Storage Disaster Recovery Service

User Guide

Issue 05

Date 2021-09-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Permissions Management

1.1 Creating a User and Granting SDRS Permissions

This chapter describes how to use **IAM** to implement fine-grained permissions control for your SDRS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing SDRS resources.
- Grant only the permissions required for users to perform a task.
- Entrust HUAWEI CLOUD accounts or cloud services to perform efficient O&M on your ECS resources.

If your HUAWEI CLOUD account does not need individual IAM users, skip over this section.

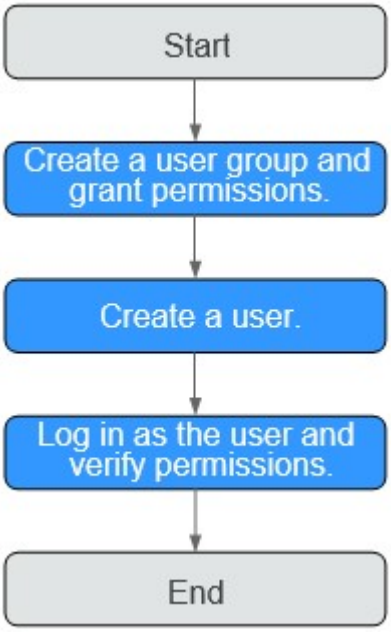
This section describes the procedure for granting permissions (see **Figure 1-1**).

Prerequisites

Before assigning permissions to user groups, you should learn about the system-defined roles and policies listed in **Supported system roles**. For the system policies of other services, see **System Permissions**.

Process Flow

Figure 1-1 Process for granting SDRS permissions



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**.

   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 (Under Restricted OBT)

2.1 Managing a Replica Pair

2.1.1 Deleting a Replica Pair

Scenarios

Delete replica pairs that are no longer required to release resources.

Prerequisites

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

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.

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

----End

2.2 Managing a Protection Group

2.2.1 Creating a Protection Group

Scenarios

In a replica pair, 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**.

The **Create Protection Group** page is displayed.

Step 5 Enter a group name and click **Next**.

The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.

----End

2.2.2 Enabling Protection

Scenarios

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 right pane, locate the replica pair housing the protection group you want to enable 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** > **Enable Protection**.

Step 6 In the displayed dialog box, confirm information and click **Yes**.

----End

2.2.3 Disabling Protection

Scenarios

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.

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**.

Step 6 In the displayed dialog box, confirm information and click **Yes**.

----End

2.2.4 Executing a Planned Failover

Scenarios

A planned failover changes the disaster recovery direction of a protection group and switches services from the production site to the disaster recovery site.

Disaster recovery site servers are created using the latest available data and billed based on the server billing standards. If a server is still running during the planned failover, the system synchronizes all the server data of the current time point to the disaster recovery site server. If a server becomes faulty, some data may fail to synchronize and lose.

After a planned failover, the disaster recovery direction is from the disaster recovery site to the production site. Perform planned failovers based on your planned outages to ensure no data loss. For example, if you plan to power off the production site, perform a planned failover to switch services to the disaster recovery site.

After a planned 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.

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 **Synchronizing**, **Synchronization finished**, or **Planned failover failed**.
- Protected instance services are running at the production site.

Precautions

During a planned 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 execute a planned 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 Planned Failover**.

The **Execute Planned Failover** page is displayed.

Step 6 Set the parameters as prompted.

Table 2-1 Parameter description

Parameter	Description	Example Value
Protected Instance	Select the protected instances you want to execute a planned failover.	-
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 a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name 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**.

----End

2.2.5 Performing a Reverse Reprotection

Scenarios

After a planned 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 a reverse reprotection, initial data synchronization starts. During this process, if disaster recovery site servers are restarted, data will be resynchronized until the synchronization is complete.
- After a reverse reprotection is complete, if disaster recovery site servers are restarted, data will not be resynchronized. If data is then written to the disaster recovery site servers, the incremental data is then synchronized.

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 **Planned 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.

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

----End

2.2.6 Executing a Planned Failback

Scenarios

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

Prerequisites

- Initial synchronization is completed for all the protected instances in the protection group, and the status of protected instances is **Synchronizing**, **Synchronization finished**, or **Planned failback failed**.
- Protected instance services are running at the disaster recovery 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 execute a planned 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 Planned Failback**.

The **Execute Planned Failback** page is displayed.

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

----End

2.2.7 Reprotecting a Protection Group

Scenarios

After a planned 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 **Planned 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**.

The **Reprotect** page is displayed.

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

----End

2.2.8 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 **Synchronizing**, **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**.

The **Create Disaster Recovery Drill** page is displayed.

Step 6 Set the parameters as prompted.

Table 2-2 Parameter description

Parameter	Description	Example Value
Protected Instance	Select all the protected instances you want to perform a disaster recovery drill.	-
Disaster Recovery Site Server	Select the specifications for disaster recovery site servers.	-
Name	Enter a drill name for each protected instance. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Drill-ECS02

Parameter	Description	Example Value
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**.

Step 8 Confirm the drill information and click **Submit**.

After the disaster recovery drill is created, you can log in to a drill server and check whether services are running properly.

----End

2.2.9 Deleting a Protection Group

Scenarios

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

Prerequisites

- The protection group contains no protected instances.
- 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 housing the protection group you want to delete 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** > **Delete**.

Step 6 In the displayed dialog box, confirm information and click **Yes**.

----End

2.3 Managing Protected Instances

2.3.1 Creating Protected Instances

Scenarios

Create protected instances for servers that demand disaster recovery in a protection group. If a lot of production site servers become faulty due to force majeure, you can execute a planned 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.

Prerequisites

- Production site servers are not used to create protected instances.
- Production site servers are in the same AZ as the cloud disaster recovery gateway.
- Production site servers have been restarted after disks are attached.
- In the scenario that a reverse reprotection is performed for a protected instance, data is syncronized, and the instance is then deleted, the production site server can be used to create a new protected instance only after original disks are manually attached, and the proxy client is uninstalled and then reinstalled on the server.
- In the scenario that a planned failback is performed for a protected instance, production site server is not configured, and the instance is then deleted, the production site server can be used to create a new protected instance only after the proxy client is uninstalled and then reinstalled on the server.

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.

Step 4 Set the parameters as prompted.

Table 2-3 Parameter description

Parameter	Description	Example Value
Production Site Server	• Select production site servers you want to protect. • Select the disk type for each disaster recovery site disk. • Enter a name for each protected instance. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	-
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 specified business to one protection group. In this case, you can start protection, perform planned failovers, and run disaster recovery drills for the entire group.	protected-group-01

Step 5 Click **Next**.

The **Details** page is displayed.

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

Protected instances are created.

----End

2.3.2 Enabling Protection

Scenarios

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.

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

Step 6 In the displayed dialog box, confirm information and click **Yes**.

----End

2.3.3 Disabling Protection

Scenarios

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 **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** > **Disable Protection** in the **Operation** column.

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

Step 6 In the displayed dialog box, confirm information and click **Yes**.

----End

2.3.4 Executing a Planned Failover

Scenarios

A planned failover changes the disaster recovery direction of a protected instance and switches services from the production site to the disaster recovery site.

Disaster recovery site servers are created using the latest available data and billed based on the server billing standards. If a server is still running during the planned failover, the system synchronizes all the server data of the current time point to the disaster recovery site server. If a server becomes faulty, some data may fail to synchronize and lose.

After a planned failover, the server disaster recovery direction is from the disaster recovery site to the production site. Perform planned failovers based on your planned outages to ensure no data loss.

After a planned 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.

Prerequisites

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

Precautions

During a planned 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 execute a planned 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 Planned Failover** in the **Operation** column.

Step 6 Set the parameters as prompted.

Table 2-4 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 a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	ECS02-DR
Subnet	Select the subnet where the disaster recovery 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.	-

Step 7 Click **Next**.

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

----End

2.3.5 Performing a Reverse Reprotection

Scenarios

After a planned 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 a reverse reprotection, initial data synchronization starts. During this process, if disaster recovery site servers are restarted, data will be resynchronized until the synchronization is complete.
- After a reverse reprotection is complete, if disaster recovery site servers are restarted, data will not be resynchronized. If data is then written to the disaster recovery site servers, the incremental data is then synchronized.

Prerequisites

- The disaster recovery site server has been preconfigured according to **Configuring Disaster Recovery Site Servers**.
- The status of the protected instance is **Planned 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.

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** > **Perform Reverse Reprotection** in the **Operation** column.

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

Step 6 Click **Submit**.

----End

2.3.6 Executing a Planned Failback

Scenarios

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

Prerequisites

- Initial synchronization is completed for the protected instance, and the status of the protected instance is **Synchronizing**, **Synchronization finished**, or **Planned failback failed**.

- Protected instance services are running at the disaster recovery 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 execute a planned 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 Planned Failback** in the **Operation** column.

The **Execute Planned Failback** page is displayed.

Step 6 Click **Submit**.

----End

2.3.7 Reprotecting a Protected Instance

Scenarios

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

Prerequisites

- The production site server has been preconfigured according to **Configuring Production Site Servers**.
- The status of the protected instance is **Planned 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.

The **Reprotect** page is displayed.

Step 6 Click **Submit**.

----End

2.3.8 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 **Synchronizing**, **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 click **Create Disaster Recovery Drill** in the **Operation** column.

The **Create Disaster Recovery Drill** page is displayed.

Step 6 Set parameters as prompted.

Table 2-5 Parameter description

Parameter	Description	Example Value
Specifications	Select the drill server specifications.	-
Name	Enter a drill name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name 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**.

Step 8 Confirm the drill information and click **Submit**.

After the disaster recovery drill is created, you can log in to a drill server and check whether services are running properly.

----End

2.3.9 Deleting a Protected Instance

Scenarios

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 need to manually detach the original disk from the production site server and then re-attach the disk through the disaster recovery gateway before deleting the instance.
- 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.

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

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

Delete disaster recovery site servers

- Deselected: The replication relationship between the production site servers and disaster recovery site servers is canceled, but the disaster recovery site servers and disks are retained.
- Selected: The replication relationship between the production site servers and disaster recovery site servers is canceled, and the disaster recovery site servers and disks are deleted. If there are no disaster recovery site servers, EVS disks will be deleted.

Step 7 Click **Yes**.

----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 the drill.

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.

Step 5 In the drill list, locate the target drill and click **Delete** in the **Operation** column.

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

Step 6 In the displayed dialog box, confirm drill information and click **Yes**.

----End

3 Synchronous Replication

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 Planned Failover

Scenarios

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

Table 3-1 DR direction change after a planned failover

-	Production Site	DR Site
Before	AZ1	AZ2
After	AZ2	AZ1

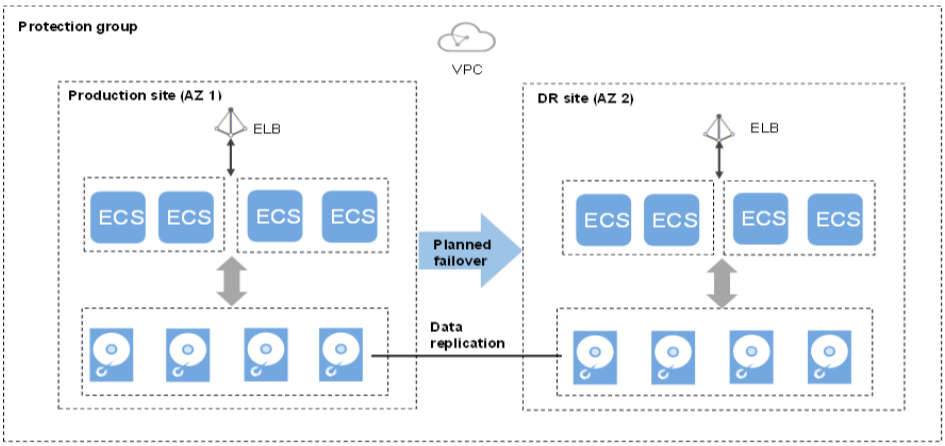
After the planned failover, data synchronization continues, but the DR direction is changed from the DR site to the production site. You can perform a planned failover when you are certain that the production site will encounter an interruption. For example, if the production site (AZ1) is going to encounter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

SDRS will migrate NICs on the server during the planned failover. After the planned 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

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

Figure 3-1 Performing a planned failover



Notes

For Linux servers with Cloud-Init installed, if you have changed **hostname** of the production site server before you perform a planned 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 Planned Failover or Failover?**

Prerequisites

- All the servers in the protection group are stopped.
- The protection group has replica pairs.
- Protection is enabled for the protection group, and the protection group is in the **Protecting** or **Planned 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**.

Step 4 On the operation page of the protection group, click **Execute Planned Failover** in the upper right corner.

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 **Execute Planned Failover** dialog box, click **Execute Planned Failover**.

NOTE

During the planned failover, do not start the servers in the protection group. Otherwise, the planned failover 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.

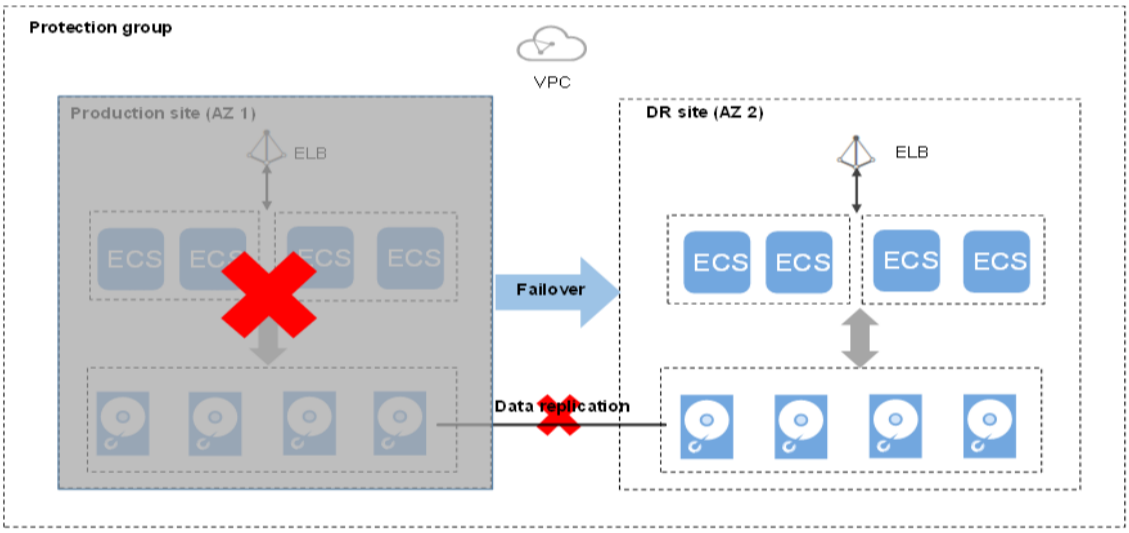
Once you perform a failover, the DR site servers and disks become available immediately. You can power on the servers, or use Cloud Server Backup Service (CSBS) or Volume Backup Service (VBS) to restore the data to a specified data recovery point.

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 Planned Failover or Failover?**

Prerequisites

- You have confirmed with the customer service that the servers and disks at the production site are faulty, and the deployed services are unavailable.
- The protection group contains replication pairs.
- Protection is enabled for the protection group, and the protection group is in the **Protecting**, **Planned failover 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 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 replica 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

If a protection group is no longer used, you can release the virtual resources by deleting the protection group from the system.

Prerequisites

All the protected instances, DR drills, and replica 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, 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**, **Planned failover 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 operation page for the protection group 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
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

Parameter	Description	Example Value
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
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 Replica Pair

Scenarios

You can perform steps provided in this section to attach a replica 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 the number of replications not attached to any protected instance reaches five, you cannot create another replica pair.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- The protected instance is in the **Available** or **Protecting** state.
- The replica pair is in the **Available** or **Protecting** state.
- The non-shared replica 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 In the pane of the protection group for which the replica pair is to be attached to the protected instance, click **Protected Instances**.

The operation page for the protection group 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 replica pair** page is displayed.

Step 5 Select the replica pair to be attached and a desired device name, and click **OK**.

The replica 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**, **Planned failover failed**, or **Failover failed** state.
- The protected instance is in the **Available**, **Protecting**, **Failover complete**, **Enabling protection failed**, **Disabling protection failed**, **Planned failover 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**, **Planned failover 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

Parameter	Description	Example Value
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
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 Replica Pair Capacity

Scenarios

If the replica pair capacity of your protection groups cannot meet your service requirements, you can perform steps provided in this section to expand the capacity of the specified replica pair. Replica pairs do not support capacity reduction or rollback after a successful capacity expansion.

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

Prerequisites

- The replica pair for which the capacity is to be expanded is in the **Available**, **Protecting**, or **Expansion failed** state.
- The disks in the replica pair are in the **Available** or **In-use** state.
- If the billing mode of the disks in the replica pair is yearly/monthly, capacity expansion is not supported. If you want to increase the capacity of disks in the replica pair, delete the replica pair, expand the capacity of the production site disk, and then use the disk to create a replica pair.

NOTE

- When the disks in a replica pair are not shared

  If the disks in the replica pair are in the **In-use** state, the replica pair capacity can be expanded only when online capacity expansion is supported. If online capacity expansion is not supported, **Expand Capacity** in the **Operation** column is unavailable.
- The disks in a replica pair are shared.

  The replica pair capacity cannot be expanded online if the disks are in the **In-use** 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 capacity of the replica pair is to be expanded, click **Replica Pairs**.

The operation page for the protection group is displayed.

Step 4 On the **Replica Pairs** tab, locate the row containing the replica pair for which the capacity is to be expanded and click **Expand Capacity** in the **Operation** column.

The **Expand Capacity** page is displayed.

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

Step 6 If you do not need to modify the information, click **Submit**.

If you want to modify the information, click **Previous** and modify the information as required.

----End

3.3.3 Deleting a Replica Pair

Scenarios

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

When you delete a replica pair, the production site disk in the replica 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**, **Planned failover failed**, **Failover failed**, Deletion failed, or **Re-enabling protection failed** state.
- The replica pair is in the **Available**, **Protecting**, **Failover complete**, **Creation failed**, **Enabling protection failed**, **Disabling protection failed**, **Planned failover failed**, **Failover failed**, **Deletion failed**, **Re-enabling protection failed**, **Attaching failed**, **Expansion failed**, **Invalid**, or **Faulty** state.
- The replica pair is not attached to any protected instance. For details about how to detach a replica 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 **Replica Pairs**.

The operation page for the protection group is displayed.

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

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

NOTE

When you delete a replica 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 replica pair 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 replica pair 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 Disaster Recovery Drill (Synchronous Replication)

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. This way, drill servers will have the same server specifications and disk types as the production site servers.

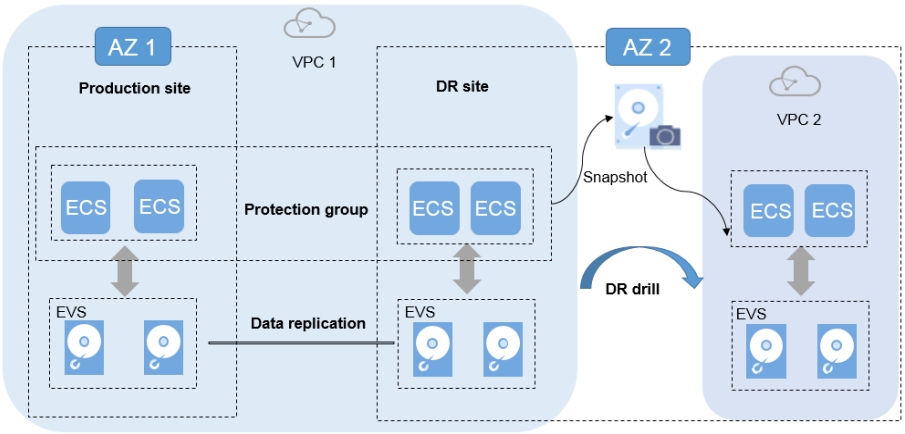
NOTE

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 to check that:

- Data between the production site and disaster recovery site is consistent at the moment you create a disaster recovery drill.
- Services run properly at the disaster recovery site after a planned failover.

Figure 3-3 Disaster recovery drill



Precautions

- If the disaster recovery 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 an existing drill VPC is used for a new drill, the subnet ACL rule of the drill VPC will be different from that of the protection group VPC. Manually set them to be the same as needed.
- If a custom route table is configured and associated with a subnet in the protection group VPC, the corresponding route table will not be automatically created in the drill VPC. Manually create one as needed.
- If the disaster recovery site servers run Windows and use key pairs for login, ensure that the key pairs exist when you create the drill. Otherwise, drill servers may fail to create, resulting in the drill creation failure.

  NOTE

  If a key pair has been deleted, recreate the key pair with the same name.
- If the disaster recovery 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 and before it is executed, modifications made to **Hostname**, **Name**, **Agency**, **ECS Group**, **Security Group**, **Tags**, and **Auto Recovery** of disaster recovery site servers will not synchronize to drill servers. Log in to the console and manually make the modifications for the drill servers.
- If the synchronization progress of replication pairs in the protection group is not all 100%, the created drill servers may fail to start. It is recommended that you run disaster recovery drills after all replication pairs are synchronized.

Prerequisites

- The protection group is in the **Available**, **Protecting**, **Failover complete**, **Enabling protection failed**, **Disabling protection failed**, **Planned failover failed**, **Re-enabling protection failed**, or **Failover failed** state.
- Do not run disaster recovery drills before the first time data synchronization between the production site servers and disaster recovery site servers completes. Otherwise, drill servers may not start properly.

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 which a DR drill is to be added, click **DR Drills**.

The protection group details page is displayed.

Step 4 On the **DR Drills** tab, click **Create DR Drill**.

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

Step 5 Configure **Name** and **Drill VPC**.

Table 3-4 Parameter description

Parameter	Description	Example Value
Name	DR drill name	DR drill servername
Drill VPC	VPC that used for a DR drill. It cannot be the same as the VPC of the DR site server. The value can be **Automatically create** or **Use existing**. • **Automatically create**: The system automatically creates a drill VPC and subnet for the protection group. • **Use existing**: The system uses an existing VPC as the drill VPC. If you select to use an existing VPC, the subnet CIDR block of the drill VPC must be consistent with that of the production group VPC. **NOTE** The drill VPC cannot be the same as the VPC of the protection group.	vpc-f9f7

Step 6 Click **OK**.

After the disaster recovery drill is created, you can log in to a drill server and check whether services are running properly.

----End

3.4.2 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 3-5 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

Operation	Resource Type	Trace Name
Enabling protection for a protection group (when the protection group is in the **failed-over** state)	protectionGroup	reprotectProtec-tionGroup
Disabling protection for a protection group	protectionGroup	stopProtectionGroup
Performing a failover for a protection group	protectionGroup	failoverProtectionGroup
Performing a planned failover	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

Operation	Resource Type	Trace Name
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?

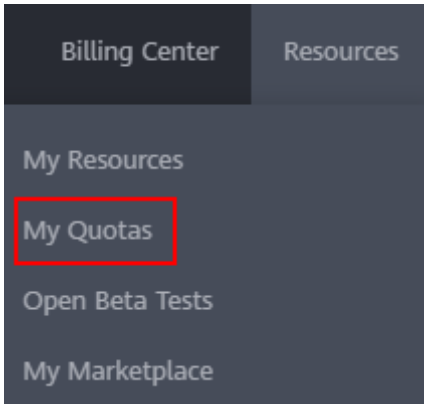
Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

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 3-4 My Quotas

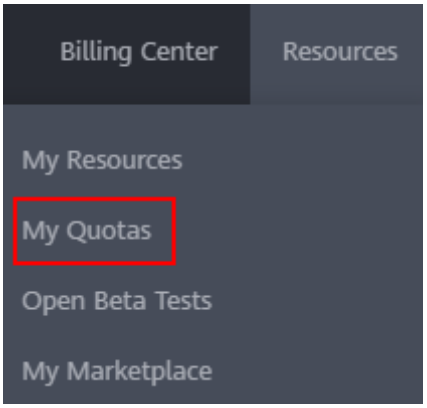
   

4. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, apply for a higher quota.

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 3-5 My Quotas



3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, configure parameters as required.
   In **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 Tenant Authorization Letter 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 following command as user **root**:

curl -ik --request POST --url "https://`netstat -ntlp | grep 7443 | awk '{print $4}'`/v1/gateway-servers" --header 'Accept: application/json' --header 'Content-Type: application/json' --data '{"replication_scene":"*replicationScene***","source_platform_property":{"platform_type":"hws","project_id":"***sourceProjectId***","ecs_endpoint":"***sourceEcs***","evs_endpoint":"***sourceEvs***","iam_keys":{"iam_ak":"***sourceIamAk***","iam_sk":"***sourceIamSk***"},"if_target_proxy":false},"target_platform_property":{"platform_type":"hws","project_id":"***targetProjectId***","sdrs_endpoint":"***targetSdrs***","iam_keys":{"iam_ak":"***targetIamAk***","iam_sk":"***targetIamSk***"}}}'**

Table 4-1 describes the variables in the preceding command.

Table 4-1 Parameter description

Site	Parameter	Description	How to Obtain	Example Value
Replication	replicationScene	Replication scenario. Currently, there are three replication scenarios.	• **H2C**: IDC-to-cloud • **CA2CA** : Cross-AZ • **CR2CR** : Cross-region	H2C
HUAWEI CLOUD disaster recovery site	platform_type	Platform type	The value is **hws**.	hws
	sourceProjectId	Project ID	Log in to the HUAWEI CLOUD console and choose **My Credentials** > **API Credentials** to view the project ID.	51af777371904892a49a0c3e3e53de44
	sourceEcs	HUAWEI CLOUD ECS endpoint	Obtain the ECS endpoint by referring to **Regions and Service Endpoints**.	-
	sourceEvs	HUAWEI CLOUD EVS endpoint	Obtain the EVS endpoint by referring to **Regions and Service Endpoints**.	-
	sourceIamAk	HUAWEI CLOUD access key ID	Obtain the AK and SK by referring to **How Do I Obtain an Access Key (AK/SK)?**	-
	sourceIamSk	HUAWEI CLOUD secret access key		-
HUAWEI CLOUD disaster recovery site	targetProjectId	Project ID	Log in to the HUAWEI CLOUD console and choose **My Credentials** > **API Credentials** to view the project ID.	0605767cb280d5762fd6c0133d6bea3f
	targetSdrs	SDRS endpoint	Obtain the SDRS endpoint by referring to **Regions and Service Endpoints**.	sdrs.cn-east-2.myhuaweicloud.com
	targetIamAk	HUAWEI CLOUD access key ID	Obtain the AK and SK by referring to **How Do I Obtain an Access Key (AK/SK)?**	RZSAMHULWKKE71N0XHUT
	targetIamSk	HUAWEI CLOUD secret access key		K7bXplAT0pEpy4SAiN2fHUwEtxvgmK3lqyhqnMTA

An example command is as follows:

curl -ik --request POST --url https://`netstat -ntlp | grep 7443 | awk '{print $4}'`/v1/gateway-servers --header 'Accept: application/json' --header 'Content-Type: application/json' --data '{"replication_scene":"H2C","source_platform_property":{"platform_type":"hws","project_id":"0605767cb280d5762fd6c0133d6bea3f","ecs_endpoint":"ecs.br-iaas-odin1.huaweicloud.com","evs_endpoint":"evs.br-iaas-odin1.huaweicloud.com","iam_keys":{"iam_ak":"RZSAMHULWKKE71N0XHUT","iam_sk":"K7bXplAT0pEpy4SAiN2fHUwEtxvgmK3IqyhqnMTA"},"if_target_proxy":false},"target_platform_property":{"platform_type":"hws","project_id":"0605767cb280d5762fd6c0133d6bea3f","sdrs_endpoint":"sdrs.br-iaas-odin1.huaweicloud.com","iam_keys":{"iam_ak":"RZSAMHULWKKE71N0XHUT","iam_sk":"K7bXplAT0pEpy4SAiN2fHUwEtxvgmK3IqyhqnMTA"}}}'

Step 3 Run the following commands in sequence to configure the gateway for the proxy client on the disaster recovery site server:

su service

/opt/cloud/sdrs/hostagent/bin/agent_config.sh --drm-ip=127.0.0.1

----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. Switch the user.

   su service

2. Configure Host Agent.

   /opt/cloud/sdrs/hostagent/bin/agent_config.sh --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

A Change History

Released On	Description
2021-09-25	This issue is the fifth official release. Added the following section: **Asynchronous Replication (Under Restricted OBT)**
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**.
2019-05-30	This issue is the second official release. Modified the following content: • Added notes on attaching a replication pair in **Attaching a Replica Pair**. • Added notes on performing a planned failover in **Performing a Planned Failover**. • Added notes on performing a failover in **Performing a Failover**.
2019-05-24	This issue is the first official release.

