Storage Disaster Recovery Service

User Guide

Issue 10

Date 2020-04-29



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.

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

Trademarks and Permissions


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.

Contents

1 Permissions Management 1
1.1 Creating a User and Granting Permissions 1
2 Managing Protection Groups 3
2.1 Disabling Protection 3
2.2 Performing a Planned Failover 4
2.3 Performing a Failover 6
2.4 Performing Reprotection 7
2.5 Deleting a Protection Group 8
3 Managing Protected Instances 10
3.1 Modifying Specifications of a Protected Instance 10
3.2 Deleting a Protected Instance 11
3.3 Creating a Replication Pair 13
3.4 Attaching a Replication Pair 16
3.5 Detaching a Replication Pair 17
3.6 Adding a NIC 18
3.7 Deleting a NIC 19
4 Managing Replication Pairs 21
4.1 Creating a Replication Pair 21
4.2 Expanding Replication Pair Capacity 24
4.3 Deleting a Replication Pair 25
5 Managing DR Drills 27
5.1 Performing a DR Drill 27
5.2 Deleting a DR Drill 30
6 Interconnecting with CTS 32
6.1 Key SDRS Operations Recorded by CTS 32
6.2 Viewing Traces 33
7 Managing Quotas 35
A Change History 37

 Copyright © Huawei Technologies Co., Ltd.

1 Permissions Management

1.1 Creating a User and Granting 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 the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to SDRS resources.
- Grant only the permissions required for users to perform a task.
- Entrust a HUAWEI CLOUD account or cloud service to perform professional and efficient O&M on your SDRS resources.

If your HUAWEI CLOUD account does not need individual IAM users, then you may skip over this chapter.

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

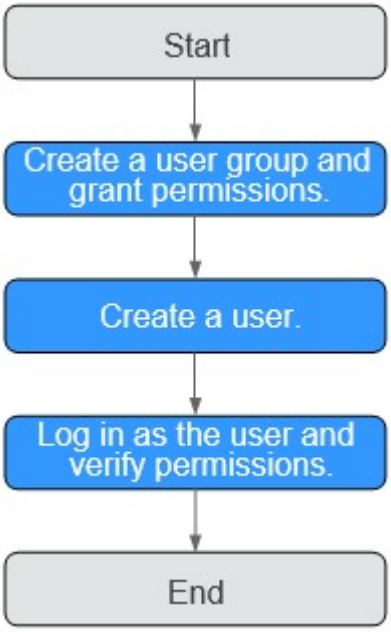
Prerequisites

Before assigning permissions to user groups, you should learn about the system policies listed in **System policy summary**. For the system policies of other services, see **Permissions Policies**.

Copyright © Huawei Technologies Co., Ltd.

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 assign the **SDRS Administrator** policy 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 by using the created user, and verify that the user only has read permissions for SDRS.

   - Choose **Service List** > **Storage Disaster Recovery Service**. Click **Create Protection Group** on the SDRS console. If a message appears indicating that you have insufficient permissions to perform the operation, the **SDRS Administrator** policy has already taken effect.
   - Choose any other service in the **Service List**. If a message appears indicating insufficient permissions to access the service, the **SDRS Administrator** policy has already taken effect.

Copyright © Huawei Technologies Co., Ltd.

2 Managing Protection Groups

2.1 Disabling Protection

Scenarios

If you want to disable protection for all resources in a specified protection group, you can perform steps provided in this section.

Once the protection is disabled, data synchronization for all protected instances in the protection group will stop.

Prerequisites

- The protection group has replication pairs.
- The protection group is in the **Protecting** or **Disabling protection 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 operation page for the protection group is displayed.

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

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

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

----End

 Copyright © Huawei Technologies Co., Ltd.

2.2 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 2-1** shows the direction change.

Table 2-1 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.

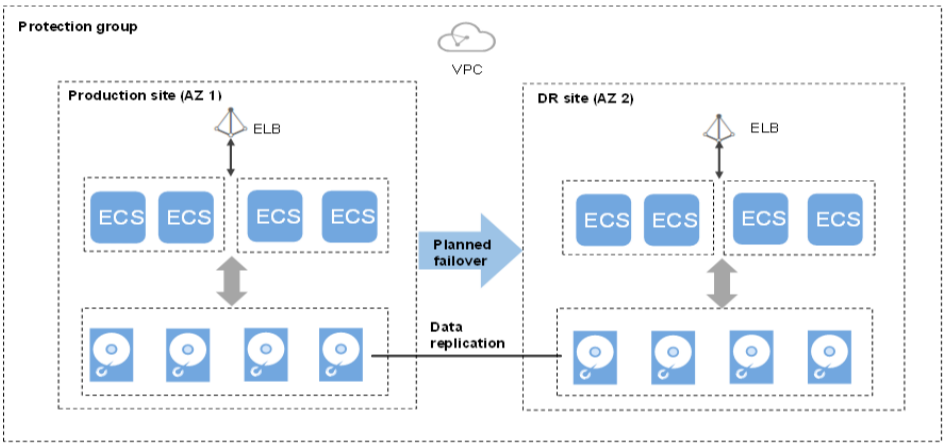
SDRS will migrate NICs on the server during the planned failover. After the planned failover, the IP, EIP, and MAC addresses of the production site server will be migrated to the DR site server, so that the IP, EIP, and MAC addresses remain the same.

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.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 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 replication 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**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

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

----End

2.3 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.

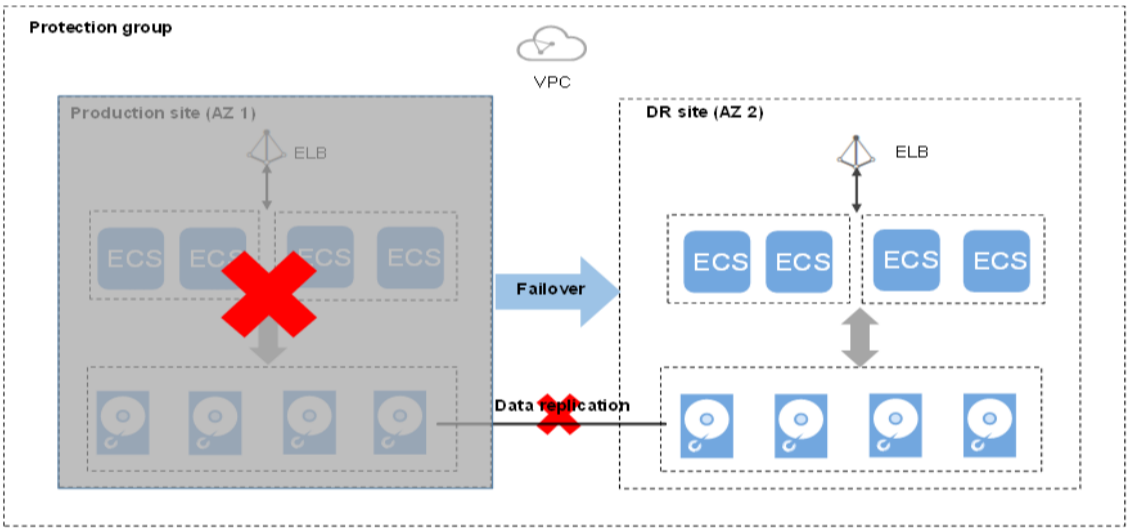
Once you perform a failover, the DR site servers and disks become available immediately. You can power on the servers, or use Cloud Server Backup Service (CSBS) or Volume Backup Service (VBS) to restore the data to a specified data recovery point.

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 2-2 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.

Copyright © Huawei Technologies Co., Ltd.

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 has 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 operation page for the protection group 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**.

2.4 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.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

The **Reprotect** dialog box is displayed.

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

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

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

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

----End

2.5 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 replication pairs have been deleted from the protection group.

Procedure

Step 1 Log in to the management console.

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

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

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

Copyright © Huawei Technologies Co., Ltd.

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

----End

 Copyright © Huawei Technologies Co., Ltd.

3 Managing Protected Instances

3.1 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**

 Copyright © Huawei Technologies Co., Ltd.

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 Deleting a Protected Instance

Scenarios

If you do not need a protected instance, you can 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.

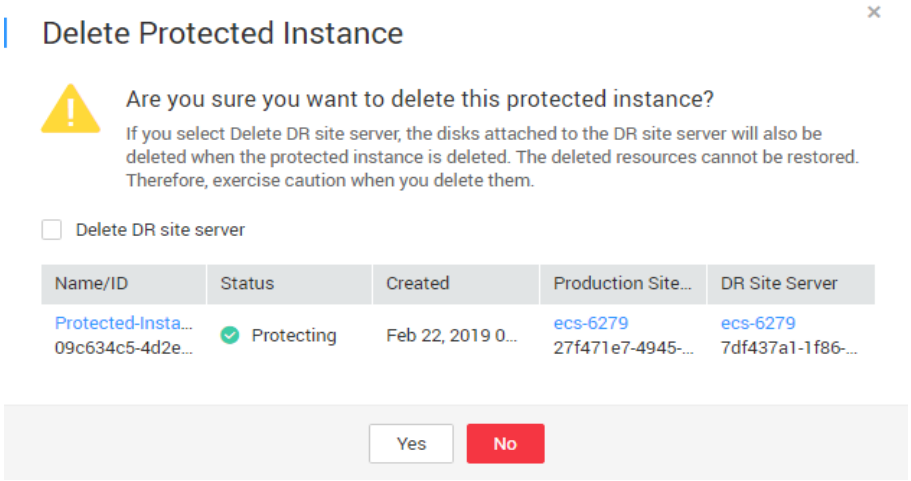
 Copyright © Huawei Technologies Co., Ltd.

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.

Figure 3-1 Deleting a protected instance



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

 Copyright © Huawei Technologies Co., Ltd.

3.3 Creating a Replication Pair

Scenarios

You can create replication pairs for desired disks and add the replication pairs to a specified protection group. When you create a replication pair:

- If the protection group is in the **Available** state, protection is disabled. The production site disk and DR site disk have formed a replication pair, but data synchronization is not started. To start data synchronization, enable protection.
- If the protection group is in the **Protecting** state, protection is enabled. After you create a replication pair, data synchronization is automatically started.

NOTE

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

To modify a disk name, click the disk name on the replication pair details page to switch to the disk details page and modify it.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- If **Server Type** of the protection group is **ECS**, the disks used to create the replication pair 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 In the pane of the protection group for which replication pairs are to be added, click **Replication Pairs**.

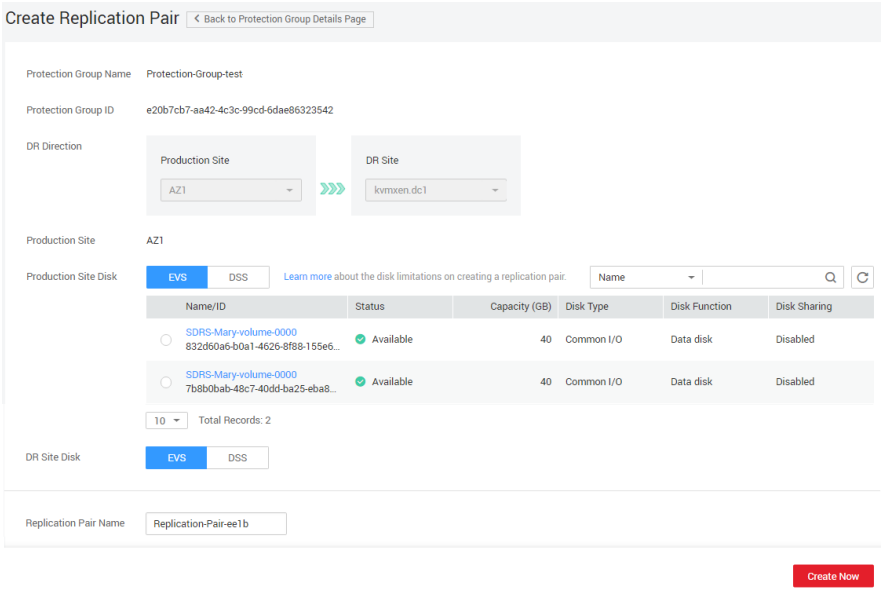
The operation page for the protection group is displayed.

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

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

Copyright © Huawei Technologies Co., Ltd.

Figure 3-2 Creating a replication pair



Step 5 Configure the basic information about the replication pair listed in **Table 3-1**.

Table 3-1 Parameter description

Parameter	Description	Example Value
Protection Group Name	Indicates the name of the protection group to which the replication pair to be created belongs. You do not need to configure it.	Protection-Group-test
Protection Group ID	Specifies the ID of a protection group.	619c57e9-3927-48f8-ad14-3e293260b8a0
DR Direction	Indicates the replication direction of the protection group to which the replication pair to be created belongs. You do not need to configure it.	-
Production Site	Specifies the AZ of the production site.	-
Production Site Disk	This parameter is mandatory. The following two options are available: • **EVS** • **DSS**	EVS

 Copyright © Huawei Technologies Co., Ltd.

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 as required. 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 Name	Indicates the replication pair name. This parameter is mandatory. Configure this parameter when you create a replication pair. Then, you can use this name to classify and search this replication pair.	replication_001

NOTE

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

Step 6 Click **Create Now**.

Step 7 On the **Confirm** page, you can 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 query the replication pairs of the protection group.

 Copyright © Huawei Technologies Co., Ltd.

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

----End

3.4 Attaching a Replication Pair

Scenarios

You can perform steps provided in this section to attach a replication pair to a protected instance. Then, the production site disk is attached to the production site server, and the DR site disk is attached to the DR site server.

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

Restrictions and Limitations

- If the number of replications not attached to any protected instance reaches five, you cannot create another replication pair.

Prerequisites

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

Procedure

Step 1 Log in to the management console.

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

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

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

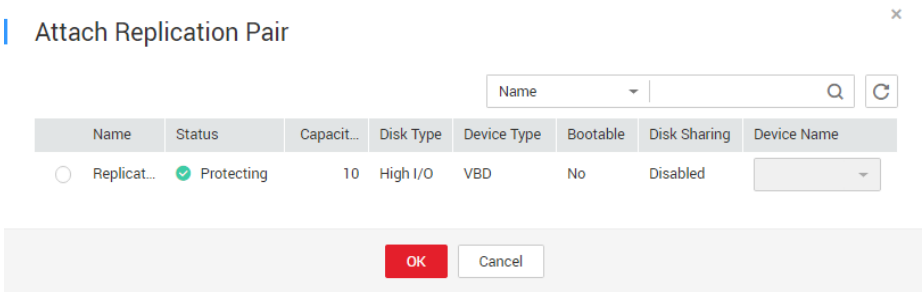
The operation page for the protection group is displayed.

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

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

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 Attaching a replication pair



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

The replication pair is attached to the specified protected instance.

----End

3.5 Detaching a Replication Pair

Scenarios

You can perform steps provided in this section to detach a replication pair from a protected instance. Then, data of the servers in the protected instance will not be written in to the disks in the replication pair.

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 to a protected instance.
- Disks in the **In-use** state have been attached to the production and DR site servers.

NOTE

- A system disk (mounted on the **/dev/sda** or **/dev/vda** mount point) can be detached from a server only when the server is in the **Stopped** state. Therefore, stop the server before detaching the system disk.
- A data disk can be detached from a server online or offline, specifically, when the server is in the **Stopped** or **Running** 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*.

 Copyright © Huawei Technologies Co., Ltd.

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.

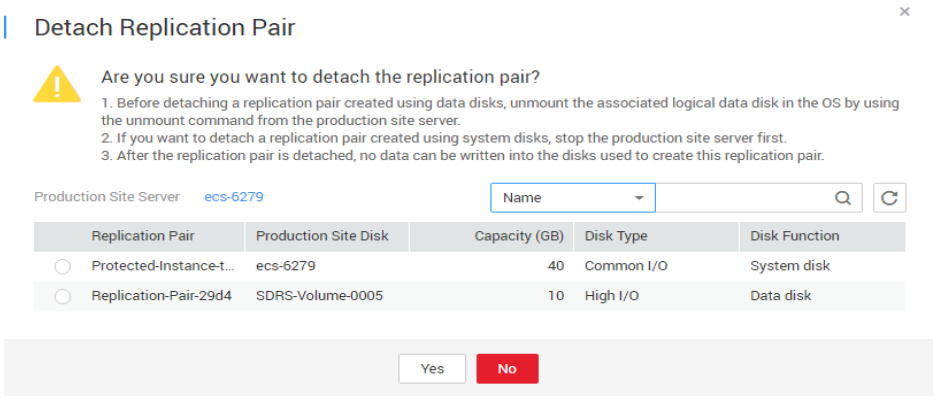
Step 3 In the pane of the protection group for which the replication pair is to be detached from the protected instance, click **Protected Instances**.

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 **Detach** in the **Operation** column.

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

Figure 3-4 Detaching a replication pair



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

Then, data of the servers in the protected instance will not be written in to the disks in the replication pair.

----End

3.6 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.

Copyright © Huawei Technologies Co., Ltd.

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

3.7 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.

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

4 Managing Replication Pairs

4.1 Creating a Replication Pair

Scenarios

You can create replication pairs for desired disks and add the replication pairs to a specified protection group. When you create a replication pair:

- If the protection group is in the **Available** state, protection is disabled. The production site disk and DR site disk have formed a replication pair, but data synchronization is not started. To start data synchronization, enable protection.
- If the protection group is in the **Protecting** state, protection is enabled. After you create a replication pair, data synchronization is automatically started.

NOTE

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

To modify a disk name, click the disk name on the replication pair details page to switch to the disk details page and modify it.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- If **Server Type** of the protection group is **ECS**, the disks used to create the replication pair 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 In the pane of the protection group for which replication pairs are to be added, click **Replication Pairs**.

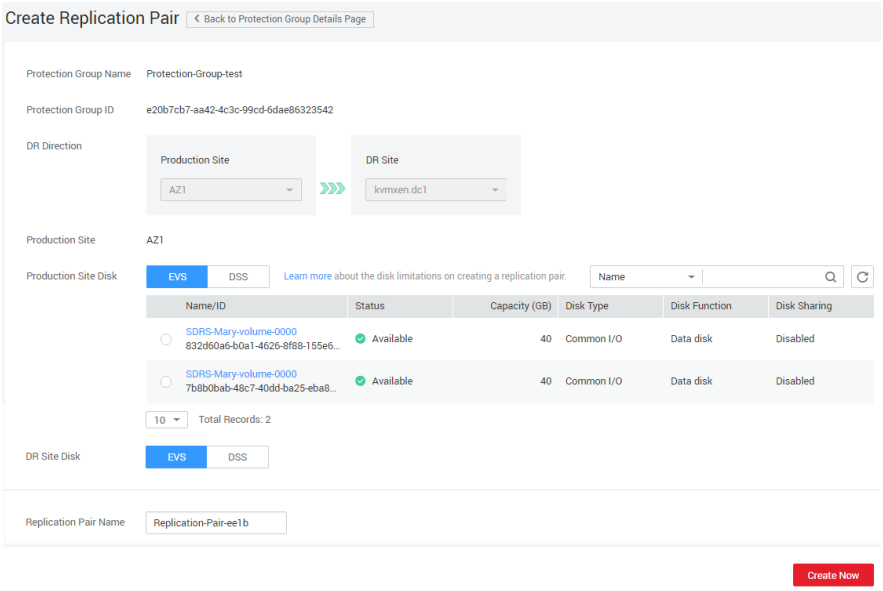
 Copyright © Huawei Technologies Co., Ltd.

The operation page for the protection group is displayed.

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

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

Figure 4-1 Creating a replication pair



Step 5 Configure the basic information about the replication pair listed in **Table 4-1**.

Table 4-1 Parameter description

Parameter	Description	Example Value
Protection Group Name	Indicates the name of the protection group to which the replication pair to be created belongs. You do not need to configure it.	Protection-Group-test
Protection Group ID	Specifies the ID of a protection group.	619c57e9-3927-48f8-ad14-3e293260b8a0
DR Direction	Indicates the replication direction of the protection group to which the replication pair to be created belongs. You do not need to configure it.	-
Production Site	Specifies the AZ of the production site.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Production Site Disk	This parameter is mandatory. The following two options are available: • **EVS** • **DSS**	EVS
DR Site Disk	This parameter is mandatory. The following two options are available: • **EVS** • **DSS** **NOTE** Disks are classified as EVS and DSS disks based on whether the storage resources used by the disks are exclusive. DSS disks are provided for users exclusively. Determine whether to use DSS disks for the DR site as required. 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 Name	Indicates the replication pair name. This parameter is mandatory. Configure this parameter when you create a replication pair. Then, you can use this name to classify and search this replication pair.	replication_001

NOTE

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

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Click **Create Now**.

Step 7 On the **Confirm** page, you can 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 query the replication pairs of the protection group.

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

----End

4.2 Expanding Replication Pair Capacity

Scenarios

If the replication 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 replication pair. Replication pairs do not support capacity reduction or rollback after a successful capacity expansion.

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

Prerequisites

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

NOTE

- When the disks in a replication pair are not shared

  If the disks in the replication pair are in the **In-use** state, the replication 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.
- When the disks in a replication pair are shared

  The replication 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.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 In the pane of the protection group for which the capacity of the replication pair is to be expanded, click **Replication Pairs**.

The operation page for the protection group is displayed.

Step 4 On the **Replication Pairs** tab, locate the row containing the replication 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 replication pair information, 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

4.3 Deleting a Replication Pair

Scenarios

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

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

Prerequisites

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

Procedure

Step 1 Log in to the management console.

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

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

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

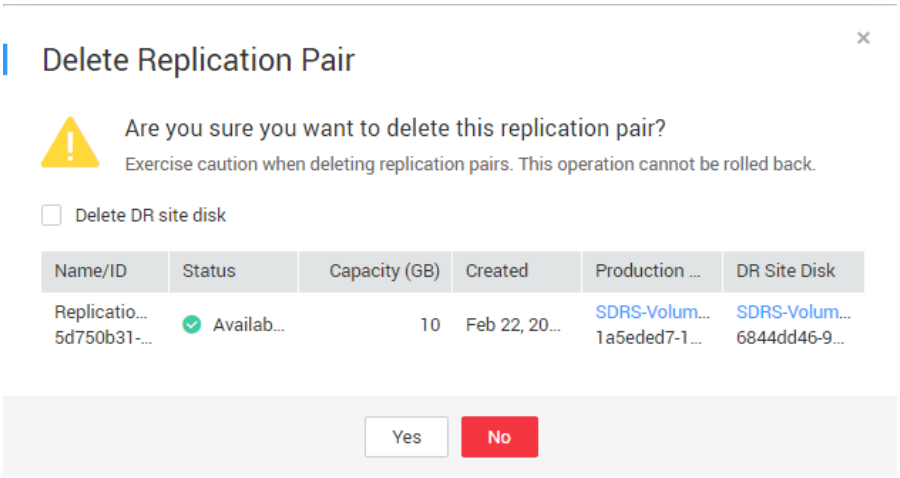
The operation page for the protection group is displayed.

 Copyright © Huawei Technologies Co., Ltd.

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

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

Figure 4-2 Deleting a replication pair



NOTE

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

Step 5 Determine the subsequent operation.

Delete DR Site Disk

- If you do not select this option, the replication 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 replication 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

 Copyright © Huawei Technologies Co., Ltd.

5 Managing DR Drills

5.1 Performing a DR Drill

Scenarios

DR drills can be used to simulate fault scenarios, specify the emergency recovery solutions, and verify whether the solutions are applicable and effective. The existing services will not be affected during the DR drill. When a real fault occurs, you can use the solutions to rapidly restore services, enhancing service continuity.

SDRS provides the DR drill function. You can perform DR drills in a drill VPC (different from the VPC of the DR site). This function allows you to use the disk snapshots of the DR site servers to create drill servers with the server specifications and disk types same as the DR site servers.

NOTE

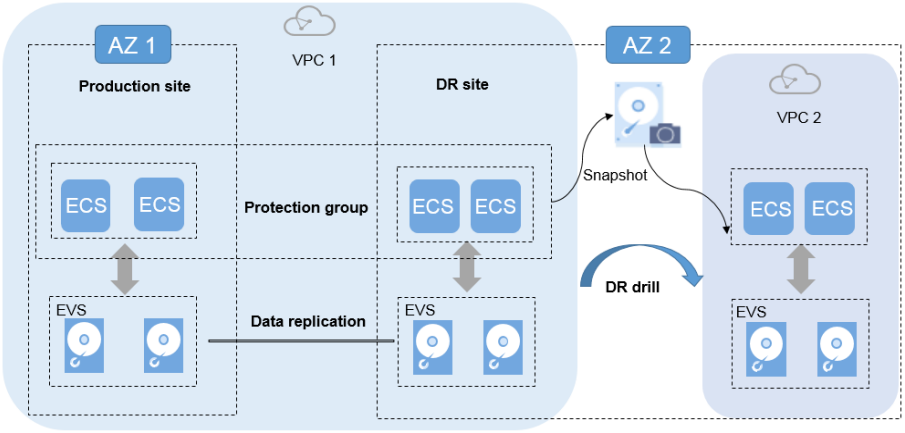
After the DR drill server is created, the production site server and DR drill server will independently run at the same time (data will not be synchronized between these two servers).

To ensure that a failover can be properly performed if a disaster happens, you are recommended to perform DR drills regularly to verify that:

- The production site data and DR site data are consistent at the moment when you create a DR drill.
- The services at the DR site can run properly after a failover.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Performing a DR drill



Notes

- If the DR site server of the protection group is added to Enterprise Project, the created DR drill server will not be automatically added to Enterprise Project. You need to manually add it to Enterprise Project if needed.
- When you use a created drill VPC to create a drill, the subnet ACL rule of the drill VPC will be different from that of the VPC of the protection group. You need to manually set them to be the same one if needed.
- When you create a DR drill, if the VPC of the protection group has a customized routing table and subnets configured, the corresponding routing table will not be automatically created for the drill VPC. You need to manually create it if needed.
- If the DR site server runs Windows and uses the key login mode, ensure that the key pair of the DR site server exists when you create a DR drill. Otherwise, the DR drill server may fail to create, causing the DR drill creation failure.

  NOTE

  If the key pair of the DR site server has been deleted, create a key pair with the same name.
- When you create a DR drill, if the DR site server runs Linux and uses the key login mode, the key pair information will not be displayed on the details page of the DR drill server after the DR drill server is created. You can use the key pair of the DR site server to log in to the DR drill server.
- After you create a DR drill, modifications to the **Hostname**, **Name**, **Agency**, **ECS Group**, **Security Group**, **Tags**, and **Auto Recovery** configurations of the DR site server before the drill will not synchronize to the DR drill server. You can log in to the management console and manually add the configuration items to the DR drill server.
- If the synchronization progress of replication pairs in the protection group is not 100%, the created DR drill server may fail to start. You are advised to perform a DR drill 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.

 Copyright © Huawei Technologies Co., Ltd.

- Do not perform a DR drill before the first time data synchronization between the production site server and DR site server completes. Otherwise, the drill server 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.

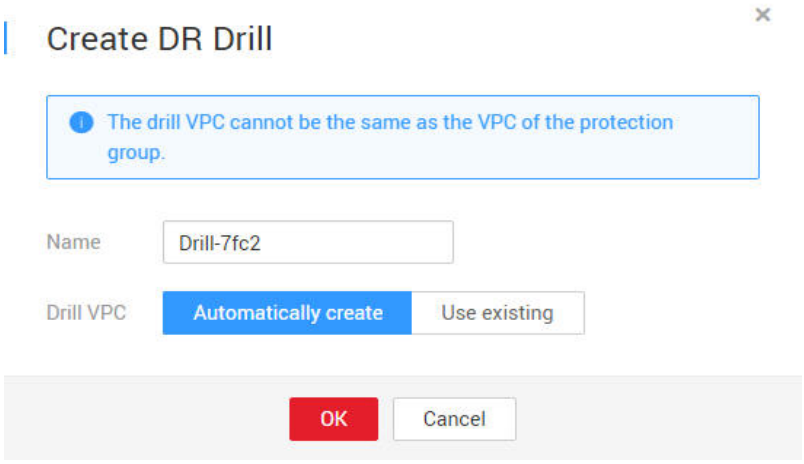
Step 3 In the pane of the protection group to which a DR drill is to be added, click **DR Drills**.

The operation page for the protection group is displayed.

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

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

Figure 5-2 Creating a DR drill



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

Table 5-1 Parameter description

Parameter	Description	Example Value
Name	Specifies the DR drill name.	DR drill servername

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Drill VPC	The VPC is used for a DR drill and cannot be the same as the VPC of the DR site server. Specifies the drill VPC. The value can be **Automatically create** or **Use existing**. • **Automatically create**: The system automatically creates a drill VPC and subnets 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 a DR drill is created, you can log in to the DR drill server and check whether services are running properly.

----End

5.2 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.

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

6 Interconnecting with CTS

6.1 Key SDRS Operations Recorded by CTS

Table 6-1 SDRS operations that can be recorded by CTS

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

 Copyright © Huawei Technologies Co., Ltd.

Operation	Resource Type	Trace Name
Creating a protected instance	protectedInstance	createProtectedInstance
Deleting a protected instance	protectedInstance	deleteProtectedInstance
Updating a protected instance	protectedInstance	updateProtectedInstance
Attaching a replication pair to a protected instance	protectedInstance	attachReplicationPair
Detaching a replication pair from a protected instance	protectedInstance	detachReplicationPair
Adding a NIC to a protected instance	protectedInstance	addNic
Deleting a NIC from a protected instance	protectedInstance	deleteNic
Modifying the specifications of a protected instance	protectedInstance	resizeProtectedInstance
Creating a replication pair	replicationPair	createReplicationPair
Deleting a replication pair	replicationPair	deleteReplicationPair
Updating a replication pair	replicationPair	updateReplicationPair
Expanding the capacity of a replication pair	replicationPair	expandReplicationPair
Creating a DR drill	disasterRecoveryDrill	createDrDrill
Deleting a DR drill	disasterRecoveryDrill	deleteDrDrill
Updating a DR drill	disasterRecoveryDrill	updateDrDrill

6.2 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.

 Copyright © Huawei Technologies Co., Ltd.

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 on the left, 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.

 Copyright © Huawei Technologies Co., Ltd.

7 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.

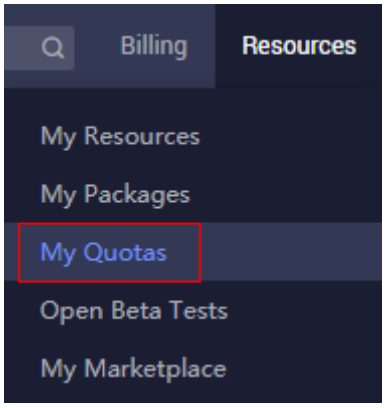
If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

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 7-1 My Quotas

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

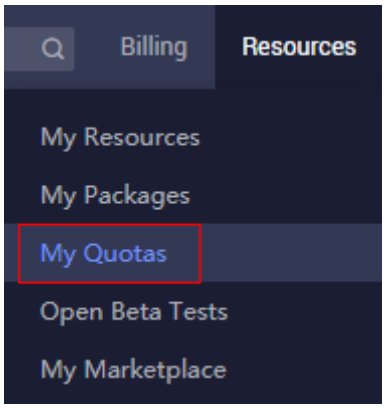
   If a quota cannot meet service requirements, apply for a higher quota.

 Copyright © Huawei Technologies Co., Ltd.

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 7-2 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**.

 Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2020-04-29	This is the tenth 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 ninth official release. Modified the following content: Added a parameter example in **Creating a Replication Pair**.
2019-05-30	This issue is the seventh official release. Added the following content: • **Permissions Management** Modified the following content: • Added notes on attaching a replication pair in **Attaching a Replication Pair**.
2019-03-30	This issue is the sixth official release. Modified the following content: • Modified descriptions of modifying the specifications of the production site server and DR site server in **Modifying Specifications of a Protected Instance**. Deleted the following content: • Section "Performing a Planned Failback" • Section "Performing a Failback"

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2019-01-30	This issue is the fifth official release. Added the following content: • **Managing Quotas** Modified the following content: • Deleted concepts of the source end, target end, preferred end, and added the concepts of the production site and DR site.
2018-11-30	This issue is the fourth official release. Added FAQs: What Can I Do When the EIP Cannot Be Pinged After I Perform Failover for a Protection Group Containing a SUSE Production Site Server?
2018-10-24	This issue is the third official release. This release incorporates the following change: Added FAQ "What Can I Do If Disks Detached from Servers in Protected Instances Cannot Be Attached to Xen Servers?"
2018-08-03	This issue is the second official release. This release incorporates the following change: • Modified the SDRS deployment models. • Modified the limitations of SDRS. • Optimized the descriptions of protected instance creation parameters. • Optimized the descriptions of replication pair creation parameters.
2018-05-30	This issue is the first official release.

Copyright © Huawei Technologies Co., Ltd.