Storage Disaster Recovery Service

Quick Start

Issue 05

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 Configuring Cross-AZ DR for Servers..... 1
1.1 Configuration Process..... 1
1.2 Step 1: Create a Protection Group..... 2
1.3 Step 2: Create a Protected Instance..... 4
1.4 Step 3: Enable Protection..... 10
2 Performing a DR Drill..... 13
3 Change History..... 17

 Copyright © Huawei Technologies Co., Ltd.

1 Configuring Cross-AZ DR for Servers

1.1 Configuration Process

SDRS uses storage-layer synchronization and replication to provide cross-AZ DR to ensure data crash consistency and server-level protection with zero RPO. If a source AZ encounters a disaster (such as a fire or an earthquake) or a device fault (such as a software or hardware damage), replications running in the source AZ can quickly restore in the target AZ.

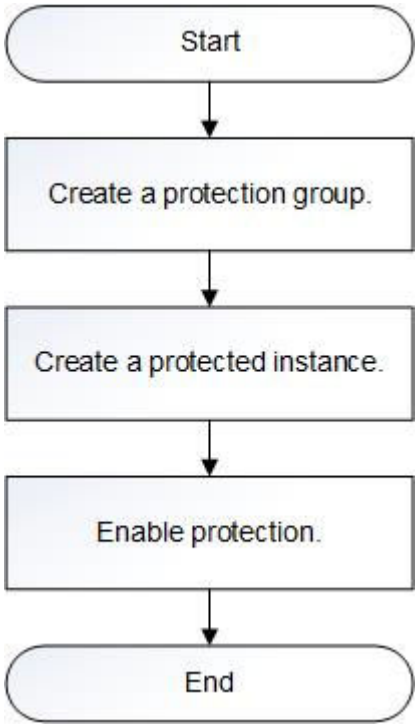
Figure 1-1 shows the cross-AZ DR configuration process.

NOTE

When you create a protected instance, the system creates a replication pair for the disks of the servers at the production and DR site by default.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 Cross-AZ DR configuration process



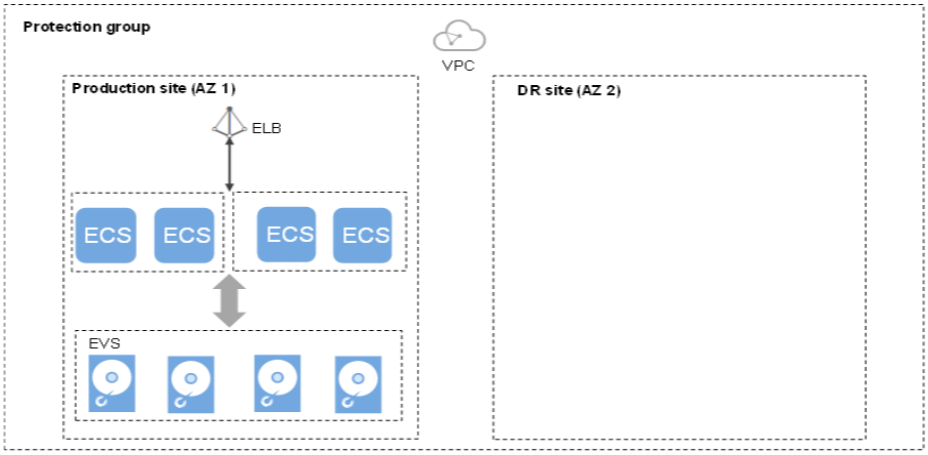
1.2 Step 1: Create a Protection Group

Scenarios

You can specify two AZs as the source and target AZs, and create a protection group. Then, you can create protected instances and replication pairs in this protection group.

Verify the servers at the production and DR sites before you create a protection group. In this version, only the VPC migration deployment model is supported. Specifically, the servers at the production and DR sites must be in different AZs but in the same VPC.

Figure 1-2 Creating a protection group



Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

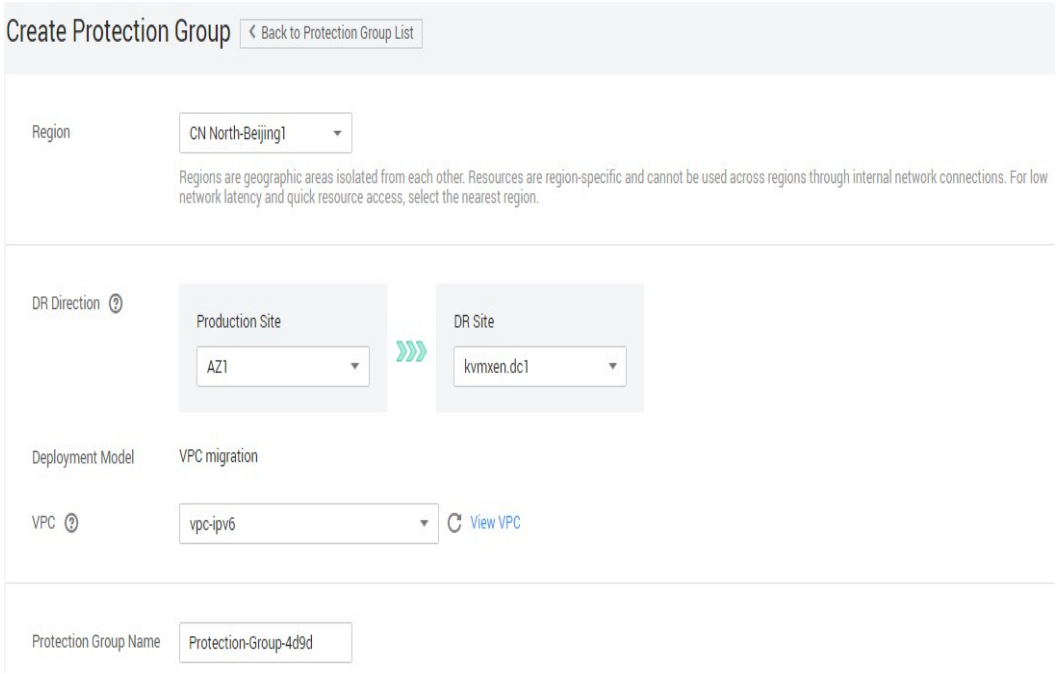
Step 2 Click **Service List** and choose **Storage** > **Storage Disaster Recovery Service**.

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

Step 3 Click **Create Protection Group**.

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

Figure 1-3 Creating a protection group



Step 4 Configure the basic information about the protection group listed in **Table 1-1**.

NOTE

All the parameters in the following table are mandatory.

Table 1-1 Parameter description

Parameter	Description	Example Value
Region	A region is a geographic area where resources used by servers are located. If the region is incorrect, click the drop-down list for correction.	CN North-Beijing1

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
DR Direction	• Production site: Select the AZ of the production site server. • DR site: Select the AZ of the DR site server. **NOTE** If SDRS is not provided in an AZ, you cannot select the AZ from the AZ list. For details about the AZs where SDRS is supported, see **Storage Disaster Recovery Service**.	Production site: az-01 DR site: az-02
Deployment Model	Currently, only the VPC migration model is supported. All resources at the production and DR sites belong to the same VPC.	VPC migration
VPC	Specifies the VPC where the protection group is located.	vpc-test
Protection Group Name	Enter the protection group name. It is used for group classification and search.	protection_group_001

Step 5 Click **Create Now**.

Step 6 Click **Back to Protection Group List** to return to the SDRS homepage and query the protection group status.

If the protection group is displayed in the **Storage Disaster Recovery Service** page and its status is **Available** ( ), the protection group has been created successfully.

----End

1.3 Step 2: Create a Protected Instance

Scenarios

You can create protected instances using the servers that you want to perform DR protection. If the current production site encounters an unexpected large-scale server failure, you can call the related protection group API to perform a failover, ensuring that services running on protected instances are not affected.

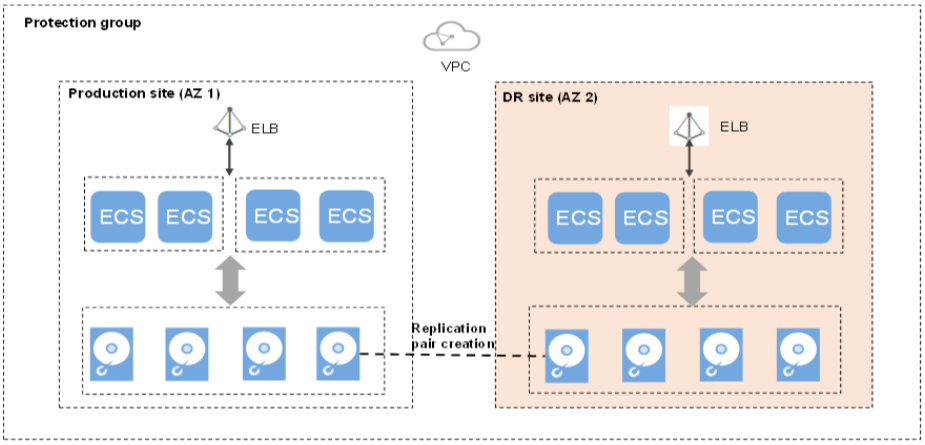
Select a protection group for each server to be replicated and create a protected instance using the server. When you create a protected instance, the server and

 Copyright © Huawei Technologies Co., Ltd.

disk will be created at the DR site for the production site server and disk. The server specifications can be configured as required. Specifically, the specifications of the DR site server can be different from those of the production site server. The disks of the production site and DR site are of the same specifications and can automatically form a replication pair.

The server at the DR site is in the Stopped state after the protected instance created. These automatically created resources, including the DR site servers and disks, cannot be used before a planned failover or failover.

Figure 1-4 Creating a protected instance



Notes

- If a production site server has been added to an ECS group, you are not allowed to specify a DeH to create the DR site server for the production site server.
- When a protected instance is created, the default name of the server at the DR site is the same as that of the server at the production site, but their IDs are different.
- To modify a server name, switch to the protected instance details page and click the server name to switch to the server details page.
- After you create a protected instance and enable protection for the protection group, modifications to the **Hostname**, **Name**, **Agency**, **ECS Group**, **Security Group**, **Tags**, and **Auto Recovery** configurations of the production site server will not synchronize to the DR site server. You can log in to the management console and manually add the configuration items to the servers at the DR site.
- If protection is enabled for servers created during capacity expansion of an Auto Scaling (AS) group, these servers cannot be deleted when the capacity of the AS group is reduced.
- If the server at the production site runs Windows and you choose the key login mode, ensure that the key pair of the server exists when you create a protected instance. Otherwise, the server at the DR site may fail to create, causing the protected instance creation failure.

  NOTE

  If the key pair of the server at the production site has been deleted, create a key pair with the same name.

Copyright © Huawei Technologies Co., Ltd.

- When you create a protected instance, if the production 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 site server after the DR site server is created. You can use the key pair of the production site server to log in to the DR site server.
- If the production site server is added to Enterprise Project, the created DR site server will not be automatically added to Enterprise Project. You need to manually add it to Enterprise Project if needed.

Prerequisites

- The protection group is in the **Available** or **Protecting** state.
- No protected instances have been created for the production site server.
- Resources of the target specifications for the server to be protected are not sold out at the DR site.
- The server that you use to create a protected instance and the protection group are in the same VPC.

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.

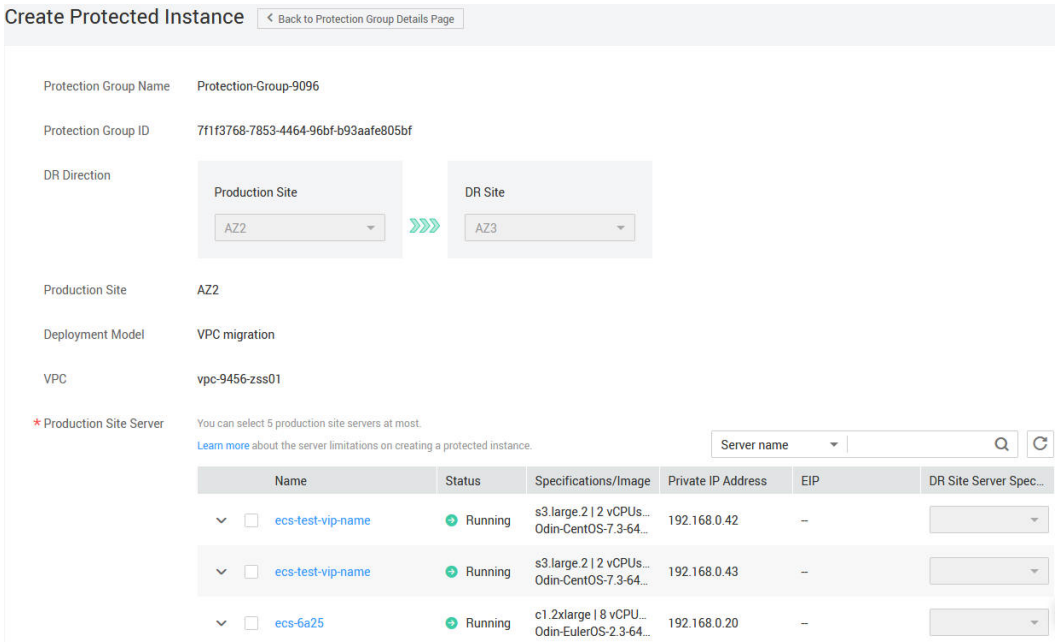
Step 3 In the pane of the protection group for which protected instances are to be added, click **Protected Instances**.

The operation page for the protection group is displayed.

Step 4 On the **Protected Instances** tab, click **Create Protected Instance**.

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

Figure 1-5 Creating a protected instance



 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the basic information about the protected instance, as described in **Table 1-2**.

Table 1-2 Parameter description

Parameter	Description	Example Value
Protection Group Name	Indicates the name of the protection group to which the protected instance to be created belongs. You do not need to configure it.	protection_group_001
Protection Group ID	Indicates the ID of the protection group to which the protected instance to be created belongs.	2a663c5c-4774-4775-a321-562a1ea163e3
DR Direction	Indicates the replication direction of the protection group to which the protected instance to be created belongs. You do not need to configure it.	-
Production Site	Indicates the AZ of the production site server. You do not need to configure it.	az-01
Deployment Model	Indicates the deployment model of the protection group to which the protected instance to be created belongs. You do not need to configure it.	VPC migration
VPC	Indicates the VPC of the protection group to which the protected instance to be created belongs. You do not need to configure it.	vpc1

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Production Site Server	This parameter is mandatory. In the server list, select the server and specifications to be used to create the protected instance. • You can select a maximum of five production site servers at a time. • If a shared disk is attached to a server, you need to select all servers to which the shared disk is attached. **NOTE** • If **Server Type** of the protection group is **ECS**, select the DR site server specifications. The specifications of the production site server and DR site server can be different. Select the specifications from the **DR Site Server Specifications** drop-down list.	ecs-test > s3.small.1
DR Site Server	This parameter is mandatory when **Server Type** of the protection group is **ECS**. You can select to use ECSs to create DR site servers or to deploy DR site servers on DeHs. DeHs are physical hosts dedicated for a specified user. You can create servers on a DeH to enhance isolation, security, and performance of your ECSs. **NOTE** If a production site server has been added to an ECS group, you are not allowed to specify a DeH to create the DR site server for the production site server.	ECS

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
DeH	This parameter is mandatory when **DR Site Server** is set to **DeH**. Select a DeH for deploying the DR site server. If multiple production site servers are selected, the DR site servers will be created on the same DeH.	deh-01
DR Site VPC	Indicates the VPC of the DR site server. Its value is the same as the **VPC** value and do not need to be configured.	vpc1
DR Site Primary NIC	This parameter is optional. Indicates the primary NIC on the DR site server. You can use the primary NIC automatically allocated by the system or specify a primary NIC based on your network plan. After your select a NIC, select an available subnet from the drop-down list and configure the private IP address. **NOTE** You cannot specify the IP addresses if you create multiple protected instances at a time.	subnet-01 (192.168.0.0/24)
DR Site Disk	This parameter is mandatory. The following two options are available: • **EVS** • **DSS** If you select **DSS** for **DR Site Disk**, **Storage Pool** is mandatory.	EVS

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
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
Protected Instance Name	This parameter is mandatory. Enter the protected instance name. It is used for protected instance classification and search.	Protected-Instance-test

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 protected instance 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 protected instances of the protection group.

If the protected instance status changes to **Available** or **Protecting**, the protected instance has been created successfully.

NOTE

After a protected instance is created, the system automatically creates replication pairs for the disks of the protected instance and backs up all the disks.

Query the replication pairs.

1. Switch to the operation page for the protection group.
2. Click the **Replication Pairs** tab.

   On this tab, you can query the statuses of the replication pairs, target protected instance, and production site disk.

----End

1.4 Step 3: Enable Protection

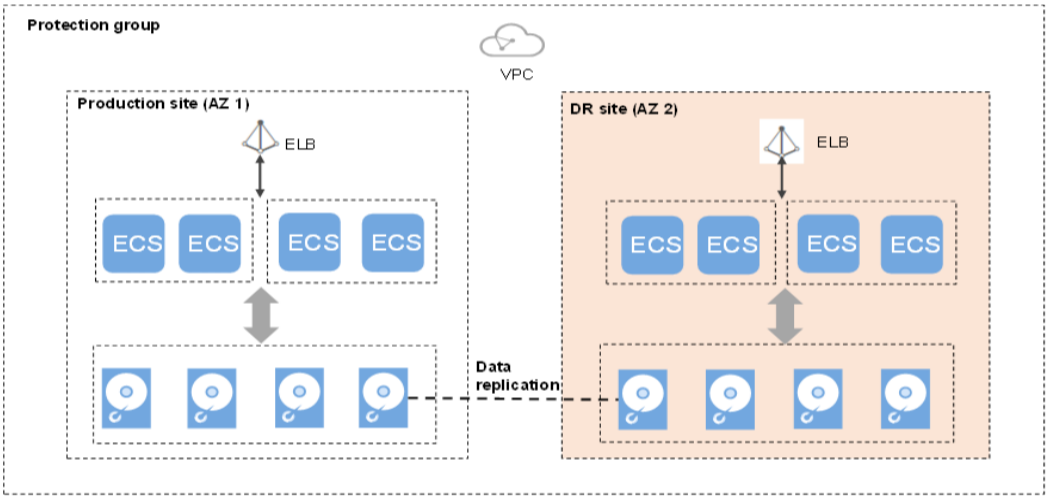
Scenarios

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

 Copyright © Huawei Technologies Co., Ltd.

When data is written to the disks of the production site server, SDRS synchronizes the data to the disks of the DR site server in real time. Both the production site and DR site can use Cloud Server Backup Service (CSBS) and Volume Backup Service (VBS) to back up the servers and disks.

Figure 1-6 Enabling protection



Prerequisites

- The protection group has replication pairs.
- The protection group is in the **Available** or **Enabling protection failed** state.
- After you create a protected instance and enable protection on servers at the production site, modifications to the **Hostname**, **Name**, **Security Group**, **Agency**, **ECS Group**, **Tags**, and **Auto Recovery** configurations of servers on the production site will not synchronize to the servers at the DR site. You can manually add the configuration items to the servers at the DR site on the management console.

Procedure

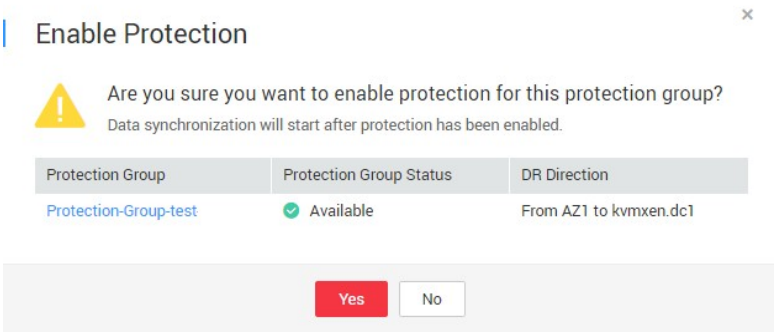
Step 1 Log in to the management console.

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 **Enable Protection**.

Figure 1-7 Enabling protection



 Copyright © Huawei Technologies Co., Ltd.

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

Once protection is enabled, data synchronization starts.

> **NOTE**
>
> The synchronization time is in direct proportion to the disk capacity. Larger disk capacity requires longer synchronization time.

----End

 Copyright © Huawei Technologies Co., Ltd.

2 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.

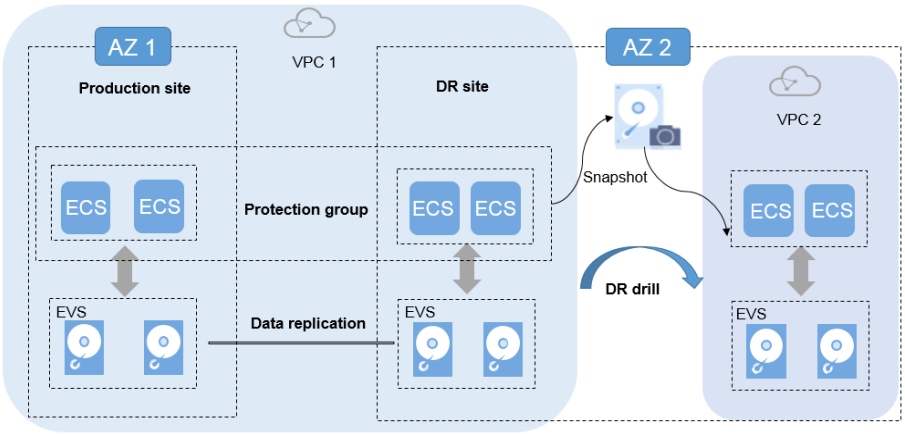
NOTE

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.

Figure 2-1 Performing a DR drill



 Copyright © Huawei Technologies Co., Ltd.

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.
- 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**.

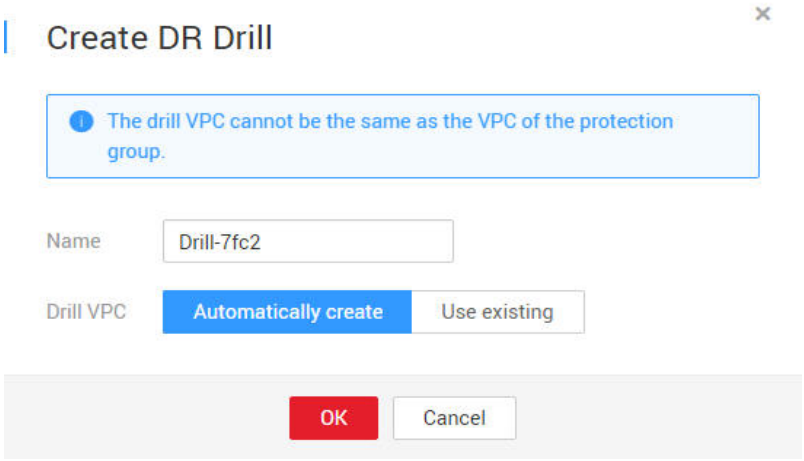
The operation page for the protection group is displayed.

 Copyright © Huawei Technologies Co., Ltd.

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

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

Figure 2-2 Creating a DR drill



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

Table 2-1 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

 Copyright © Huawei Technologies Co., Ltd.

3 Change History

Released On	Description
2020-04-29	This issue is the fifth official release. Modified the following content: Modified restrictions in **Step 2: Create a Protected Instance**. Specifically, shared disks are supported.
2019-09-30	This issue is the fourth official release. Modified the following content: Added descriptions about DeHs in **Step 2: Create a Protected Instance**.
2019-03-30	This issue is the third official release. This release incorporates the following change: Modified the following content: • Added descriptions of automatic VPC creation in **Performing a DR Drill**.
2019-01-30	This issue is the second official release. This release incorporates the following change: • Deleted concepts of the source end, target end, preferred end, and added the concepts of the production site and DR site. • Optimize the section names.
2018-05-30	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.