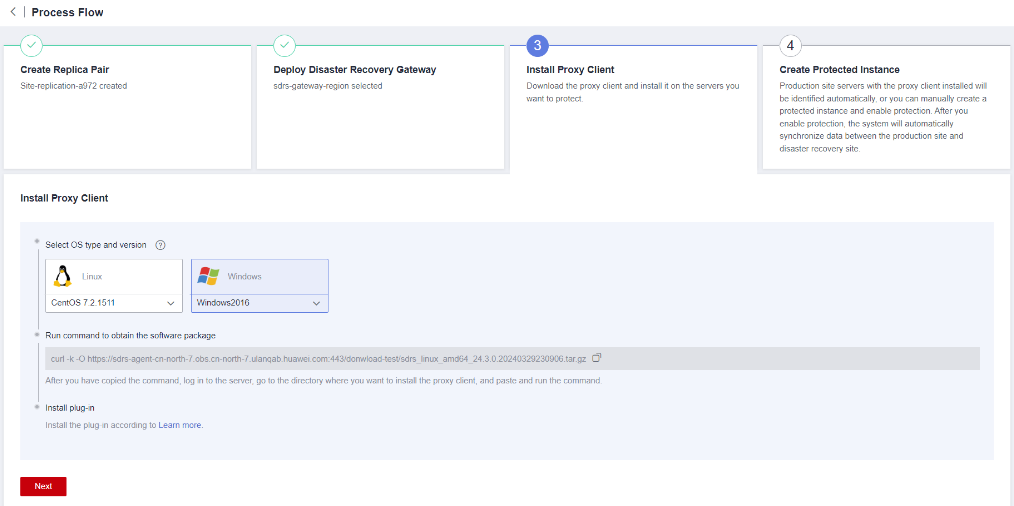
Select either of the following OSs:

Linux — Versions: CentOS 7.2.1511, CentOS 7.6.1810, RedHat 8.6
Download a version for your system and install it on the servers as an administrator.

Windows — Versions: Windows2016, Windows2019
Download a version for your system and install it on the servers as an administrator.

Linux software package integrity check: After the proxy client software package is downloaded, run sha256sum sdrs_linux_amd64_24.3.0.20240329230906.tar.gz and compare the obtained value with the downloaded sha256Code. If they are the same, no packet is lost and the software package is not tampered with during the download.
Windows software package integrity check: After the proxy client software package is downloaded, run sha256sum sdrs_win_24.3.0.20240329230913.zip and compare the obtained value with the downloaded sha256Code. If they are the same, no packet is lost and the software package is not tampered with during the download.

- **Cross-region** and **Cross-AZ**: Select the OS type and version of your production server on the console and copy the command provided. Then, log in to the production server, go to the desired directory, and paste and run the command to obtain the package.



< | **Process Flow**

✓ **Create Replica Pair**
Site-replication-a972 created

✓ **Deploy Disaster Recovery Gateway**
sdrs-gateway-region selected

3 **Install Proxy Client**
Download the proxy client and install it on the servers you want to protect.

4 **Create Protected Instance**
Production site servers with the proxy client installed will be identified automatically, or you can manually create a protected instance and enable protection. After you enable protection, the system will automatically synchronize data between the production site and disaster recovery site.

Install Proxy Client

Select OS type and version
Linux: CentOS 7.2.1511
Windows: Windows2016

Run command to obtain the software package

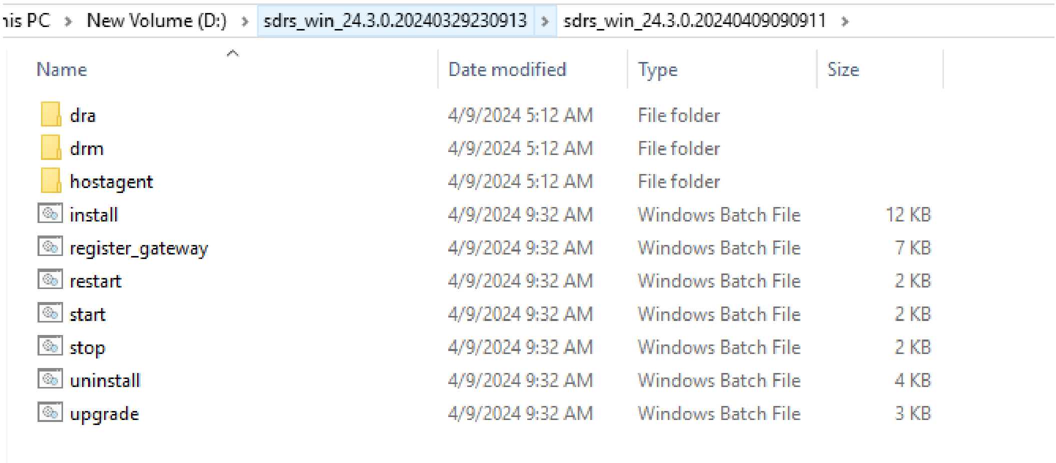
```
curl -k -O https://sdrs-agent-cn-north-7.obs.cn-north-7.ulanqab.huawei.com:443/donwload-test/sdrs_linux_amd64_24.3.0.20240329230906.tar.gz
```

After you have copied the command, log in to the server, go to the directory where you want to install the proxy client, and paste and run the command.

Install plug-in
Install the plug-in according to Learn more.

Step 2 In the directory containing the package, right-click the package to decompress it.

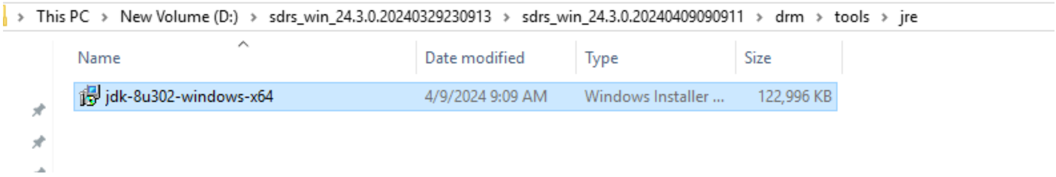
Step 3 Double-click the decompressed directory to go to the directory containing the installation script.



ıis PC > New Volume (D:) > sdrs_win_24.3.0.20240329230913 > sdrs_win_24.3.0.20240409090911 >

Name	Date modified	Type	Size
dra	4/9/2024 5:12 AM	File folder	
drm	4/9/2024 5:12 AM	File folder	
hostagent	4/9/2024 5:12 AM	File folder	
install	4/9/2024 9:32 AM	Windows Batch File	12 KB
register_gateway	4/9/2024 9:32 AM	Windows Batch File	7 KB
restart	4/9/2024 9:32 AM	Windows Batch File	2 KB
start	4/9/2024 9:32 AM	Windows Batch File	2 KB
stop	4/9/2024 9:32 AM	Windows Batch File	2 KB
uninstall	4/9/2024 9:32 AM	Windows Batch File	4 KB
upgrade	4/9/2024 9:32 AM	Windows Batch File	3 KB

Step 4 If the JDK is not installed on the production server, go to the **drm\tools\jre** directory, double-click the JDK installation program, and install JDK as prompted.



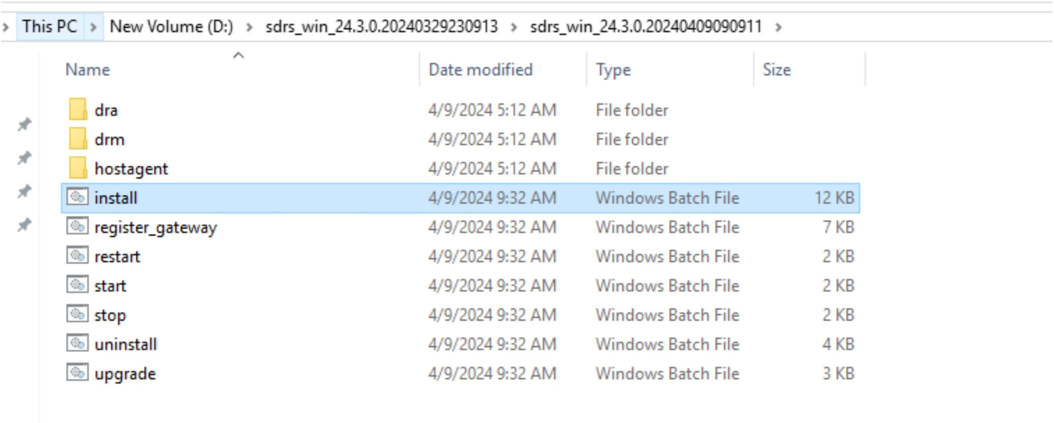
This PC > New Volume (D:) > sdrs_win_24.3.0.20240329230913 > sdrs_win_24.3.0.20240409090911 > drm > tools > jre

Name	Date modified	Type	Size
jdk-8u302-windows-x64	4/9/2024 9:09 AM	Windows Installer ...	122,996 KB

NOTICE

SDRS requires that the JDK version is jdk.8u261 or later. If the installed version is earlier than jdk.8u261, upgrade JDK.

Step 5 Double-click **install.bat** to run the script.



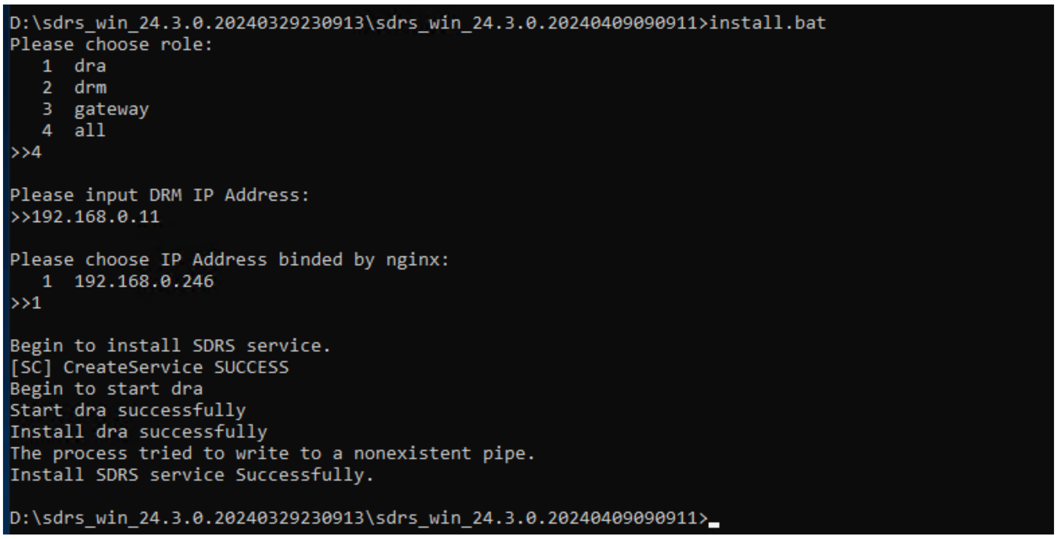
This PC > New Volume (D:) > sdrs_win_24.3.0.20240329230913 > sdrs_win_24.3.0.20240409090911 >

Name	Date modified	Type	Size
dra	4/9/2024 5:12 AM	File folder	
drm	4/9/2024 5:12 AM	File folder	
hostagent	4/9/2024 5:12 AM	File folder	
install	4/9/2024 9:32 AM	Windows Batch File	12 KB
register_gateway	4/9/2024 9:32 AM	Windows Batch File	7 KB
restart	4/9/2024 9:32 AM	Windows Batch File	2 KB
start	4/9/2024 9:32 AM	Windows Batch File	2 KB
stop	4/9/2024 9:32 AM	Windows Batch File	2 KB
uninstall	4/9/2024 9:32 AM	Windows Batch File	4 KB
upgrade	4/9/2024 9:32 AM	Windows Batch File	3 KB

Enter the parameters as prompted.

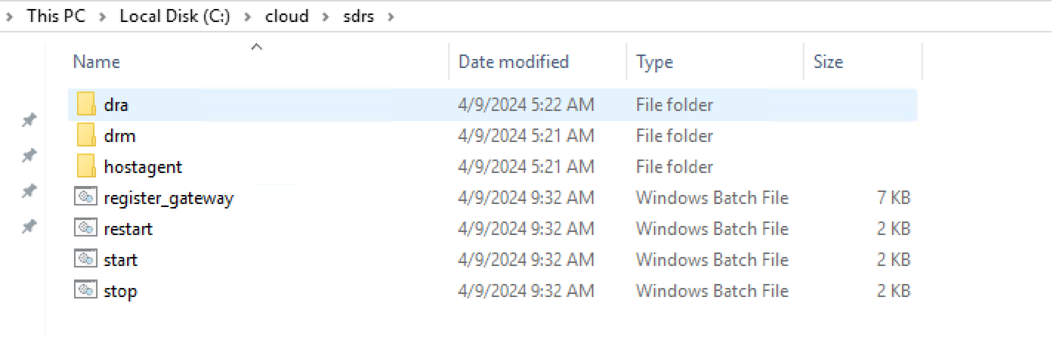
1. Select **all** for **role**.
2. Enter the gateway IP address for **DRM IP Address**.
3. If the production server has multiple NICs, all the IP addresses bound by Nginx will be displayed, enter the serial number of the IP address you required.

Figure 2-12 Proxy client installation example



```
D:\sdrs_win_24.3.0.20240329230913\sdrs_win_24.3.0.20240409090911>install.bat
Please choose role:
   1  dra
   2  drm
   3  gateway
   4  all
>>4

Please input DRM IP Address:
>>192.168.0.11

Please choose IP Address binded by nginx:
   1  192.168.0.246
>>1

Begin to install SDRS service.
[SC] CreateService SUCCESS
Begin to start dra
Start dra successfully
Install dra successfully
The process tried to write to a nonexistent pipe.
Install SDRS service Successfully.

D:\sdrs_win_24.3.0.20240329230913\sdrs_win_24.3.0.20240409090911>_
```

Step 6 The proxy client is installed in the **C:\cloud\sdrs** directory. After the installation is complete, manually delete the installation package and decompressed files.



Name	Date modified	Type	Size
dra	4/9/2024 5:22 AM	File folder	
drm	4/9/2024 5:21 AM	File folder	
hostagent	4/9/2024 5:21 AM	File folder	
register_gateway	4/9/2024 9:32 AM	Windows Batch File	7 KB
restart	4/9/2024 9:32 AM	Windows Batch File	2 KB
start	4/9/2024 9:32 AM	Windows Batch File	2 KB
stop	4/9/2024 9:32 AM	Windows Batch File	2 KB

----End

3 Synchronous Replication Management (for Installed Base Operations)

3.1 Managing Protection Groups

3.1.1 Disabling Protection

Scenarios

Disable protection for all resources in a protection group.

After protection is disabled, data synchronization stops for all protected instances in this group.

Prerequisites

- The protection group contains replication pairs.
- The protection group status is **Protecting** or **Disabling protection failed**.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the desired protection group, click **Protected Instances**.

The protection group details page is displayed.

Step 4 In the upper right corner of the page, click **Disable Protection**.

Step 5 In the displayed dialog box, click **Yes**.

After protection is disabled, data synchronization between the production site and disaster recovery site for all protected instances in the protection group will stop.

----End

3.1.2 Performing a Switchover

Scenarios

After you perform a switchover, services at the production site are switched to the DR site, and services at the DR site are switched over to the production site. **Table 3-1** shows the direction change.

Table 3-1 DR direction change after a switchover

-	Production Site	DR Site
Before	AZ1	AZ2
After	AZ2	AZ1

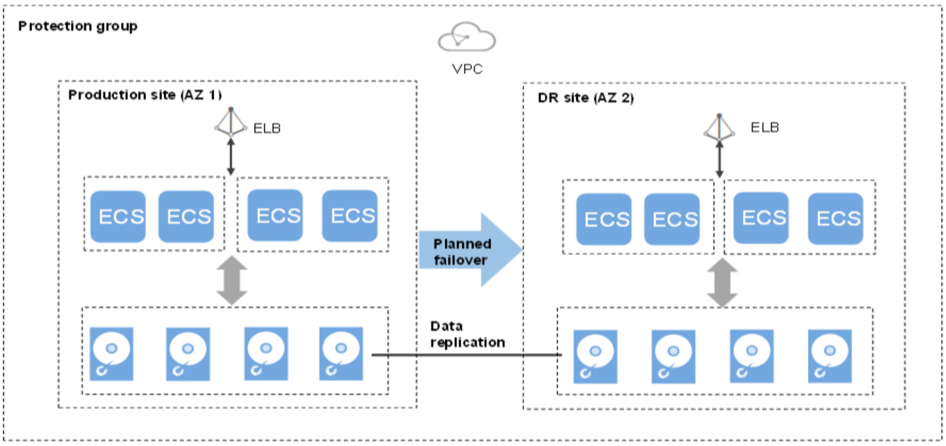
After the switchover, data synchronization continues, but the DR direction is changed from the DR site to the production site. You can perform a switchover when you are certain that the production site will encounter an interruption. For example, if the production site (AZ1) is going to encounter a power failure, you can perform a switchover to switch services in AZ1 to the DR site (AZ2). The switchover does not affect data synchronization of the protection group.

SDRS will migrate NICs on the server during the switchover. Once completed, the IP, EIP, and MAC addresses of the production site server will be migrated to the DR site server, so that the IP, EIP, and MAC addresses remain the same.

NOTE

- Check the status to ensure that all the servers in the protection group are stopped before a switchover.
- During a switchover, do not start the servers in the protection group. Otherwise, the switchover may fail.
- Once a switchover is complete, data synchronization will not stop, only the synchronization direction will reverse.
- Once a switchover is complete, the status of the protection group changes to **Protecting**. Then, you need to go to the protected instance details page and start the production site server.

Figure 3-1 Performing a switchover



Notes

For Linux servers with Cloud-Init installed, if you have changed **hostname** of the production site server before you perform a switchover for the first time, this modification will not synchronize to the DR site server.

To resolve this problem, see **What Can I Do If hostname of the Production Site Server and DR Site Server Are Different After a Switchover or Failover?**

Prerequisites

- All the servers in the protection group are stopped.
- The protection group has replication pairs.
- Protection is enabled for the protection group, and the protection group is in the **Protecting** or **Switchover failed** state.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the desired protection group, click **Protected Instances**.

Step 4 In the upper right corner of the page, click **Execute Switchover**.

Step 5 In the displayed dialog box, check whether all the servers in this protection group are stopped.

- If yes, go to step **Step 6**.
- If no, select the servers to be stopped and click **Stop**.

Step 6 In the displayed dialog box, click **Execute Switchover**.

NOTE

During a switchover, do not start the servers in the protection group. Or, the switchover may fail.

----End

3.1.3 Performing a Failover

Scenarios

When the servers and disks at the production site become faulty due to force majeure, you can perform a failover for them and enable the servers and disks at the DR site to ensure the service continuity.

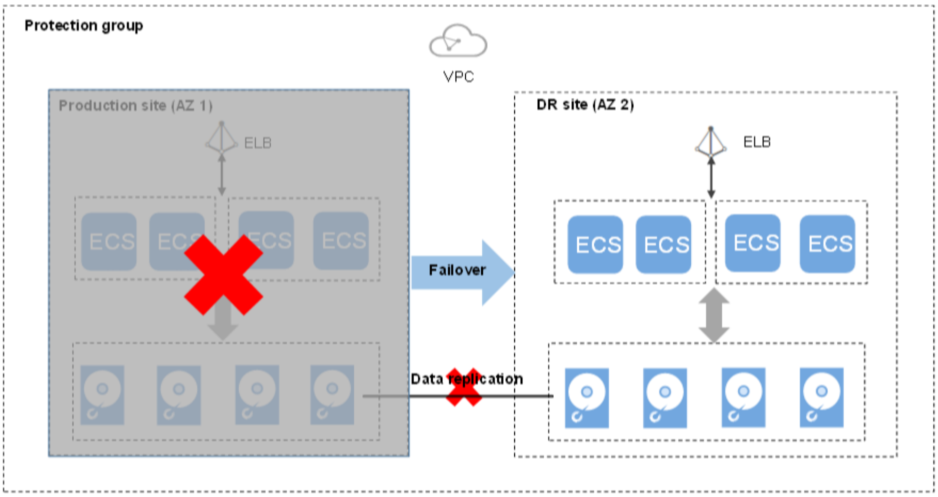
Once you perform a failover, the DR site servers and disks become available immediately. You can power on the servers, or use Cloud Server Backup Service (CSBS) or Volume Backup Service (VBS) to restore the data to a specified data recovery point.

SDRS will migrate NICs on the server during the failover. After the failover, the IP, EIP, and MAC addresses of the production site server will be migrated to the DR site server, so that the IP, EIP, and MAC addresses remain the same.

NOTE

- Once the failover is started, data synchronization stops.
- After the failover is complete, the status of the protection group changes to **Failover complete**. Then, you need to switch to the protected instance details page and start the DR site server.

Figure 3-2 Performing a failover



Notes

For Linux servers with Cloud-Init installed, if you have changed **hostname** of the production site server before you perform a failover for the first time, this modification will not synchronize to the DR site server.

To resolve this problem, see **What Can I Do If hostname of the Production Site Server and DR Site Server Are Different After a Switchover or Failover?**

Prerequisites

- You have confirmed that servers and disks in the production AZ are faulty, and the deployed services become unavailable. If you cannot confirm the information, **submit a service ticket** for help.
- The protection group contains replication pairs.
- Protection is enabled for the protection group, and the protection group is in the **Protecting**, **Switchover failed**, or **Failover failed** state.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the desired protection group, click **Protected Instances**.

The protection group details page is displayed.

Step 4 In the upper right corner of the page, click **More** and choose **Fail Over** from the drop-down list.

The **Fail Over** dialog box is displayed.

Step 5 Click **Fail Over**.

During the failover, do not start or stop the servers in the protection group. Otherwise, the failover may fail.

----End

Related Operations

- After the failover is complete, the status of the protection group changes to **Failover complete**. Then, you need to switch to the protected instance details page and manually start the DR site server.
- After the failover is complete, the protection group is in the **Protection disabled** state. You need to enable protection again to start data synchronization. For details, see **Performing Reprotection**.

3.1.4 Performing Reprotection

Scenarios

Once the failover is started, data synchronization stops. After the failover is complete, the protection group is in the **Protection disabled** state. To restart data synchronization, perform steps provided in this section.

Prerequisites

- The protection group has replication pairs.
- The protection group is in the **Failover complete** or **Re-enabling protection failed**.
- The DR site server is stopped.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the desired protection group, click **Protected Instances**.

Step 4 In the upper right corner of the page, click **More** and choose **Reprotect** from the drop-down list.

The **Reprotect** dialog box is displayed.

Step 5 Check whether all the DR site servers in this protection group are stopped.

- If yes, go to step **Step 6**.
- If no, select the servers to be stopped and click **Stop**.

Step 6 On the **Reprotect** dialog box, click **Reprotect**.

During the reprotection, do not start the DR site servers in the protection group. Otherwise, the reprotection may fail.

----End

3.1.5 Deleting a Protection Group

Scenarios

Delete protection groups that are no longer needed to release resources.

Prerequisites

All the protected instances, DR drills, and replication pairs have been deleted from the protection group.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the protection group to be deleted, click **More** and choose **Delete** from the drop-down list.

Step 4 In the displayed dialog box, confirm information and click **Yes**.

----End

3.2 Managing Protected Instances

3.2.1 Modifying Specifications of a Protected Instance

Scenarios

If the specifications of an existing protected instance cannot meet the service requirements, you can perform steps provided in this section to modify the server specifications, including the vCPU and memory.

The following scenarios may involve:

- Modifying the specifications of both the production and DR site servers
- Modifying the specifications of the production site server only
- Modifying the specifications of the DR site server only

Prerequisites

- The protection group is in the **Available** or **Protecting state**.
- The protected instance is in the **Available**, **Protecting**, or **Modifying specifications failed**.
- Servers of which the specifications to be modified are stopped.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the protection group for which the protected instance specifications are to be modified, click **Protected Instances**.

The operation page for the protection group is displayed.

Step 4 On the **Protected Instances** tab, locate the row containing the target protected instance, click **More** in the **Operation** column, and choose **Modify Production Site Server Specifications** or **Modify DR Site Server Specifications** from the drop-down list.

Step 5 In the displayed dialog box, select new server type, vCPU, and memory specifications.

Step 6 (Optional) If you need to modify the specifications of both the production site server and DR site server, select **Modify the specifications of both the production and DR site servers**. After you select this item, the system will modify the specifications of both the production site server and DR site server to the same specifications.

NOTE

This item is deselected by default, indicating that the system modifies the specifications of only the production site server or DR site server.

Step 7 Click **OK**.

To ensure proper server running, do not perform any operations to the servers during specification modifications.

----End

3.2.2 Deleting a Protected Instance

Scenarios

If you do not need a protected instance, delete it to cancel the protection relationship between the servers and the protection group.

When you delete a protected instance, the production site server in the protected instance will not be deleted, and services at the production site will not be affected.

Prerequisites

The protected instance is in the **Available**, **Protecting**, **Failover complete**, **Creation failed**, **Enabling protection failed**, **Disabling protection failed**, **Switchover failed**, **Failover failed**, **Deletion failed**, **Re-enabling protection failed**, **Modifying specifications failed**, **Invalid**, or **Faulty** state.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the protection group for which the protected instance is to be deleted, click **Protected Instances**.

The protection group details page is displayed.

Step 4 On the **Protected Instances** tab, locate the row containing the protected instance to be deleted, click **More** in the **Operation** column, and choose **Delete** from the drop-down list.

To delete protected instances in batches, select the target protected instances and click **Delete** above the protected instance list.

The **Delete Protected Instance** page is displayed.

Step 5 On the **Delete Protected Instance** page, select the desired operation.

NOTE

- If you select **Delete DR site server**, do not perform any other operations on the DR site server or its related resources when the system is deleting the DR site server.

- Delete DR site server
  - If you do not select this option, the protection relationship between the protected instance and protection group will be canceled, but the DR site server and disks attached to the server will be retained.
  - If you select this option, the protection relationship between the protected instance and protection group will be canceled, and the DR site server and disks attached to the server will be deleted.
- Release the EIP bound to the following DR site server

  This parameter is displayed when you select **Delete DR site server**.
  - If you do not select this option, the DR site server will be deleted, but the EIP bound to the server will be retained.
  - If you select this option, the DR site server will be deleted, and the EIP bound to the server will be released.

Step 6 Click **Yes**.

----End

3.2.3 Creating a Replication Pair

Scenarios

Create replication pairs for desired disks of a specified protection group. When you create a replication pair:

- If the protection group status is **Available**, protection is disabled. Creating the replication pair only establishes the replication relationship between the production site disk and DR site disk, but data between the disks is not synchronized. To synchronize data, enable protection.
- If the protection group status is **Protecting**, protection is enabled. After a replication pair has been created, data synchronization automatically starts.

NOTE

In a replication pair, the name of the DR site disk is the same as that of the production site disk, but their IDs are different.

To change disk name, click the disk name on the replication pair details page to go to the disk details page and change it.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- If the servers in the protection group are ECSs, ensure that the disks used to create replication pairs are in the **Available** state.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Locate the protection group where you want to add replication pairs and click **Replication Pairs**.

The protection group details page is displayed.

Step 4 On the **Replication Pairs** tab, click **Create Replication Pair**.

The **Create Replication Pair** page is displayed.

Step 5 Set the parameters by referring to **Table 3-2**.

Table 3-2 Parameter description

Parameter	Description	Example Value
Protection Group Name	Name of the protection group where you want to create replication pairs. You do not need to configure it.	Protection-Group-test

Parameter	Description	Example Value
Protection Group ID	ID of the protection group	619c57e9-3927-48f8-ad14-3e293260b8a0
DR Direction	Replication direction of the protection group. You do not need to configure it.	-
Production Site	AZ where the production site resides	-
Production Site Disk	This parameter is mandatory. The following two options are available: ● **EVS** ● **DSS**	EVS
DR Site Disk	This parameter is mandatory. The following two options are available: ● **EVS** ● **DSS** **NOTE** Disks are classified as EVS and DSS disks based on whether the storage resources used by the disks are exclusive. DSS disks are provided for users exclusively. Determine whether to use DSS disks for the DR site. The disks at the production and DR site do not need to be of the same type.	EVS
Storage Pool	● If you select **EVS** for **DR Site Disk**, **Storage Pool** is not required. ● If you select **DSS** for **DR Site Disk**, **Storage Pool** is mandatory.	dss-01

Parameter	Description	Example Value
Replication Pair	Replication pair name. This parameter is mandatory. A replication pair name is defined for classification and future search.	replication_001

NOTE

DR Site Disk and **Storage Pool** are available only when **DSS** is selected.

Step 6 Click **Create Now**.

Step 7 On the **Confirm** page, confirm the replication pair information.

- If you do not need to modify the information, click **Submit**.
- If you need to modify the information, click **Previous**.

Step 8 Click **Back to Protection Group Details Page** and view the replication pair list.

If the replication pair status changes to **Available** or **Protecting**, it has been created successfully.

----End

3.2.4 Attaching a Replication Pair

Scenarios

You can attach a replication pair to a protected instance. Then, the production site disk is attached to the production site server, and the DR site disk is attached to the DR site server.

After protection is enabled for a protection group, when data is written into the production site disk, the same data is written into the DR site disk synchronously.

Restrictions and Limitations

- If there are five replication pairs that are not attached to any protected instance, you cannot create any new replication pair.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- The protected instance is in the **Available** or **Protecting** state.
- The replication pair is in the **Available** or **Protecting** state.
- The non-shared replication pair has not been attached to any protected instance.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Locate the protection group where you want to attach replication pairs and click **Protected Instances**.

The protection group details page is displayed.

Step 4 On the **Protected Instances** tab, locate the row containing the desired protected instance and click **Attach** in the **Operation** column.

The **Attach Replication Pair** page is displayed.

Step 5 Select the replication pair, select a desired device name, and click **OK**.

The replication pair is attached to the specified protected instance.

----End

3.2.5 Detaching a Replication Pair

Scenarios

Detach replication pairs from protected instances. After a replication pair is detached from a protected instance, the replication relationship between the two disks remains, but the server data can no longer be written to the disks.

Prerequisites

- The protection group is in the **Available**, **Protecting**, **Failover complete**, **Enabling protection failed**, **Disabling protection failed**, **Switchover failed**, or **Failover failed** state.
- The protected instance is in the **Available**, **Protecting**, **Failover complete**, **Enabling protection failed**, **Disabling protection failed**, **Switchover failed**, **Failover failed**, **Deletion failed**, **Re-enabling protection failed**, **Modifying specifications failed**, **Invalid**, or **Faulty** state.
- The replication pair is in the **Available**, **Protecting**, **Failover complete**, **Attaching failed**, **Detaching failed**, **Enabling protection failed**, **Disabling protection failed**, **Switchover failed**, **Failover failed**, **Deletion failed**, **Re-enabling protection failed**, **Expansion failed**, **Invalid**, or **Faulty** state.
- The replication pair has been attached.
- Disks in the **In-use** state have been attached to the production and DR site servers.

NOTE

- A system disk (attached to **/dev/sda** or **/dev/vda**) can be detached only when the server is in the **Stopped** state. Therefore, stop the server before detaching the system disk.
- Data disks can be detached online or offline, which means that the server containing the disks can either be in the **Running** or **Stopped** state.

  For details about how to detach a disk online, see **Disk** > **Detaching an EVS Disk from a Running ECS** in the *Elastic Cloud Server User Guide*.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Locate the protection group where you want to detach replication pairs and click **Protected Instances**.

The protection group details page is displayed.

Step 4 On the **Protected Instances** tab, locate the row containing the desired protected instance and click **Detach** in the **Operation** column.

The **Detach Replication Pair** page is displayed.

Step 5 Select the replication pair to be detached and click **Yes**.

After the operation succeeds, the server data can no longer be written to the disks.

----End

3.2.6 Adding a NIC

Scenarios

If more NICs are required for your protected instance, you can perform steps provided in this section to add a NIC to the protected instance.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- The protected instance is in the **Available** or **Protecting** state.
- The subnet of the NIC to be added must belong to the same VPC of the protection group and protected instance.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the protection group, click **Protected Instances**.

The operation page for the protection group is displayed.

Step 4 On the **Protected Instances** tab, click the protected instance.

The protected instance details page is displayed.

Step 5 Click the **NICs** tab and click **Add NIC**.

Step 6 Select the security group and subnet to be added.

NOTE

- You can select multiple security groups. When multiple security groups are selected, the access rules of all the selected security groups apply on the server.
- If you want to add a NIC with a specified IP address, enter an IP address into the **Private IP Address** field.

Step 7 Click **OK**.

----End

3.2.7 Deleting a NIC

Scenarios

A protected instance can have up to 12 NICs, including one primary NIC that cannot be deleted. You can perform steps provided in this section to delete a NIC other than the primary one.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- The protected instance is in the **Available** or **Protecting** state.
- The primary NIC cannot be deleted.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the protection group for which a NIC is to be deleted from the protected instance, click **Protected Instances**.

The operation page for the protection group is displayed.

Step 4 On the **Protected Instances** tab, click the protected instance.

The protected instance details page is displayed.

Step 5 Click the **NICs** tab. Then, click **Delete** in the row that contains the NIC to be deleted.

Step 6 Click **Yes**.

----End

3.3 Managing Replication Pairs

3.3.1 Creating a Replication Pair

Scenarios

Create replication pairs for desired disks of a specified protection group. When you create a replication pair:

- If the protection group status is **Available**, protection is disabled. Creating the replication pair only establishes the replication relationship between the production site disk and DR site disk, but data between the disks is not synchronized. To synchronize data, enable protection.
- If the protection group status is **Protecting**, protection is enabled. After a replication pair has been created, data synchronization automatically starts.

NOTE

In a replication pair, the name of the DR site disk is the same as that of the production site disk, but their IDs are different.

To change disk name, click the disk name on the replication pair details page to go to the disk details page and change it.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- If the servers in the protection group are ECSs, ensure that the disks used to create replication pairs are in the **Available** state.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Locate the protection group where you want to add replication pairs and click **Replication Pairs**.

The protection group details page is displayed.

Step 4 On the **Replication Pairs** tab, click **Create Replication Pair**.

The **Create Replication Pair** page is displayed.

Step 5 Set the parameters by referring to **Table 3-3**.

Table 3-3 Parameter description

Parameter	Description	Example Value
Protection Group Name	Name of the protection group where you want to create replication pairs. You do not need to configure it.	Protection-Group-test
Protection Group ID	ID of the protection group	619c57e9-3927-48f8-ad14-3e293260b8a0
DR Direction	Replication direction of the protection group. You do not need to configure it.	-
Production Site	AZ where the production site resides	-
Production Site Disk	This parameter is mandatory. The following two options are available: ● **EVS** ● **DSS**	EVS
DR Site Disk	This parameter is mandatory. The following two options are available: ● **EVS** ● **DSS** **NOTE** Disks are classified as EVS and DSS disks based on whether the storage resources used by the disks are exclusive. DSS disks are provided for users exclusively. Determine whether to use DSS disks for the DR site. The disks at the production and DR site do not need to be of the same type.	EVS
Storage Pool	● If you select **EVS** for **DR Site Disk**, **Storage Pool** is not required. ● If you select **DSS** for **DR Site Disk**, **Storage Pool** is mandatory.	dss-01

Parameter	Description	Example Value
Replication Pair	Replication pair name. This parameter is mandatory. A replication pair name is defined for classification and future search.	replication_001

NOTE

DR Site Disk and **Storage Pool** are available only when **DSS** is selected.

Step 6 Click **Create Now**.

Step 7 On the **Confirm** page, confirm the replication pair information.

- If you do not need to modify the information, click **Submit**.
- If you need to modify the information, click **Previous**.

Step 8 Click **Back to Protection Group Details Page** and view the replication pair list.

If the replication pair status changes to **Available** or **Protecting**, it has been created successfully.

----End

3.3.2 Expanding Capacity of a Replication Pair

Scenarios

If the replication pair capacity of your protection group cannot meet your service requirements, you can expand the capacities of replication pairs. Replication pair capacity cannot be reduced, and their capacity expansion cannot be rolled back.

After you expand the capacity of a replication pair, capacities of both the production and DR site disks are changed.

Prerequisites

- The replication pair must be in the **Available**, **Protecting**, or **Expansion failed** state.
- Disks in the replication pair are in the **Available** or **In-use** state.
- Capacity expansion is not supported for replication pairs consist of yearly/monthly disks. To expand the capacity of such a replication pair, delete the replication pair, expand the capacity of the production site disk, and then use the disk to create a new replication pair.

NOTE

- For replication pairs consist of non-shared disks:

  If the disk status is **In-use**, the replication pair capacity can be expanded only when online capacity expansion is supported. If online capacity expansion is not supported, the **Expand Capacity** button will be grayed out.
- For replication pairs consist of shared disks:

  Online capacity expansion is not supported.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 Locate the protection group where you want to expand the replication pair capacity and click **Replication Pairs**.

The protection group details page is displayed.

Step 4 On the **Replication Pairs** tab, locate the row containing the target replication pair and click **Expand Capacity** in the **Operation** column.

The **Expand Capacity** page is displayed.

Step 5 On the **Expand Capacity** page, confirm the replication pair information, configure **Add Capacity**, and click **Next**.

Step 6 Confirm the information and click **Submit**.

If you want to modify the configuration, click **Previous**.

----End

3.3.3 Deleting a Replication Pair

Scenarios

If a replication pair is no longer used, you can release the associated virtual resources by deleting the replication pair.

When you delete a replication pair, the production site disk in the replication pair will not be deleted. You can decide whether to delete the DR site disk.

Prerequisites

- The protection group is in the **Available**, **Protecting**, **Failover complete**, **Enabling protection failed**, **Disabling protection failed**, **Switchover failed**, **Failover failed**, Deletion failed, or **Re-enabling protection failed** state.
- The replication pair is in the **Available**, **Protecting**, **Failover complete**, **Creation failed**, **Enabling protection failed**, **Disabling protection failed**, **Switchover failed**, **Failover failed**, **Deletion failed**, **Re-enabling protection failed**, **Attaching failed**, **Expansion failed**, **Invalid**, or **Faulty** state.
- The replication pair is not attached to any protected instance. For details about how to detach a replication pair, see **Detaching a Replication Pair**.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the protection group, click **Replication Pairs**.

The protection group details page is displayed.

Step 4 On the **Replication Pairs** tab, locate the row containing the replication pair to be deleted and click **Delete** in the **Operation** column.

The **Delete Replication Pair** dialog box is displayed.

NOTE

When you delete a replication pair, the production site disk will not be deleted.

Step 5 Determine the subsequent operation.

Delete DR Site Disk

- If you do not select this option, the replication relationship between the production site disk and DR site disk will be canceled, and the DR site disk will be retained.
- If you select this option, the replication relationship between the production site disk and DR site disk will be canceled, and the DR site disk will be deleted.

Step 6 Click **Yes**.

----End

3.4 Managing DR Drills

3.4.1 Deleting a DR Drill

Scenarios

If a DR drill is no longer used, you can release the virtual resources by deleting the DR drill from the system. When you delete a DR drill, all the drill servers in it are automatically deleted.

Prerequisites

The DR drill is in the **Available**, **Creation failed**, or **Deletion failed** state.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

The **Storage Disaster Recovery Service** page is displayed.

Step 3 In the pane of the protection group from which a DR drill is to be deleted, click **DR Drills**.

The operation page for the protection group is displayed.

Step 4 On the **DR Drills** tab, locate the row containing the DR drill to be deleted and click **Delete** in the **Operation** column.

The **Delete DR Drill** dialog box is displayed.

NOTE

If you bind an EIP to a DR drill server, the EIP will be unbound from the DR drill server when you delete the DR drill but will not be deleted. You can bind the EIP to another server.

Step 5 Click **Yes**.

----End

3.5 Interconnecting with CTS

3.5.1 Key SDRS Operations Recorded by CTS

Table 3-4 SDRS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a protection group	protectionGroup	createProtectionGroup
Deleting a protection group	protectionGroup	deleteProtectionGroup
Updating a protection group	protectionGroup	updateProtectionGroup
Enabling protection for a protection group (when the protection group is in the **Available** state)	protectionGroup	startProtectionGroup
Enabling protection for a protection group (when the protection group is in the **failed-over** state)	protectionGroup	reprotectProtectionGroup
Disabling protection for a protection group	protectionGroup	stopProtectionGroup
Performing a failover for a protection group	protectionGroup	failoverProtectionGroup

Operation	Resource Type	Trace Name
Reprotecting a protection group	protectionGroup	reverseProtectionGroup
Action performed when a job of the protection group failed to submit	protectionGroup	protectionGroupAction
Creating a protected instance	protectedInstance	createProtectedInstance
Deleting a protected instance	protectedInstance	deleteProtectedInstance
Updating a protected instance	protectedInstance	updateProtectedInstance
Attaching a replication pair to a protected instance	protectedInstance	attachReplicationPair
Detaching a replication pair from a protected instance	protectedInstance	detachReplicationPair
Adding a NIC to a protected instance	protectedInstance	addNic
Deleting a NIC from a protected instance	protectedInstance	deleteNic
Modifying the specifications of a protected instance	protectedInstance	resizeProtectedInstance
Creating a replication pair	replicationPair	createReplicationPair
Deleting a replication pair	replicationPair	deleteReplicationPair
Updating a replication pair	replicationPair	updateReplicationPair
Expanding the capacity of a replication pair	replicationPair	expandReplicationPair
Creating a DR drill	disasterRecoveryDrill	createDrDrill
Deleting a DR drill	disasterRecoveryDrill	deleteDrDrill
Updating a DR drill	disasterRecoveryDrill	updateDrDrill

3.5.2 Viewing Traces

Scenarios

After you enable CTS, the system starts recording operations on SDRS. You can view operation records of the last seven days on the management console.

Procedure

1. Log in to the management console.
2. Click **Service List** and select **Cloud Trace Service** under **Management & Deployment**.
3. In the navigation pane, choose **Trace List**.
4. In the upper right corner of the trace list, click **Filter** to set the search criteria.

   The following four filters are available:

   - **Trace Source**, **Resource Type**, and **Search By**
     - Select a filter criterion from the drop-down list. Select **SDRS** for **Trace Source**.
     - When you select **Trace name** for **Search By**, you need to select a specific trace name.
     - When you select **Resource ID** for **Search By**, you need to select or enter a specific resource ID.
     - When you select **Resource name** for **Search By**, you need to select or enter a specific resource name.
   - **Operator**: Select a specific operator (at user level rather than tenant level).
   - **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.
   - **Time Range**: You can query traces generated during any time range of the last seven days.
5. Click ⌄ on the left of the required trace to expand its details.
6. Locate a trace and click **View Trace** in the **Operation** column.

3.6 Managing Quotas

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

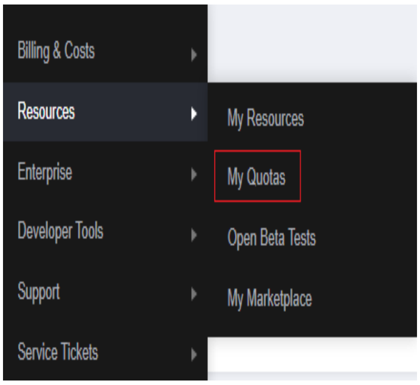
If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.

   Figure 3-3 My Quotas

4. View the used and total quota of each type of resources on the displayed page.

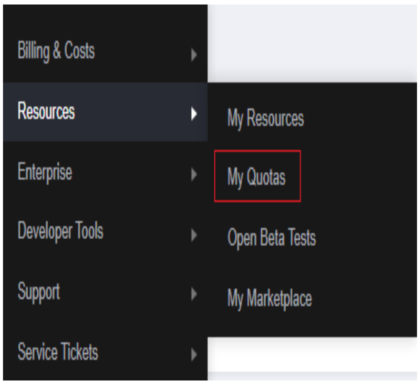
   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

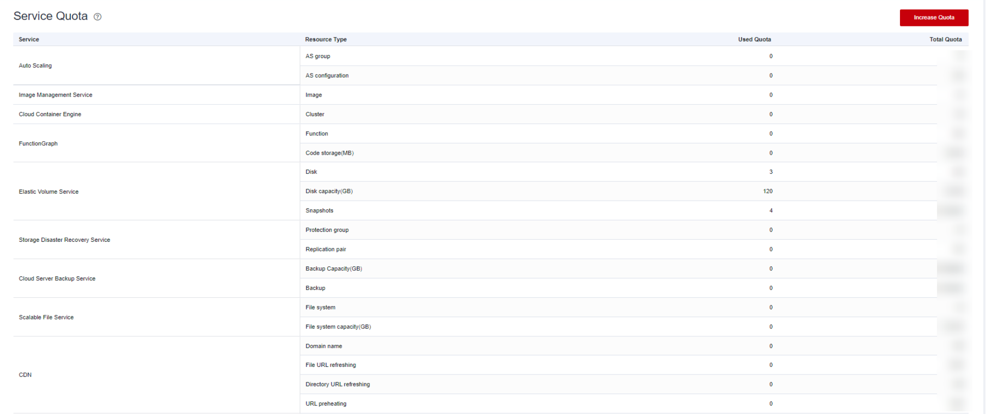
   The **Service Quota** page is displayed.

   Figure 3-4 My Quotas

3. Click **Increase Quota** in the upper right corner of the page.

Figure 3-5 Increasing quota



Service Quota

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	[redacted]
	AS configuration	0	[redacted]
Image Management Service	Image	0	[redacted]
Cloud Container Engine	Cluster	0	[redacted]
FunctionGraph	Function	0	[redacted]
	Code storage(MB)	0	[redacted]
Elastic Volume Service	Disk	3	[redacted]
	Disk capacity(GB)	120	[redacted]
	Snapshots	4	[redacted]
Storage Disaster Recovery Service	Protection group	0	[redacted]
	Replication pair	0	[redacted]
Cloud Server Backup Service	Backup Capacity(GB)	0	[redacted]
	Backup	0	[redacted]
Scalable File Service	File system	0	[redacted]
	File system capacity(GB)	0	[redacted]
CDN	Domain name	0	[redacted]
	File URL refreshing	0	[redacted]
	Directory URL refreshing	0	[redacted]
	URL preheating	0	[redacted]

4. On the **Create Service Ticket** page, configure parameters as required.

   In the **Problem Description** area, fill in the content and reason for adjustment.

5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

4 Appendixes

4.1 Configuring Disaster Recovery Site Servers

Scenarios

Configure disaster recovery site servers before you perform reverse reprotection for the protected instances on the console.

Procedure

Step 1 Log in to a disaster recovery site server.

Step 2 Run the require script to configure the gateway.

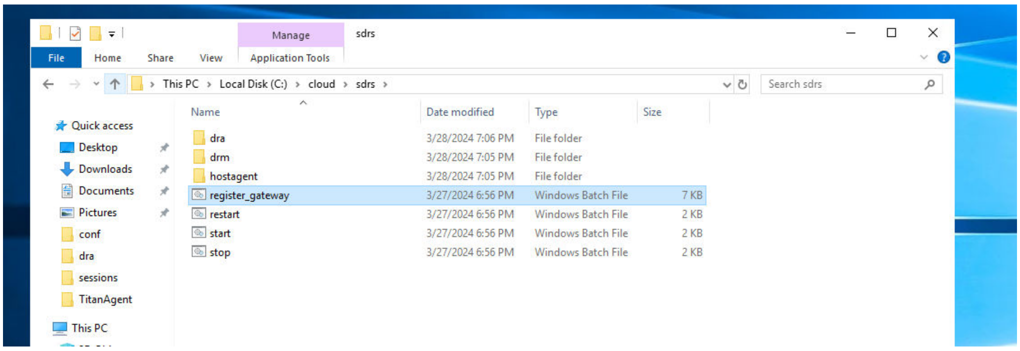
- Linux server:

  sh /opt/cloud/sdrs/register_gateway.sh

- Windows server:

  Go to the **C:\cloud\sdrs** directory and double-click **register_gateway.bat** to run the script.

Figure 4-1 Windows configuration script

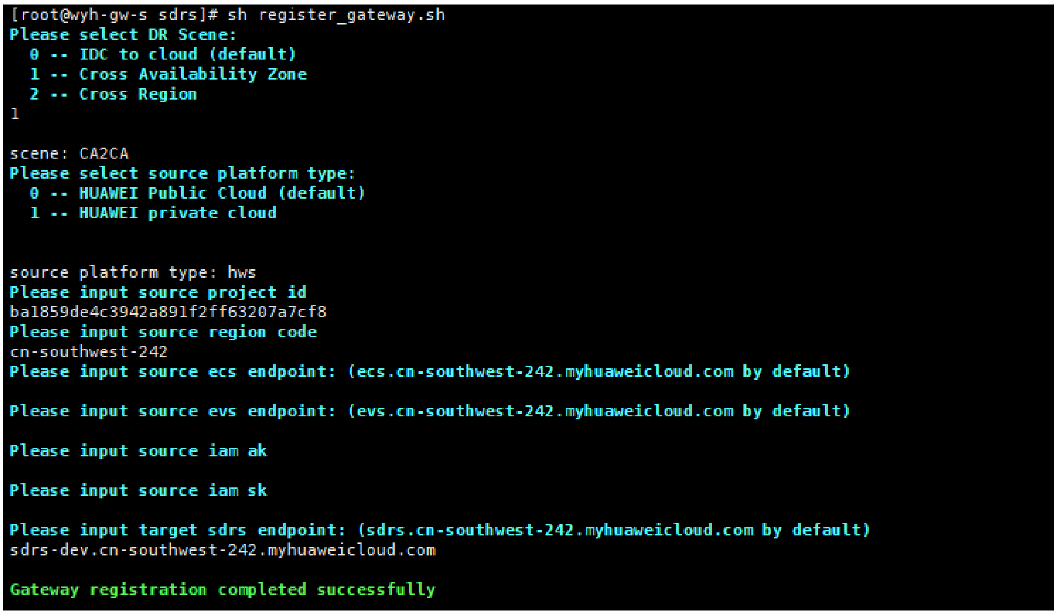


Name	Date modified	Type	Size
dra	3/28/2024 7:06 PM	File folder	
drm	3/28/2024 7:05 PM	File folder	
hostagent	3/28/2024 7:05 PM	File folder	
register_gateway	3/27/2024 6:56 PM	Windows Batch File	7 KB
restart	3/27/2024 6:56 PM	Windows Batch File	2 KB
start	3/27/2024 6:56 PM	Windows Batch File	2 KB
stop	3/27/2024 6:56 PM	Windows Batch File	2 KB

Step 3 Configure the script parameters.

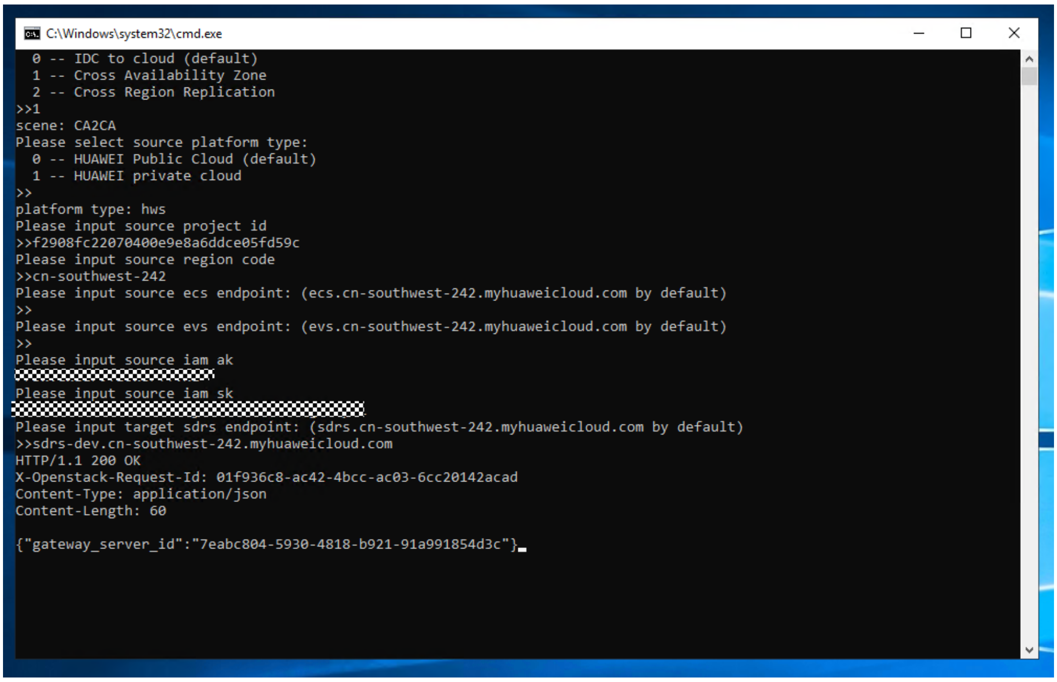
1. **Cross-AZ scenario:**

Figure 4-2 Example configuration in Linux



```
[root@wyh-gw-s sdrs]# sh register_gateway.sh
Please select DR Scene:
  0 -- IDC to cloud (default)
  1 -- Cross Availability Zone
  2 -- Cross Region
1

scene: CA2CA
Please select source platform type:
  0 -- HUAWEI Public Cloud (default)
  1 -- HUAWEI private cloud


source platform type: hws
Please input source project id
ba1859de4c3942a891f2ff63207a7cf8
Please input source region code
cn-southwest-242
Please input source ecs endpoint: (ecs.cn-southwest-242.myhuaweicloud.com by default)

Please input source evs endpoint: (evs.cn-southwest-242.myhuaweicloud.com by default)

Please input source iam ak

Please input source iam sk

Please input target sdrs endpoint: (sdrs.cn-southwest-242.myhuaweicloud.com by default)
sdrs-dev.cn-southwest-242.myhuaweicloud.com

Gateway registration completed successfully
```

Figure 4-3 Example configuration in Windows



```
  0 -- IDC to cloud (default)
  1 -- Cross Availability Zone
  2 -- Cross Region Replication
>>1
scene: CA2CA
Please select source platform type:
  0 -- HUAWEI Public Cloud (default)
  1 -- HUAWEI private cloud
>>
platform type: hws
Please input source project id
>>f2908fc22070400e9e8a6ddce05fd59c
Please input source region code
>>cn-southwest-242
Please input source ecs endpoint: (ecs.cn-southwest-242.myhuaweicloud.com by default)
>>
Please input source evs endpoint: (evs.cn-southwest-242.myhuaweicloud.com by default)
>>
Please input source iam ak
[redacted]
Please input source iam sk
[redacted]
Please input target sdrs endpoint: (sdrs.cn-southwest-242.myhuaweicloud.com by default)
>>sdrs-dev.cn-southwest-242.myhuaweicloud.com
HTTP/1.1 200 OK
X-Openstack-Request-Id: 01f936c8-ac42-4bcc-ac03-6cc20142acad
Content-Type: application/json
Content-Length: 60

{"gateway_server_id":"7eabc804-5930-4818-b921-91a991854d3c"}
```

Table 4-1 describes the variables in the command.

Table 4-1 Cross-AZ scenario parameters

Site	Parameter	Description	How to Obtain	Example Value
Replication	replicationScene	Replication scenario. There are three replication scenarios.	– **0**: IDC-to-cloud – **1**: Cross-AZ – **2**: Cross-region	1
Disaster recovery site on Huawei Cloud	platform_type	Platform type	– **0**: Huawei public cloud – **1**: Huawei private cloud	0
	sourceProjectId	Project ID	Log in to the console and choose **My Credentials** > **API Credentials** to view the project ID.	51af777371904892a49a0c3e3e53de44
	sourceEcs	ECS endpoint	Obtain the ECS endpoint by referring to **ECS Endpoints**.	-
	sourceEvs	EVS endpoint	Obtain the EVS endpoint by referring to **EVS Endpoints**.	-
	sourceIamAk	Access key ID	Obtain AK/SK by referring to **How Do I Obtain an Access Key (AK/SK)?**	-
	sourceIamSk	Secret access key		-
Disaster recovery site on Huawei Cloud	targetProjectId	Project ID	Log in to the console and choose **My Credentials** > **API Credentials** to view the project ID.	0605767cb280d5762fd6c0133d6bea3f
	targetSdrs	SDRS endpoint	Obtain the SDRS endpoint by referring to **SDRS Endpoints**.	sdrs.cn-east-2.myhuaweicloud.com
	targetIamAk	Access key ID	Obtain AK/SK by referring to **How Do I Obtain an Access Key (AK/SK)?**	RZSAMHULWKKE71N0XHUT
	targetIamSk	Secret access key		K7bXplAT0pEpy4SAiN2fHUwEtxvgmK3IqyhqnMTA

2. Cross-region scenario:

Table 4-2 Cross-region scenario parameters

Parameter	Description	How to Obtain	Example Value
DR Scene	Replication	– **0**: IDC-to-cloud – **1**: Cross-AZ – **2**: Cross-region	2
source/ target platform type	Type of the disaster recovery site	– **0**: Huawei public cloud – **1**: Huawei private cloud	0
source/ target project id	Project ID of the region where the disaster recovery server resides	Log in to the console and choose **My Credentials** > **API Credentials** to view the project ID.	51af777371904892a49a0c3e3e53de44
source region code	Destination region ID	Obtain the SDRS endpoint by referring to **SDRS Endpoints**.	sdrs.cn-east-2.myhuaweicloud.com
source ecs endpoint	ECS endpoint in the region where the disaster recovery server resides	Obtain the ECS endpoint by referring to **ECS Endpoints**.	-
source evs endpoint	EVS endpoint in the region where the disaster recovery server resides	Obtain the EVS endpoint by referring to **EVS Endpoints**.	-

Parameter	Description	How to Obtain	Example Value
source/ target iam ak	Access key ID of the region where the disaster recovery server resides	Obtain AK/SK by referring to **How Do I Obtain an Access Key (AK/SK)?**	-
source/ target iam sk	Access key of the region where the disaster recovery server resides		-
target sdrs endpoint	SDRS endpoint in the region where the disaster recovery server resides	Obtain the SDRS endpoint by referring to **SDRS Endpoints**.	sdrs.cn-east-2.myhuaweicloud.com

Step 4 Configure the gateway for the proxy client on the disaster recovery site server:

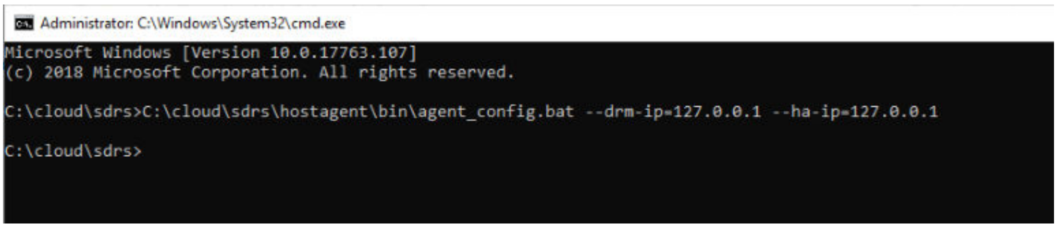
1. Linux disaster recovery server:

   su - service -c "**/opt/cloud/sdrs/hostagent/bin/agent_config.sh --drm-ip=127.0.0.1 --ha-ip=127.0.0.1**"

2. Windows disaster recovery server:

   Open the cmd window and run the following command:

   C:\cloud\sdrs\hostagent\bin\agent_config.bat --drm-ip=127.0.0.1 --ha-ip=127.0.0.1



```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\cloud\sdrs>C:\cloud\sdrs\hostagent\bin\agent_config.bat --drm-ip=127.0.0.1 --ha-ip=127.0.0.1

C:\cloud\sdrs>
```

----End

4.2 Configuring Production Site Servers

Scenarios

Configure production site servers before you reprotect the protected instances on the console.

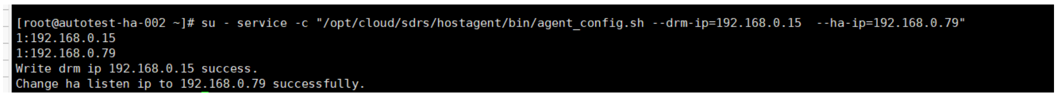
Procedure

Step 1 Log in to a production site server.

Step 2 Run the following commands in sequence to configure the gateway for the proxy client on the production site server:

1. Linux server:

   su - service -c "**/opt/cloud/sdrs/hostagent/bin/agent_config.sh --drm-ip=***drm ip* **--ha-ip=***HostAgentIp*"

   ```
   [root@autotest-ha-002 ~]# su - service -c "/opt/cloud/sdrs/hostagent/bin/agent_config.sh --drm-ip=192.168.0.15  --ha-ip=192.168.0.79"
   1:192.168.0.15
   1:192.168.0.79
   Write drm ip 192.168.0.15 success.
   Change ha listen ip to 192.168.0.79 successfully.
   ```

2. Windows server:

   Open the cmd window and run the following command:

   C:\cloud\sdrs\hostagent\bin\agent_config.bat --drm-ip=*drm ip* **--ha-ip=***HostAgentIp*

   NOTE

   - *drm ip*: IP address of the primary NIC of the cloud disaster recovery gateway
   - *HostAgentIp*: IP address of the primary NIC of the current server
   - Ensure that the gateway configured for production site servers is the same as that of the protected instances.

----End

4.3 Port Description (Asynchronous Replication)

Table 4-3 DR gateway port description

Port	Protocol	Description
29210	TCP	Used to communicate with proxy clients.
29211	TCP	Used to receive control commands.
7443	TCP	Used for API communication.

Table 4-4 Production and DR site server port description

Port	Protocol	Description
8091	TCP	Used to transfer messages between proxy clients.
59526	TCP	Used to communicate with the DR gateway.
29210	TCP	The local listening port used to communicate with proxy clients after a failover.
29211	TCP	The local listening port used to receive control commands after a failover.
7443	TCP	The local listening port used for API communication after a failover.

4.4 Changing the Password of User rdadmin

Scenarios

- To improve O&M security, you are advised to change the user **rdadmin**'s password of the client OS regularly and disable this user's remote login permission.
- In Linux, user **rdadmin** does not have a password.
- This section describes how to change the password of user **rdadmin** in Windows 2016. Change the password according to actual situation in other versions.

Prerequisites

- The username and password for logging in to the console have been obtained.
- The username and password for logging in to a Windows ECS have been obtained.

Procedure

Step 1 Go to the ECS console and log in to the Windows ECS.

Step 2 Choose **Start** > **Control Panel**. In the **Control Panel** window, click **User Accounts**.

Step 3 Click **User Accounts** to open the **User Account Control** dialog box. Select **rdadmin** and click **Reset Password**.

Step 4 Enter the new password and click **OK**.

Step 5 In **Task Manager**, click the **Services** tab and then click **Open Service**.

Step 6 Select RdMonitor and RdNginx respectively. In the displayed dialog box, select **Login**, change the password to the one entered in **Step 4**, and click **OK**.

----End

A Change History

Released On	Description
2024-04-30	This issue is the eighth official release. Added the following section: **Installing Clients**
2024-01-12	This issue is the seventh official release. Added the following content: Added the method of changing the password of user **rdadmin** in section **Changing the Password of User rdadmin**.
2023-11-06	This issue is the sixth official release. 1. Added support for Windows Server 2016 and 2019 for asynchronous replication. 2. Add a note that regardless of whether the production server runs Linux or Windows, it is recommended that the disaster recovery gateway be deployed on a Linux server. 3. Add an asynchronous replication FAQ **How Do I Handle the drm Process Start Failure?**
2021-09-25	This issue is the fifth official release. Added the following section: **Asynchronous Replication**
2020-04-29	This issue is the fourth official release. Modified the following content: Modified restrictions in **Deleting a Protected Instance**. Specifically, shared disks are supported.
2019-11-30	This issue is the third official release. Modified the following content: Added a parameter example in **Creating a Replication Pair**.

Released On	Description
2019-05-30	This issue is the second official release. Modified the following content: ● Added notes on attaching a replication pair in **Attaching a Replication Pair**. ● Added notes on performing a switchover in **Performing a Switchover**. ● Added notes on performing a failover in **Performing a Failover**.
2019-05-24	This issue is the first official release.