eSDK Enterprise Storage Plugins 2.2.RC1

User Guide (SRA)

Issue	01
Date	2020-07-30

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

HUAWEI 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://e.huawei.com

Preface

Purpose

This document provides an overview of the Storage Replication Adapter (SRA) and describes how to install, configure, and uninstall it.

Intended Audience

This document is intended for:

- Technical support engineers
- Third-party engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

 Copyright © Huawei Technologies Co., Ltd.

Symbol	Description
NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

 Copyright © Huawei Technologies Co., Ltd.

Contents

Preface ii

1 SRA Overview 1

1.1 Introduction to the SRA 1

1.2 Networking 3

1.2.1 Networking for Active/Standby Redundancy 3

1.2.2 Networking for HyperMetro 4

1.2.3 Networking for Geo-redundant DR 5

1.2.3.1 Networking for Cascading Geo-Redundant DR 6

1.2.3.2 Networking for DR Star 6

1.3 HyperMetro Fault Scenario Description 8

2 Preparing for the Installation 12

2.1 Device Types and Versions 12

2.2 Operating Environment Requirements 12

2.2.1 Active/Standby Redundancy 12

2.2.2 HyperMetro 13

2.2.3 Geo-redundant DR 14

3 Installing SRA 16

3.1 Installing SRA in a Windows Environment 16

3.2 Installing SRA in a Linux (SRM VA) Environment(Photon OS) 19

4 Typical Scenario Configuration 20

4.1 SAN Active/Standby Scenario 20

4.2 SAN HyperMetro Scenario 21

4.3 NAS Active/Standby Scenario 22

4.4 Geo-redundant DR Scenario 23

4.5 Common Configuration Operations 24

4.5.1 Creating a Datastore (VMFS) 24

4.5.2 Creating a Datastore (NFS) 26

4.5.3 Creating VMs 28

4.5.4 Creating a Tag 32

4.5.5 Assigning the Tag to the Created Data Store 33

4.5.6 Creating a VM Storage Policy 35

4.5.7 Applying the VM Storage Policy to VMs 36

4.5.8 Setting Up a Connection Between the vCenter Servers at the Protected Site and Recovery Site.....37
4.5.9 Configuring Mapping Between the vCenter Servers at the Protected Site and Recovery Site.....39
4.5.10 Creating and Configuring Placeholder Storage.....48
4.5.11 Adding Array Managers.....49
4.5.12 Creating a Datastore-Based Protection Group.....53
4.5.13 Creating a Policy-Based Protection Group.....56
4.5.14 Creating a Recovery Plan (Based on VM Protection Groups).....58
4.5.15 Creating a Recovery Plan (Based on a Storage Policy for a Protection Group).....61

5 Fault Recovery Scenarios.....64
5.1 Recovery Plan Test.....64
5.2 Planned Migration.....67
5.3 Disaster Recovery.....70
5.4 Switchback.....72

6 Uninstalling SRA.....74
6.1 Uninstalling SRA in a Windows Environment.....74
6.2 Uninstalling SRA in the SRM VA Environment.....74

7 Troubleshooting.....76

8 FAQ.....77
8.1 System Displays an Error Message During a Planned Migration.....77
8.2 Cleanup Lock Failure.....78
8.3 Reprotection Failure.....78
8.4 A Reprotection Task Fails During Remote Replication.....79
8.5 Shutting Down the VM at the Protected Site Fails.....79
8.6 vCenter Cannot Detect the Installed SRA Plug-in.....80
8.7 No Result Is Returned for a Planned Migration.....80
8.8 Failed to Execute Planned Fault Recovery or Test a Recovery Plan.....81
8.9 "Recovered device xxx not found after HBA rescan" Is Displayed When the Recovery Plan Fails to Be Tested.....82
8.10 A File Copy Error Is Displayed During a Planned Migration or DR.....83
8.11 No Datastore Can Be Found During Data Center Switchback in the Geo-redundant DR Scenario.....84
8.12 A Placeholder Error Occurs During Reprotection.....85

1 SRA Overview

1.1 Introduction to the SRA
1.2 Networking
1.3 HyperMetro Fault Scenario Description

1.1 Introduction to the SRA

The SRA is a communication bridge between a storage system and the Site Recovery Manager (SRM). When the SRM creates, tests, and executes a recovery plan or executes a planned migration, the SRA enables the storage system to cooperate with the SRM to complete the operations.

The SRA is a software product that enables a storage system to cooperate with the SRM to implement storage system management. The SRA provides the SRM with storage system information, including information about storage system discovery, replication LUN discovery, failover tests, and disaster recovery. When the SRM creates, tests, and executes a recovery plan, the SRA immediately provides corresponding resources for the SRM and cooperates with the SRM to complete uninterrupted tests, site recovery automation, and migration process automation in a virtual environment.

Two types of disaster recovery solution are available: active/standby redundancy and HyperMetro. Both types are supported by the SRA.

Active/Standby Redundancy

In the active/standby redundancy, one protected site and one recovery site are deployed. The recovery site does not work unless the protected site breaks down upon a disaster.

HyperMetro

When natural or human-caused disasters happen or some devices or a data center fails, large-scale enterprises require not only disaster recovery switchovers for data protection, but also online service switchovers between data centers or even the load balancing function. Therefore, functions such as effective online service check, switchover, and load balancing are required in addition to a real-time copy

 Copyright © Huawei Technologies Co., Ltd.

of data. The HyperMetro data center solution can meet all the preceding requirements.

HyperMetro is a feature of Hyper feature series of Huawei storage systems. HyperMetro can implement synchronous data replication, real-time monitoring of service running status, and switchovers between storage systems.

HyperMetro requires at least two storage systems. The two storage systems can be placed in the same equipment room, the same city, or two cities with a 100 km distance between them.

Two HyperMetro modes are available: A/A and A/P. In A/A mode, the storage arrays at both ends provide services. In A/P mode, only the storage array at one end provides services. When this storage array fails, the storage array at the other end provides services. HyperMetro implements LUN A/A.

In LUN A/A, data on the LUNs at the two ends is synchronized in real time, and hosts can read and write LUNs at both ends. If the storage array at one end malfunctions, hosts access services on the storage array at the other end.

Application Scenarios

Application Scenario	Function Description
The SRM creates a recovery plan.	The SRA provides the SRM with storage system information, including the storage array name, system type, and LUN information, to help the SRM create a recovery plan.
The SRM tests a recovery plan.	The SRA receives a recovery plan test command from the SRM and sends the command to a storage system at a recovery site. The storage system automatically generates an activated data snapshot. The snapshot is then used to test the data accuracy and availability of the recovery site.
The SRM executes a disaster recovery.	The SRA receives a fault recovery command from the SRM and sends the command to the storage system at a recovery site. Data storage groups in LUN duplicates of the storage system are immediately enabled, ensuring that virtual machines (VMs) at the recovery site are started correctly.

 Copyright © Huawei Technologies Co., Ltd.

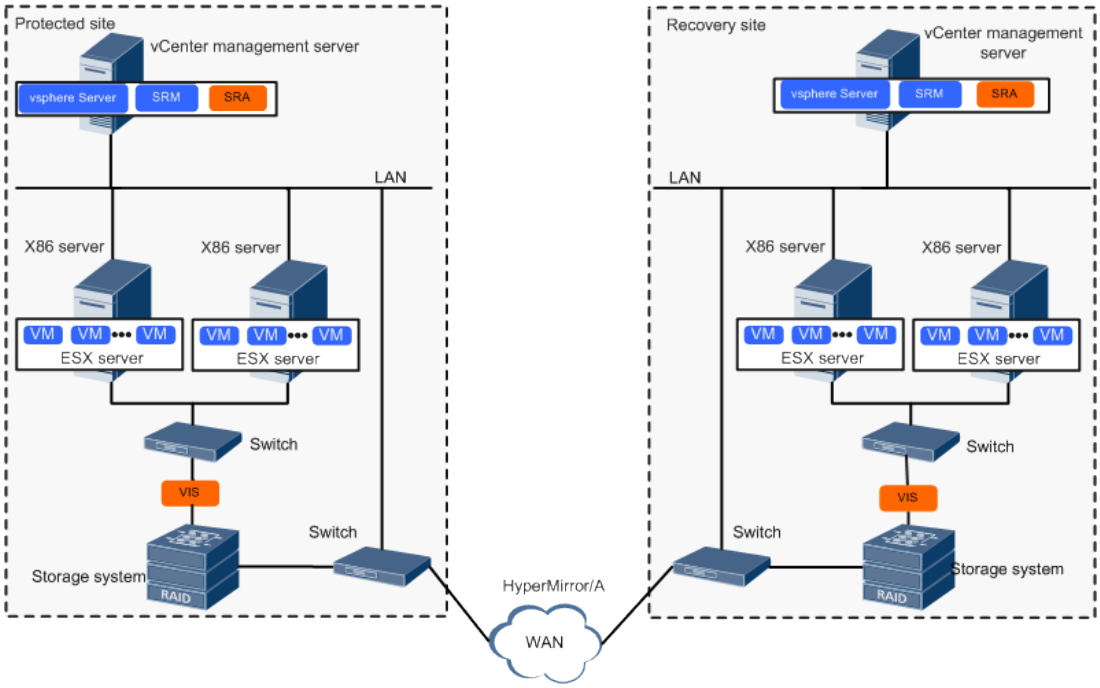
Application Scenario	Function Description
The SRM executes a planned migration.	A planned migration is performed for system maintenance or is manually performed by users to protect services against potential disasters. The planned migration ensures service consistency and data integrity. There are three migration scenarios based on whether storage arrays support SRM Stretch: ● If storage arrays do not support SRM Stretch, VMs are shut down at the protected site. After data is replicated to the recovery site, VMs are started at the recovery site. Services are interrupted during the process. ● If storage arrays support SRM Stretch and if the vSphere vMotion function is enabled, the SRM sets stretch storage from the protected site to the recovery site. Then, the SRM uses the vSphere vMotion function to migrate protected VMs in the storage profile protection groups (SPPG) to the recovery site. The services of the protected VMs are not interrupted during the process. ● If storage arrays support SRM Stretch and if the vSphere vMotion function is disabled, the SRM sets stretch storage from the protected site to the recovery site. VMs are shut down at the protected site. After data is replicated to the recovery site, VMs are started at the recovery site. Services are interrupted during the process.

1.2 Networking

1.2.1 Networking for Active/Standby Redundancy

Figure 1-1 shows the networking for active/standby redundancy.

Figure 1-1 Networking for active/standby redundancy



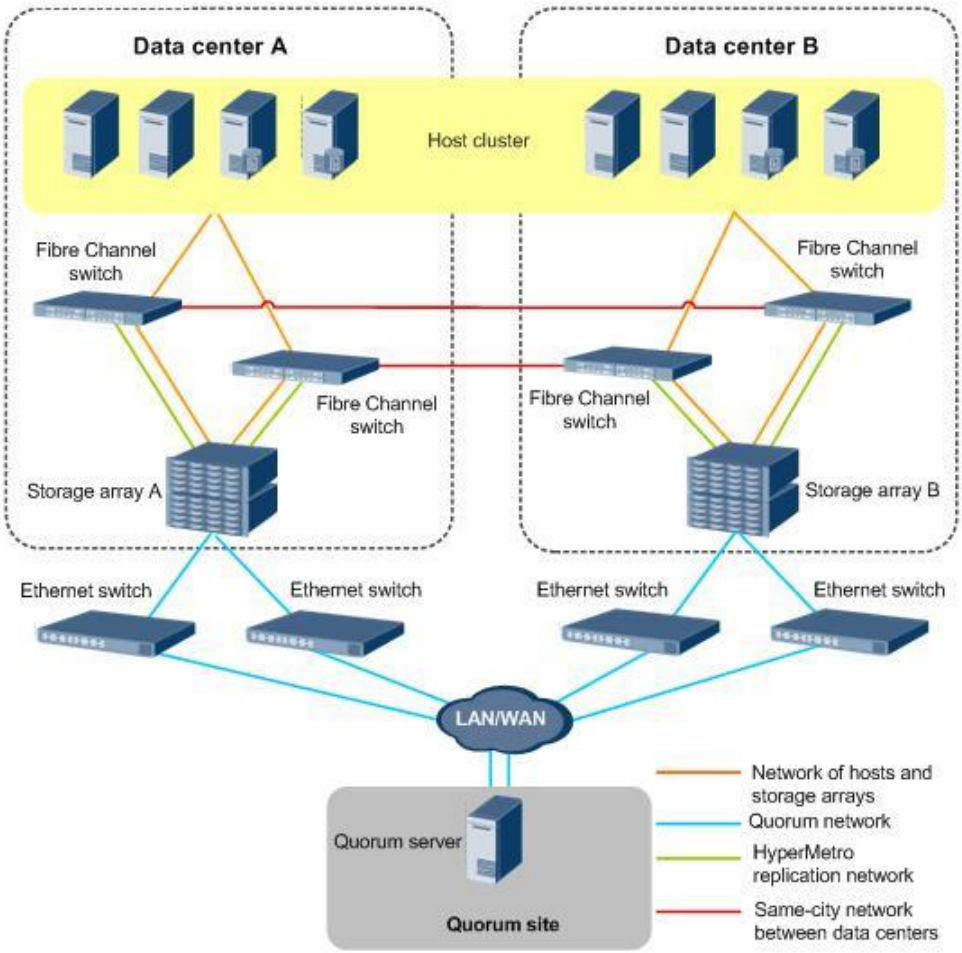
The application scenario of the SRA features in:

- Delivering block-level replication without consuming the network bandwidth of the host services.
- Generating a snapshot that helps the SRM to test the recovery plan.
- Producing a data copy that helps the SRM to run the recovery plan.
- Uniformly managing the recovery plan by integrating the management over the storage system into the SRM interface.

1.2.2 Networking for HyperMetro

Figure 1-2 shows the networking for HyperMetro.

Figure 1-2 Networking for HyperMetro



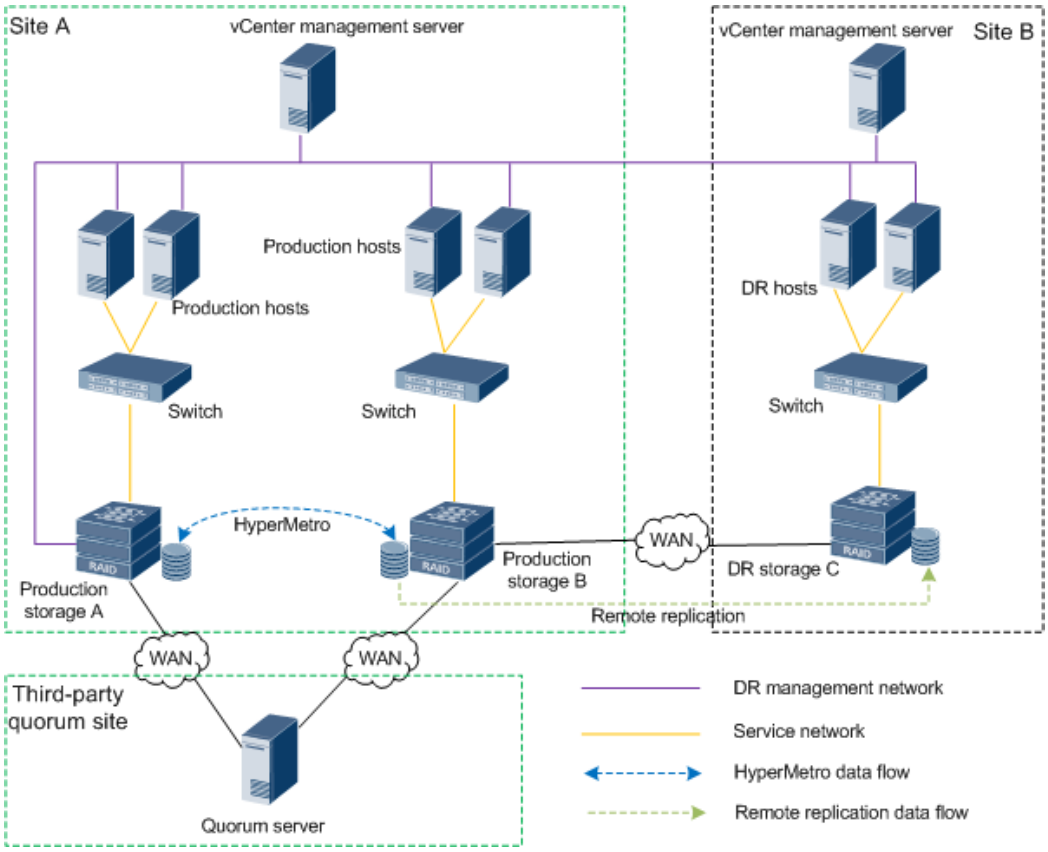
- Same-city data center network: The storage arrays in both data center A and data center B provide services for hosts and can carry the same services. A mutual backup relationship is set up between the storage arrays in the two data centers. If the storage array in one data center malfunctions, the storage array in the other data center automatically takes over services without data loss or service interruption.
- Network between hosts and storage arrays: All hosts in the two data centers can be used to form a cluster. Host networks can be interconnected across data centers.
- HyperMetro replication network: It is the heartbeat network between the storage arrays in the two data centers. It enables the storage arrays to concurrently provide services for hosts and ensures data synchronization between the storage arrays in the two data centers.
- Quorum network: The HyperMetro quorum server is deployed on the network. If communication between the storage arrays in data center A and data center B is interrupted or a storage array malfunctions, the quorum server determines which storage array can be accessed.

1.2.3 Networking for Geo-redundant DR

1.2.3.1 Networking for Cascading Geo-Redundant DR

Figure 1-3 shows the networking for cascading geo-redundant DR.

Figure 1-3 Networking for cascading geo-redundant DR

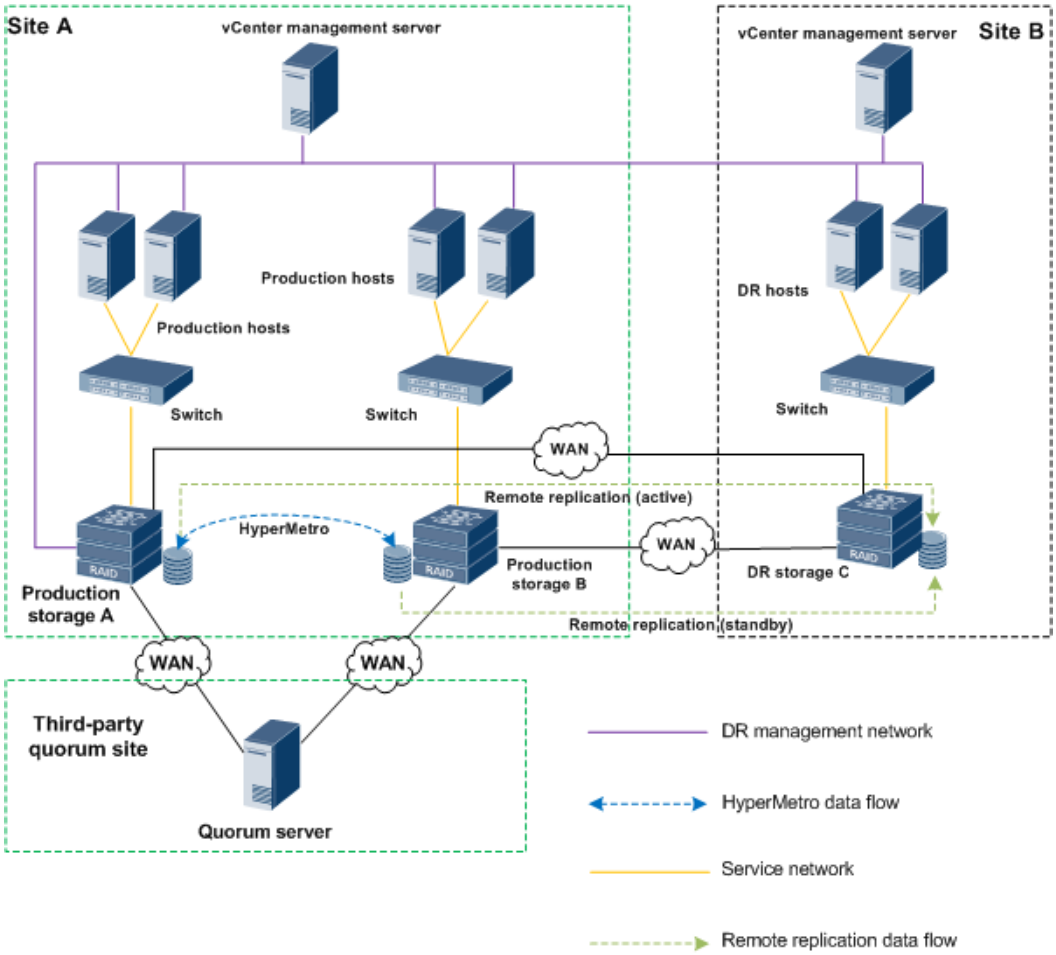


- The networking for cascading geo-redundant DR supports only SAN.
- SAN HyperMetro networking is used between production storage A and production storage B. For details, see **1.2.2 Networking for HyperMetro**.
- SAN active/standby redundancy networking is used between production storage B and DR storage C. For details, see **1.2.1 Networking for Active/Standby Redundancy**.
- When you create a DR protection plan, a protection group and a recovery plan are created only between production storage B and DR storage C.

1.2.3.2 Networking for DR Star

Figure 1-4 shows the networking for DR Star.

Figure 1-4 Networking for DR Star



- The networking for DR Star supports only SAN.
- SAN HyperMetro networking is used between production storage A and production storage B. For details, see **1.2.2 Networking for HyperMetro**.
- SAN active/standby redundancy networking is used between production storage A and DR storage C and between production storage B and DR storage C. For details, see **1.2.1 Networking for Active/Standby Redundancy**.
- When you create a DR protection plan for the first time, a protection group and a recovery plan are created only between the members of the active remote replication pair.

NOTE

For DR Star, if the production storage where the active remote replication pair resides is faulty, SRM cannot automatically establish DR protection for the standby remote replication pair. If you want to establish DR protection for the standby remote replication pair, you need to manually delete the original recovery plan of the active remote replication pair and then create a recovery plan for the standby remote replication pair.

1.3 HyperMetro Fault Scenario Description

If the link between two data centers breaks down, data cannot be synchronized between the two data centers and only one data center continues providing services. To ensure data consistency, HyperMetro adopts an arbitration mechanism to determine priorities of services in data centers.

HyperMetro supports two arbitration modes:

- Static Priority Mode: Applies to scenarios where no third-place quorum server is deployed.
- Quorum Server Mode: Applies to scenarios where third-place quorum servers are deployed.

Types of Faults in Static Priority Mode

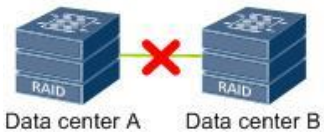
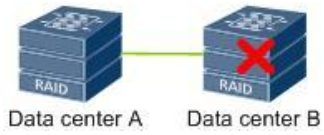
The Static Priority Mode applies to scenarios where no third-place quorum server is deployed. In a HyperMetro pair, you can set one data center as a preferred site and the other data center as a non-preferred site.

- If the link between the two storage arrays in the two data centers or the storage array at the non-preferred site breaks down, LUNs of the storage array at the preferred site continue providing services for hosts but LUNs of the storage array at the non-preferred site stop providing services for hosts.
- If the storage array at the preferred site breaks down, the storage array at the non-preferred site cannot automatically take over HyperMetro services from the storage array at the preferred site. As a result, HyperMetro services stop. In this case, the storage array at the non-preferred site cannot provide services for hosts by performing disaster migration on SRM. Instead, you must forcibly start the storage array at the non-preferred site to provide services for hosts.

In the following example, data center A is used as a preferred site. **Table 1-1** lists the types of faults in Static Priority Mode.

 Copyright © Huawei Technologies Co., Ltd.

Table 1-1 Types of faults in Static Priority Mode

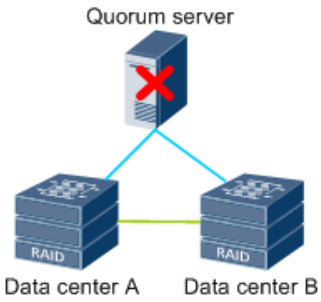
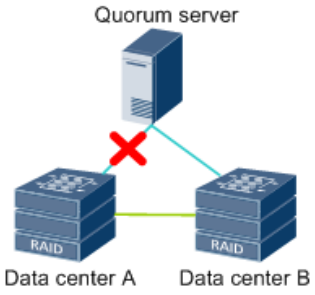
No.	Fault Diagram	Fault Type	HyperMetro Pair Running Status	Arbitration Result
1		The link between two storage arrays breaks down.	Synchronized	The storage array in data center A continues providing services but the storage array in data center B stops providing services.
2		The storage array in data center B (non-preferred site) malfunctions.	Synchronized	The storage array in data center A continues providing services but the storage array in data center B stops providing services.
3		The storage array in data center A (preferred site) malfunctions.	Synchronized	The storage array in data center A loses efficacy and the storage array in data center B stops providing services. You must forcibly start the storage array in data center B to enable the storage array to provide services for hosts.
Green cable: Indicates that HyperMetro replication network.				

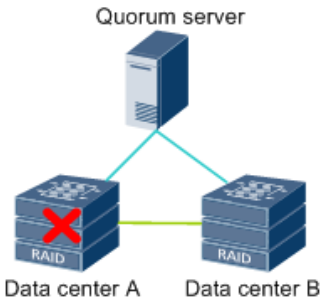
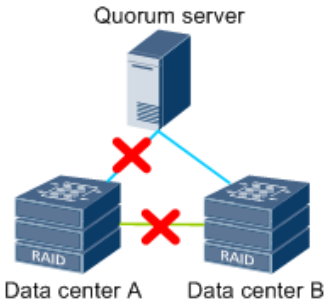
Types of Faults in Quorum Server Mode

In Quorum Server Mode, you can determine whether the storage systems work properly based on the heartbeats between storage systems in the data center. If the storage array in one data center crashes or the link between two storage arrays is down, the storage array in each data center sends an arbitration request to the quorum server. The storage array that wins the arbitration continues providing services but the storage array that fails in the arbitration stops providing services. The preferred site takes the precedence in an arbitration.

The quorum server provides different arbitration results depending on fault scenarios. Data center A is used as a preferred site. **Table 1-2** lists the types of faults in Quorum Server Mode.

Table 1-2 Types of faults in Quorum Server Mode

No.	Fault Diagram	Fault Type	HyperMetro Pair Running Status	Arbitration Result
1		The quorum server breaks down.	Normal	The storage arrays in data center A and data center B continue providing services. **NOTE** The arbitration mode of HyperMetro automatically becomes the priority mode.
2		The link between one storage array and the quorum server breaks down.	Normal	The storage arrays in data center A and data center B continue providing services.

No.	Fault Diagram	Fault Type	HyperMetro Pair Running Status	Arbitration Result
3		One storage array malfunctions.	Synchronized	The storage array in data center A loses efficacy but the storage array in data center B continues providing services.
4		Both the link between two storage arrays and the link between one storage array and the quorum server are down.	Synchronized	The storage array in data center A stops providing services but the storage array in data center B continues providing services
Green cable: Indicates that quorum network. Blue cable: Indicates that HyperMetro replication network.				

NOTICE

In Quorum Server Mode, if the storage array at the preferred site is faulty, the storage array at the non-preferred site automatically takes over services. In this case, the SRM disaster migration cannot be performed.

 Copyright © Huawei Technologies Co., Ltd.

2 Preparing for the Installation

2.1 Device Types and Versions

2.2 Operating Environment Requirements

2.1 Device Types and Versions

You can query the version mapping table of eSDK plug-ins to obtain the storage system versions. To obtain the version mapping table, log in to **http://support.huawei.com/enterprise/en/index.html**. In the search box, enter **eSDK Enterprise Storage Plugins** to search for and download the *eSDK Enterprise Storage Plugins x.x.xxx Version Mapping*. *x.x.xxx* indicates the version number.

2.2 Operating Environment Requirements

The active/standby redundancy and HyperMetro solutions have different requirements on the operating environment.

2.2.1 Active/Standby Redundancy

The SRA is based on Huawei storage array replication. Before configuring and using the SRA, check whether the storage device where the to-be-protected VMs reside has been added into a remote replication pair or a remote replication consistency group. If the storage device is not added into a remote replication pair or a remote replication consistency group, the storage array manager for the site recovery function may fail to discover the correct remote replication pair.

The configuration that needs to be performed before you configure and use the SRA includes creating LUNs, mapping LUNs to an ESXi host, partitioning the database file system,creating an NFS share, and creating a remote replication pair or a remote replication consistency group. See ***OceanStor S2600T&S5500T&S5600T&S5800T&S6800T Storage System V200R002C20 Product Documentation*** or **OceanStor Dorado 3000 V6, Dorado 5000 V6, and Dorado 6000 V6 Product Documentation**, or contact Huawei storage technical support to perform the configuration.

The SRA is designed for the service continuity plan and recovery plan of the SRM of VMware. The corresponding software environment must meet the requirements of the SRA.

Device Type	Requirements
VMware ESXi Server 6.0/6.5/6.7/7.0	VMware ESXi Servers are deployed at the protected site and recovery site.
VMware vCenter Server 6.0/6.5/6.7/7.0	VMware vSphere Servers are deployed at the protected site and recovery site.
VMware vSphere Web Client 6.0/6.5/6.7/7.0	VMware vSphere Web Clients are deployed at the protected site and recovery site.
VM	VM instances are deployed at the protected site.
SRM Server Manager 6.5/8.1/8.2/8.3	SRM Server Managers are deployed on the VMware vSphere Servers at the protected site and recovery site.
Operating system	Photon OS;Windows Server 2016 or earlier (64-bit).

2.2.2 HyperMetro

The SRA is based on Huawei storage array replication. Before configuring and using the SRA, check whether the storage device where the to-be-protected VMs reside has been added into a HyperMetro pair or a HyperMetro consistency group. If the storage device is not added into a HyperMetro pair or a HyperMetro consistency group, the storage array manager for the site recovery function may fail to discover the correct active-active pair.

The configuration that needs to be performed before you configure and use the SRA includes creating LUNs, mapping LUNs to an ESXi host, and creating a HyperMetro pair or a HyperMetro consistency group. See ***OceanStor S2600T&S5500T&S5600T&S5800T&S6800T Storage System V200R002C20 Product Documentation*** or ***OceanStor Dorado 3000 V6, Dorado 5000 V6, and Dorado 6000 V6 Product Documentation*** and ***OceanStor 5300 V3&5500 V3&5600 V3&5800 V3&6800 V3 Storage System V300R003 HyperMetro Feature Guide*** or ***OceanStor Dorado 5000 V6 6.0.0 HyperMetro Feature Guide***, or contact Huawei storage technical support to perform the configuration.

The SRA is designed for the service continuity plan and recovery plan of the SRM of VMware. The corresponding software environment must meet the requirements of the SRA.

Device Type	Requirements
Platform Services Controller 6.0/6.5/6.7	The protected site and recovery site share one Platform Services Controller.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements
VMware ESXi Server 6.0/6.5/6.7/7.0	VMware ESXi Servers are deployed at the protected site and recovery site.
VMware vCenter Server 6.0/6.5/6.7/7.0	● vSphere vCenter Servers are deployed at the protected site and recovery site. ● The two vSphere vCenter Server instances must be in enhanced link mode and must be located in the same vCenter Single Sign-On domain so that the target vSphere vCenter Server can authenticate the source vSphere vCenter Server. ● The two vSphere vCenter Server instances must synchronize time with each other so that vCenter Single Sign-On token authentication can be performed correctly. ● If only computer resources need to be migrated, the two vSphere vCenter Server instances must be connected to the shared VM storage.
VMware vSphere Web Client 6.0/6.5/6.7/7.0	VMware vSphere Web Clients are deployed at the protected site and recovery site.
VM	VM instances are deployed at the protected site.
SRM Server Manager 6.5/8.1/8.2/8.3	SRM Server Managers are deployed on the VMware vSphere Servers at the protected site and recovery site.
Operating system	Photon OS; Windows Server 2016 or earlier (64-bit)

2.2.3 Geo-redundant DR

The SRA is based on Huawei storage array replication. Before configuring and using the SRA, check whether the storage device where the to-be-protected VMs reside has been added into a remote replication pair or a remote replication consistency group. If the storage device is not added into a remote replication pair or a remote replication consistency group, the storage array manager for the site recovery function may fail to discover the correct remote replication pair.

The configuration of data center B and data center C that needs to be performed before you configure and use the SRA includes creating LUNs, mapping LUNs to

an ESXi host, partitioning the database file system, and creating a remote replication pair or a remote replication consistency group. See ***OceanStor S2600T&S5500T&S5600T&S5800T&S6800T Storage System V200R002C20 Product Documentation*** or **OceanStor Dorado 3000 V6, Dorado 5000 V6, and Dorado 6000 V6 Product Documentation**, or contact Huawei storage technical support to perform the configuration.

The configuration of data center A and data center B that needs to be performed before you configure and use the SRA includes creating LUNs, mapping LUNs to an ESXi host, and creating a HyperMetro pair or a HyperMetro consistency group. See **OceanStor S2600T&S5500T&S5600T&S5800T&S6800T Storage System V200R002C20 Product Documentation** or **OceanStor Dorado 3000 V6, Dorado 5000 V6, and Dorado 6000 V6 Product Documentation** and **OceanStor 5300 V3&5500 V3&5600 V3&5800 V3&6800 V3 Storage System V300R003 HyperMetro Feature Guide** or **OceanStor Dorado 5000 V6 6.0.0 HyperMetro Feature Guide**, or contact Huawei storage technical support to perform the configuration.

The SRA is designed for the service continuity plan and recovery plan of the SRM of VMware. The corresponding software environment must meet the requirements of the SRA.

Device Type	Requirements
VMware ESXi Server 6.0/6.5/6.7/7.0	VMware ESXi Servers are deployed at host cluster A and host cluster B.
VMware vCenter Server 6.0/6.5/6.7/7.0	VMware vSphere Servers are deployed at host cluster A and host cluster B.
VMware vSphere Web Client 6.0/6.5/6.7/7.0	VMware vSphere Web Clients are deployed at host cluster A and host cluster B.
VM	VM instances are deployed at host cluster A.
SRM Server Manager 6.5/8.1/8.2/8.3	SRM Server Managers are deployed on the VMware vSphere Servers at host cluster A and host cluster B.
Operating system	Photon OS; Windows Server 2016 or earlier (64-bit)

 Copyright © Huawei Technologies Co., Ltd.

3 Installing SRA

3.1 Installing SRA in a Windows Environment

3.2 Installing SRA in a Linux (SRM VA) Environment(Photon OS)

3.1 Installing SRA in a Windows Environment

Prerequisites

- SRM has been deployed at the production site and DR site.
- For the SRM installation and configuration, see *Site Recovery Manager Administration Guide*, which is available at the **VMware official website.**

Context

SRA must be installed at both the production site and DR site.

NOTE

- Currently, only the SRA installer of the English version is provided.
- SRA must be installed on the same server as SRM.
- SRA and SRM can be installed on the same server as vSphere Server or on a different server. If SRA and SRM are installed on a different server, the server must be connected to vSphere Server. In this example, SRA and SRM are installed on the same server as vSphere Server.

Procedure

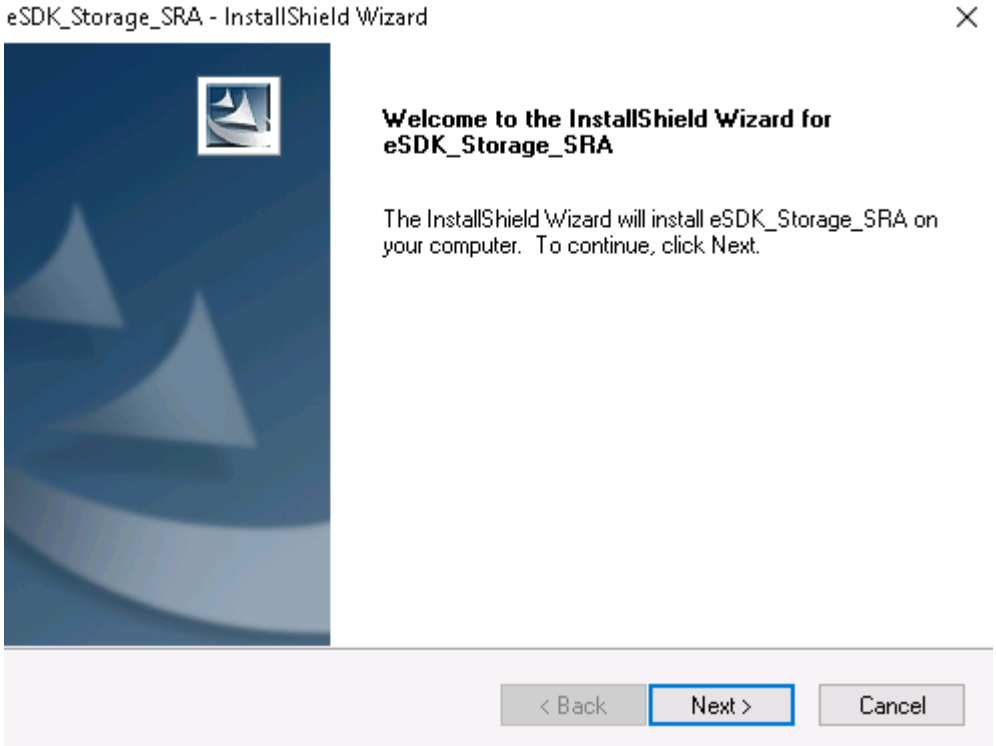
Step 1 Copy the SRA installation file to any directory (the directory name cannot contain Chinese characters) at the production site where SRM has been deployed. Double-click the **.exe** file.

The SRA installation wizard dialog box is displayed, as shown in **Figure 3-1**.

NOTE

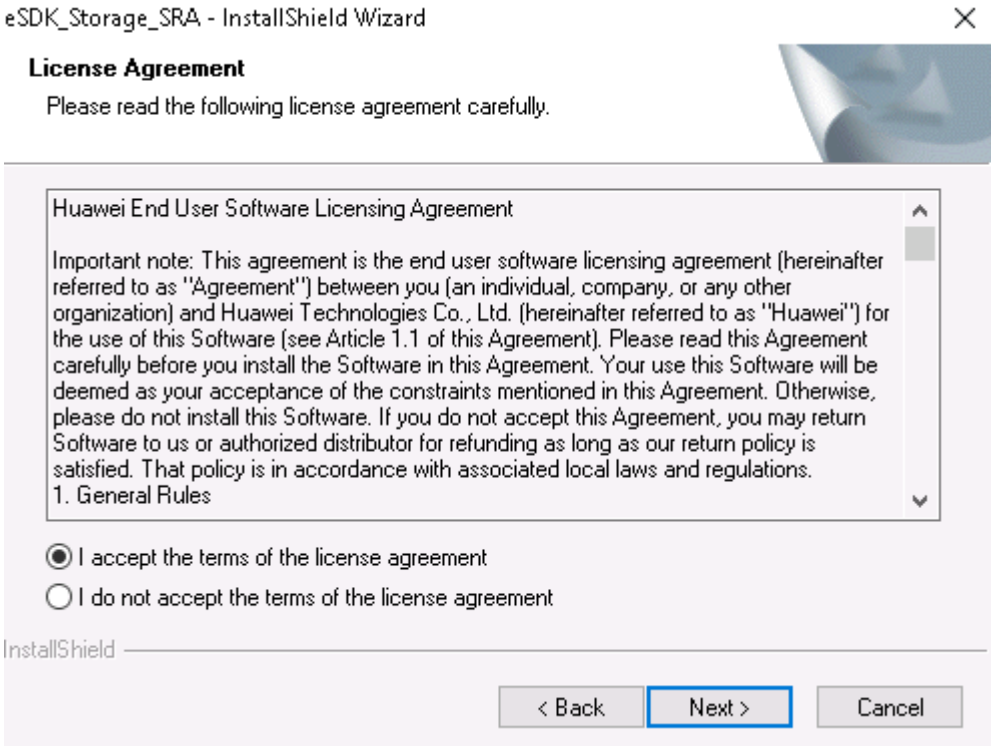
The SRA installation file name in a Windows environment is eSDK_Storage_*.*.**_SRA_Plugin_X.X.XX_Windows.exe. *X.X.XX* is the version number.

Figure 3-1 Installation wizard



Step 2 Click **Next**. Select **I accept the terms of the license agreement**, as shown in **Figure 3-2**.

Figure 3-2 License Agreement



Step 3 Click **Next**. Select a setup type according to the actual situation.

- If the storage array supports HyperMetro, select **support Stretched**.

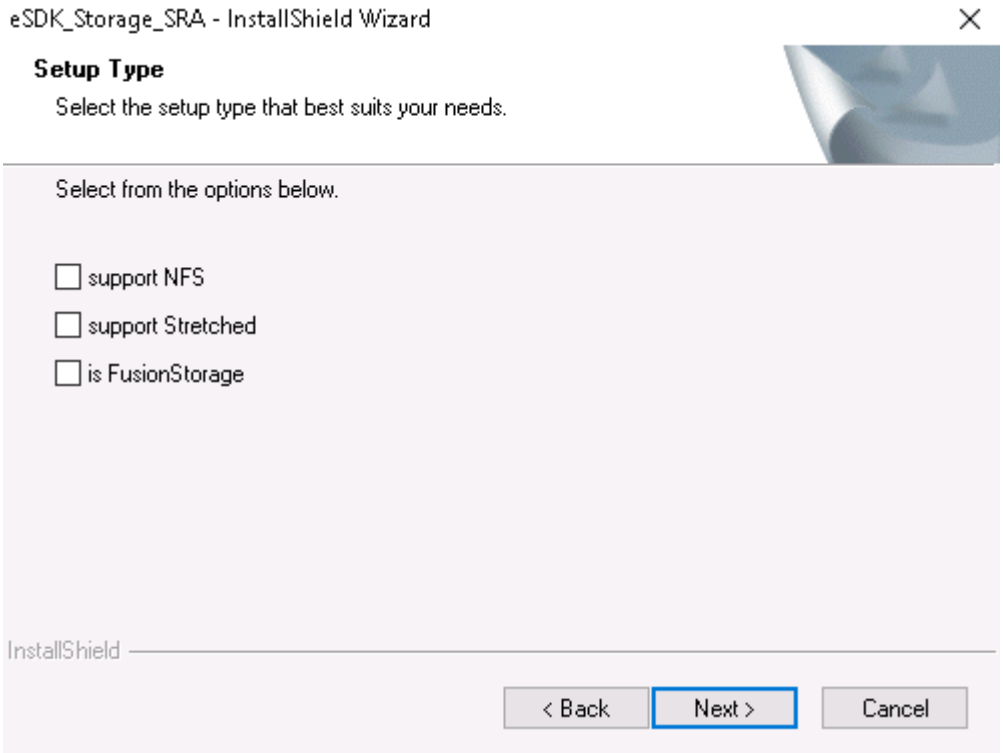
  Only SRM Server Manager 6.1/6.5/8.1/8.2 supports HyperMetro.
- If the storage array does not support HyperMetro, do not select **support Stretched.** Otherwise you will need to re-install the SRA.
- If the storage array supports file system clone, select **support NFS**.
- If FusionStorage is used, select **is FusionStorage**.

NOTICE

- Only V300R006C10SPC100 and later versions support the file system clone feature.
- Only FusionStorage 8.0 and later versions support the SRM DR feature.

- The same setup type must be set for the production site and DR site.

Figure 3-3 Setting a setup type



Step 4 Click **Next**.

The installation directory selection dialog box is displayed.

Step 5 Click **Next**.

The installation preparation dialog box is displayed.

Step 6 Click **Install**.

The installation starts.

Step 7 Click **Finish**.

The SRA software is successfully installed at the production site.

Step 8 Repeat **Step 1** to **Step 7** to install SRA at the DR site.

----End

3.2 Installing SRA in a Linux (SRM VA) Environment(Photon OS)

Prerequisites

- SRM VA has been deployed at the production site and DR site.
- For the SRM VA installation and configuration, see the VMware official website.

Procedure

Step 1 Log in to the SRM management GUI as user **admin**. The login address is **https://** *<SRM server IP address>***:5480**.

Step 2 Click **Storage Replicaiton Adapters**. The SRA plug-in management GUI is displayed.

Step 3 Click **NEW ADAPTER** to upload the SRA installation package.

NOTE

The name of the installation package is **eSDK_Storage_****.*.***_**SRA_Plugin**_*X.X.XX*_**Linux.tar.gz**, where *X.X.XX* indicates the version number.

----End

4 Typical Scenario Configuration

4.1 SAN Active/Standby Scenario
4.2 SAN HyperMetro Scenario
4.3 NAS Active/Standby Scenario
4.4 Geo-redundant DR Scenario
4.5 Common Configuration Operations

4.1 SAN Active/Standby Scenario

Scenario Identification

In a SAN active/standby scenario, SRM is used to manage VMs residing on the replication LUN.

Prerequisites

- The SRA has been installed on the protected site and recovery site.
- LUNs and a remote replication pair (or a consistency group) have been created on the storage arrays at the protected site and the recovery site.
- LUNs have been mapped to ESXi Hosts at the protected site.

Configuration Process

Step 1 Use LUNs to create a VMFS-based datastore at the protected site. For details, see **4.5.1 Creating a Datastore (VMFS)**.

Step 2 Create a VM at the protected site. For details, see **4.5.3 Creating VMs**.

Step 3 Set up a connection between the vCenter servers at the protected site and recovery site. For details, see **4.5.8 Setting Up a Connection Between the vCenter Servers at the Protected Site and Recovery Site**.

Step 4 Configure mappings between the vCenter servers at the protected site and recovery site. For details, see **4.5.9 Configuring Mapping Between the vCenter Servers at the Protected Site and Recovery Site**.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Create and configure placeholder storage at the protected site and recovery site. For details, see **4.5.10 Creating and Configuring Placeholder Storage**.

Step 6 Add an array manager. For details, see **4.5.11 Adding Array Managers**.

Step 7 Create a dabastore-based protection group. For details, see **4.5.12 Creating a Datastore-Based Protection Group**.

Step 8 Create a recovery plan based on the VM protection group. For details, see **4.5.14 Creating a Recovery Plan (Based on VM Protection Groups)**.

----End

4.2 SAN HyperMetro Scenario

Scenario Identification

In a SAN HyperMetro scenario, SRM Stretch is used to perform DR management on VMs that reside on HyperMetro LUNs.

Prerequisites

- The SRA that supports Stretch has been installed on the protected site and recovery site.
- Storage arrays at the protected site and recovery site support the SAN HyperMetro feature.
- LUNs and a HypermMetro pair (or a consistency group) have been created on the storage arrays at the protected site and the recovery site, and are mapped to ESXi hosts.
- If vSphere 7.0 is used, configure vCenter Enhanced Linked Mode for vCenter Server appliances to support vMotion live migration for Stretch. For details, see **https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-4394EA1C-0800-4A6A-ADBF-D35C41868C53.html**.

NOTICE

If the arbitration service is required, install and configure the quorum server.For details about how to configure HyperMetro, see the ***OceanStor 5300 V3&5500 V3&5600 V3&5800 V3&6800 V3 Storage System V300R003 HyperMetro Feature Guide*** *or* **OceanStor Dorado 5000 V6 6.0.0 HyperMetro Feature Guide**.

Configuration Process

Step 1 Use LUNs to create a VMFS-based datastore at the protected site. For details, see **4.5.1 Creating a Datastore (VMFS)**.

Step 2 Create a VM at the protected site. For details, see **4.5.3 Creating VMs**.

Step 3 Create a tag at the protected site. For details, see **5.4.4-Creating a Tag**.

Step 4 Assign the tag to the datastore. For details, see **5.4.5-Assigning the Tag to the Created Data Store**.

Step 5 Create VM storage policies with the same name at the protected site and recovery site, respectively. For details, see **5.4.6-Creating a VM Storage Policy**.

Step 6 Allocate the storage policy to VMs at the protected site. For details, see **5.4.7-Applying the VM Storage Policy to VMs**.

Step 7 Set up a connection between the vCenter servers at the protected site and recovery site. For details, see **5.4.8-Setting Up a Connection Between the vCenter Servers at the Protected Site and Recovery Site**.

Step 8 Configure mappings between the vCenter servers at the protected site and recovery site. For details, see **5.4.9-Configuring Mapping Between the vCenter Servers at the Protected Site and Recovery Site**.

Step 9 Create and configure placeholder storage at the protected site and recovery site. For details, see **4.5.10 Creating and Configuring Placeholder Storage**.

Step 10 Add an array manager. For details, see **4.5.11 Adding Array Managers**.

Step 11 Create a dabastore-based protection group. For details, see **4.5.13 Creating a Policy-Based Protection Group**.

Step 12 Create a recovery plan based on the VM protection group. For details, see **4.5.15 Creating a Recovery Plan (Based on a Storage Policy for a Protection Group)**.

----End

4.3 NAS Active/Standby Scenario

Scenario Identification

In a NAS HyperMetro scenario, SRM is used to perform DR management on VMs that reside on HyperMetro LUNs.

Prerequisites

- The SRA that supports NFS has been installed on the protected site and recovery site.
- Storage arrays at the protected site and recovery site support the file system clone feature.
- File systems and the replication pair have been created on the storage arrays at the protected site and recovery site, and the NFS V3 service has been enabled.
- NFS shares of the file system have been created at the protected site and the ESXi host has been added to the NFS share client.
- ESXi hosts can access the IP address of all logical ports on the storage arrays at the production site and recovery site.

Configuration Process

Step 1 Use the file system to create an NFS-based datastore at the protected site. For details, see **4.5.2 Creating a Datastore (NFS)**.

Step 2 Create a VM at the protected site. For details, see **4.5.3 Creating VMs**.

Step 3 Set up a connection between the vCenter servers at the protected site and recovery site. For details, see **4.5.8 Setting Up a Connection Between the vCenter Servers at the Protected Site and Recovery Site**.

Step 4 Configure mappings between the vCenter servers at the protected site and recovery site. For details, see **4.5.9 Configuring Mapping Between the vCenter Servers at the Protected Site and Recovery Site**.

Step 5 Create and configure placeholder storage at the protected site and recovery site. For details, see **4.5.10 Creating and Configuring Placeholder Storage**.

Step 6 Add an array manager. For details, see **4.5.11 Adding Array Managers**.

Step 7 Create a dabastore-based protection group. For details, see **4.5.12 Creating a Datastore-Based Protection Group**.

Step 8 Create a recovery plan based on the VM protection group. For details, see **4.5.14 Creating a Recovery Plan (Based on VM Protection Groups)**.

----End

4.4 Geo-redundant DR Scenario

Scenario Identification

For details about geo-redundant DR, see **2.2.3 Geo-redundant DR**. In a geo-redundant DR scenario, SRM is used to manage VMs residing on data center B and data center C.

Prerequisites

- The SRA has been installed on host cluster A and host cluster B.
- A HyperMetro pair or consistency group has been created between data center A and data center B, and a replication pair or consistency group has been created between data center B and data center C.
- LUNs created on storage arrays at data center A and data center B have been mapped to ESXi hosts at host cluster A, and LUNs created on storage arrays at data center C have been mapped to ESXi hosts at host cluster B.

Configuration Process

Step 1 Use LUNs to create a VMFS-based datastore at the host cluster A. For details, see **4.5.1 Creating a Datastore (VMFS)**.

Step 2 Create a VM at host cluster A. For details, see **4.5.3 Creating VMs**.

Step 3 Set up a connection between the vCenter servers at host cluster A and host cluster B. For details, see **4.5.8 Setting Up a Connection Between the vCenter Servers at the Protected Site and Recovery Site**.

Step 4 Configure mappings between the vCenter servers host cluster A and host cluster B. For details, see **4.5.9 Configuring Mapping Between the vCenter Servers at the Protected Site and Recovery Site**.

Step 5 Create and configure placeholder storage at host cluster A and host cluster B. For details, see **4.5.10 Creating and Configuring Placeholder Storage**.

Step 6 Add an array manager. For details, see **4.5.11 Adding Array Managers**.

Step 7 Create a dabastore-based protection group. For details, see **4.5.12 Creating a Datastore-Based Protection Group**.

Step 8 Create a dabastore-based protection group. For details, see **4.5.14 Creating a Recovery Plan (Based on VM Protection Groups)**.

----End

4.5 Common Configuration Operations

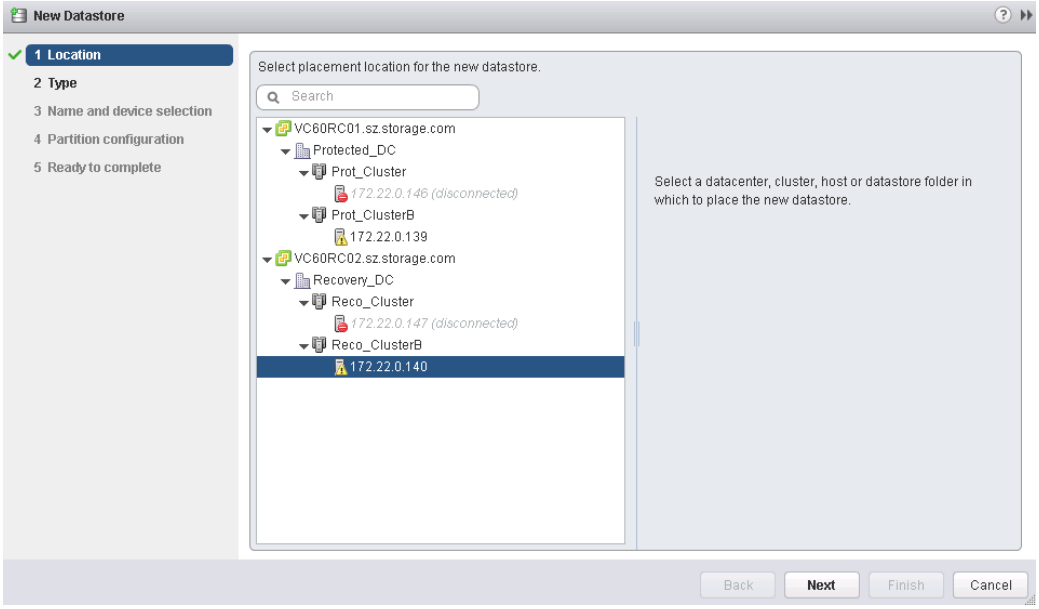
4.5.1 Creating a Datastore (VMFS)

Step 1 Log in to the VMware vSphere Web Client at the protected site.

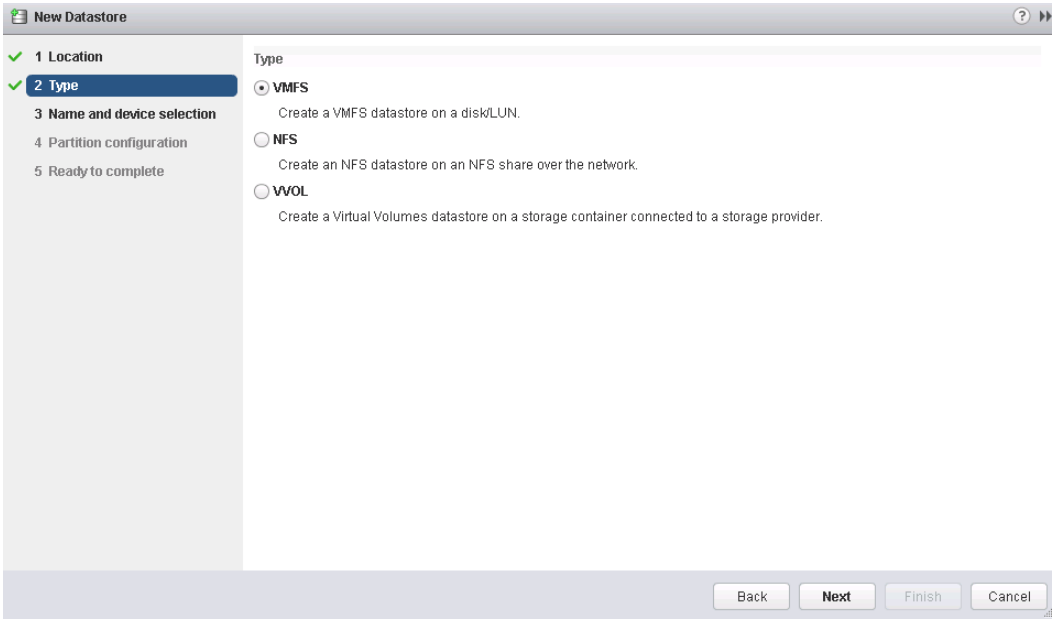
Step 2 Choose v**Center Inventory Lists** > **Datastores**.

Step 3 Click to create a data store.

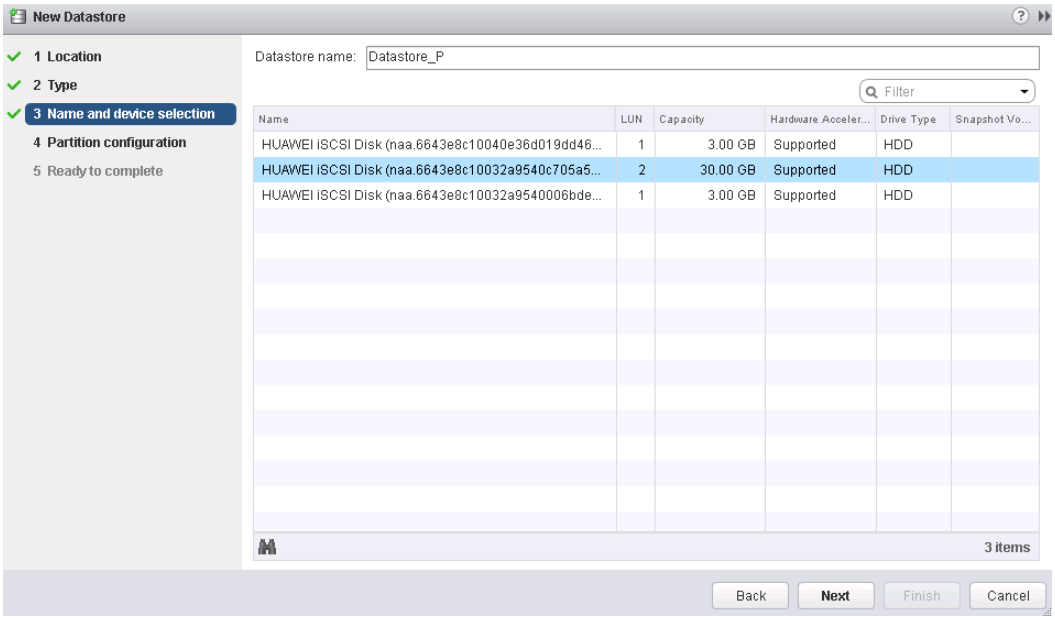
Step 4 Select the host of the protected site and click **Next**.



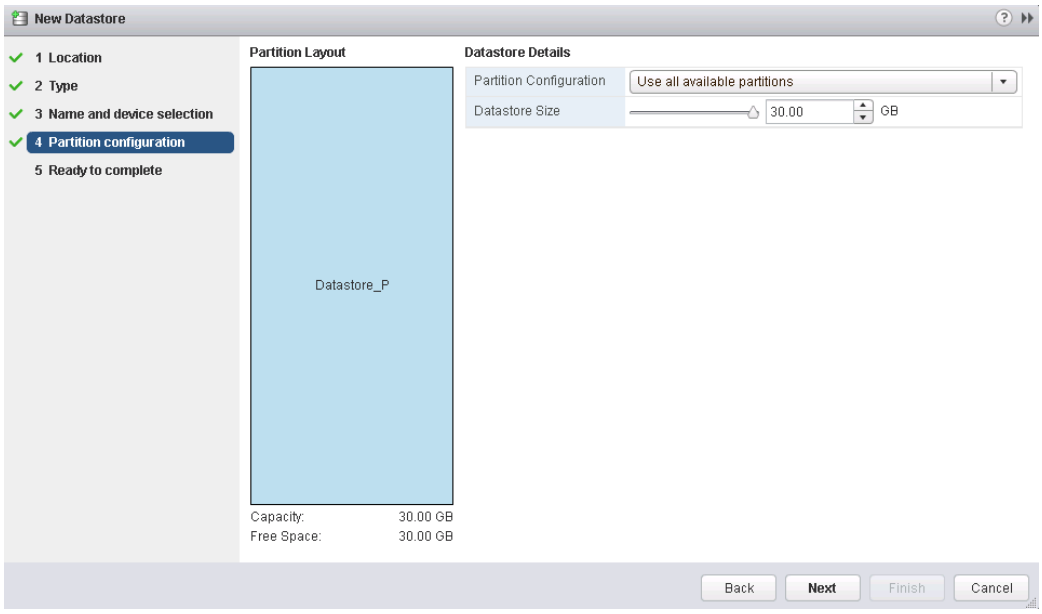
Step 5 Click **VMFS** and then **Next**.



Step 6 Set the data store name, select a LUN, and click **Next**.



Step 7 Select **Use all available partitions** from the **Partition Configuration** drop-down list box.



Step 8 Click **Finish**.

----End

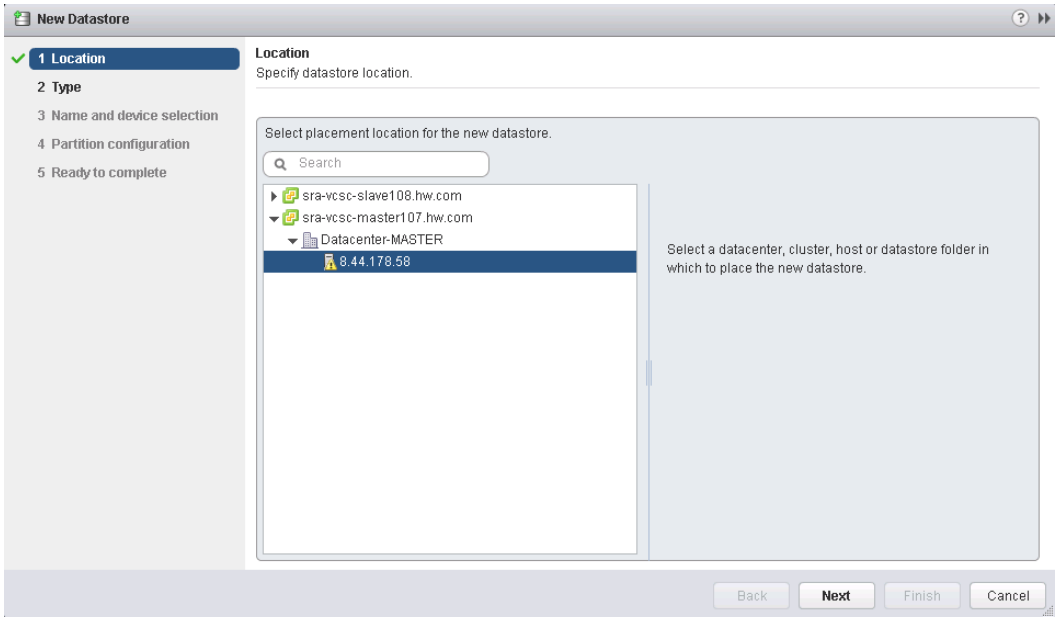
4.5.2 Creating a Datastore (NFS)

Step 1 Log in to the VMware vSphere Web Client.

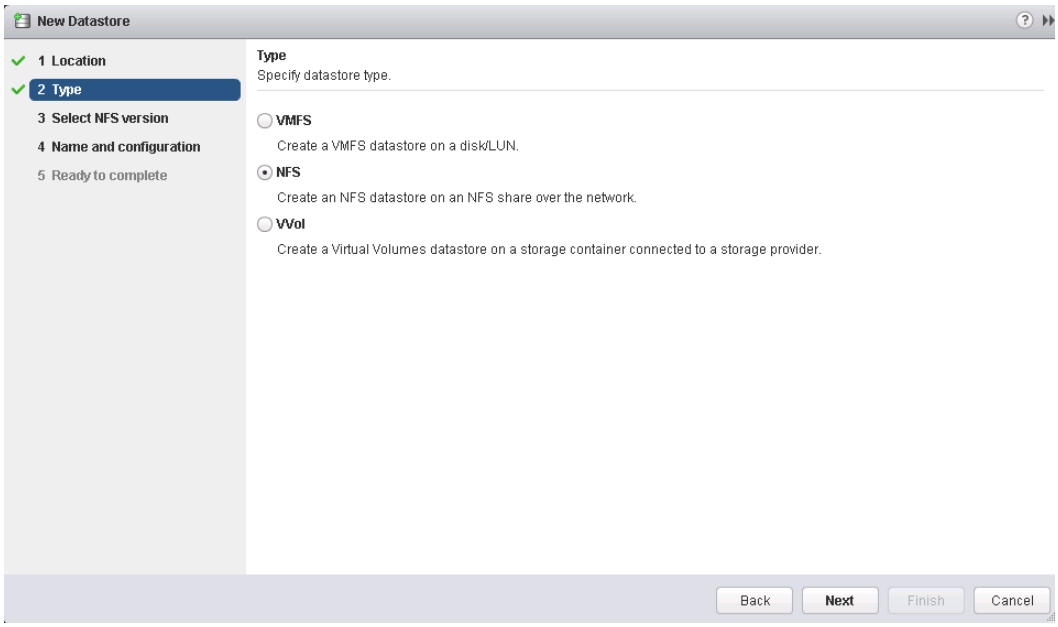
Step 2 Choose v**Center Inventory Lists** > **Datastores**.

Step 3 Click to create a data store.

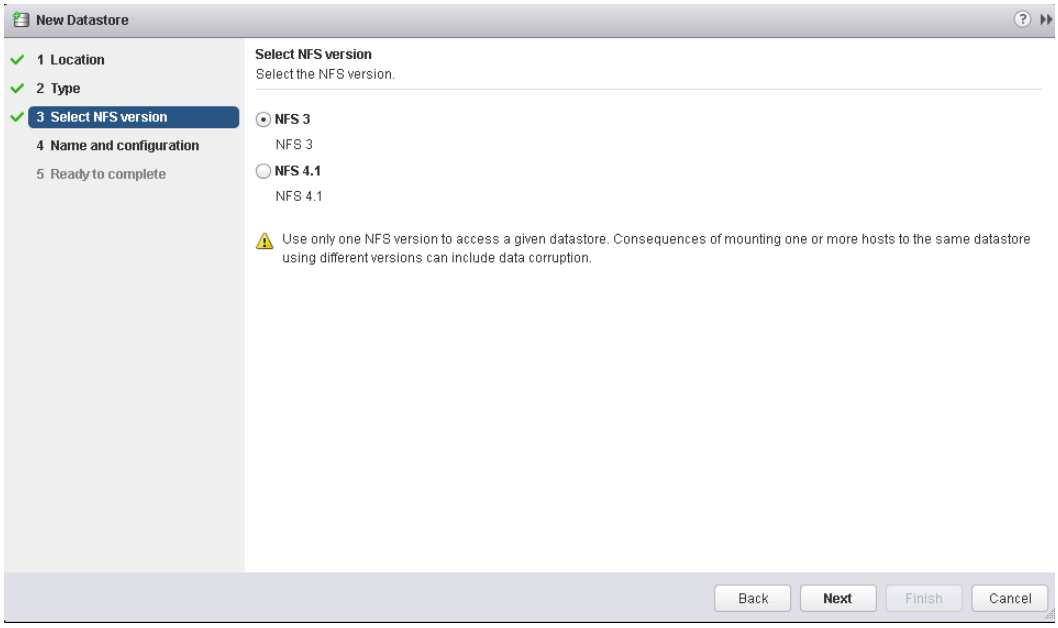
Step 4 Select the host of the protected site and click **Next**.



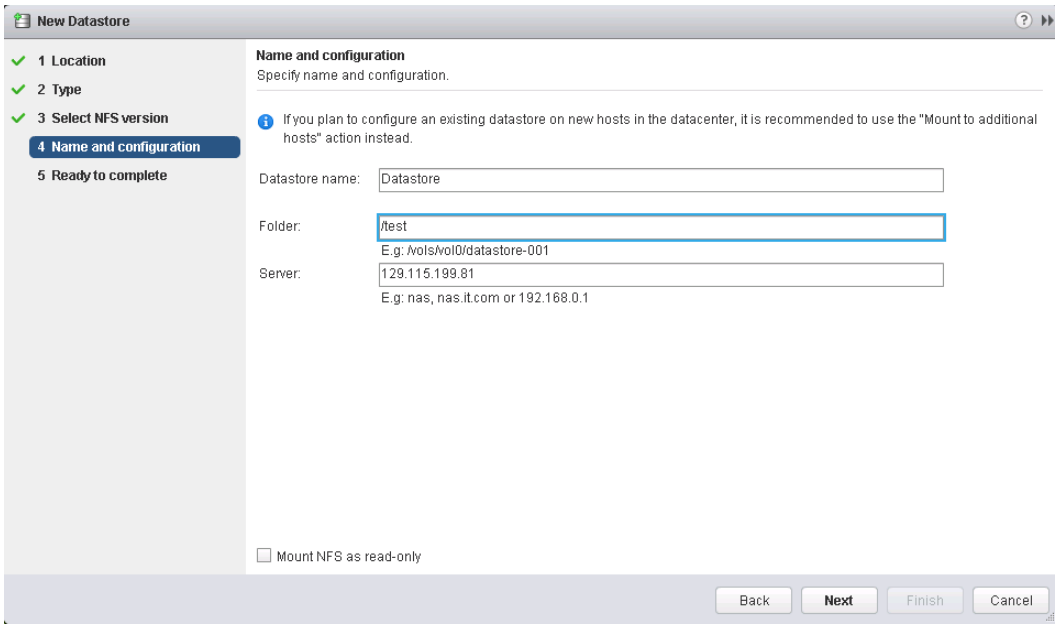
Step 5 Select **NFS** and then click **Next**.



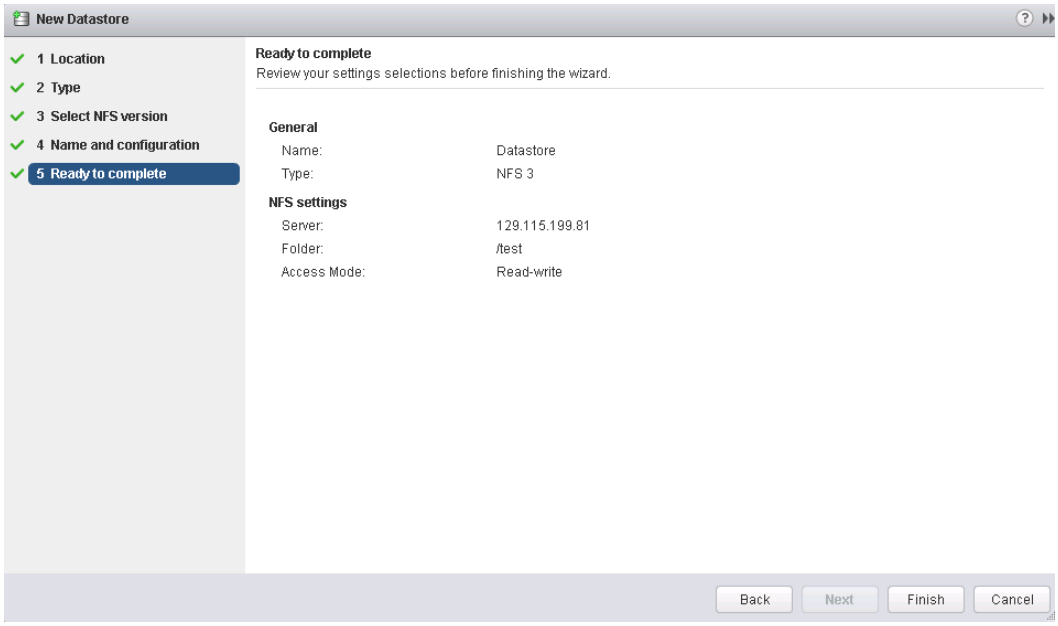
Step 6 Select **NFS 3** and click **Next**.



Step 7 Set the name of the datastore, enter the NFS share name and the IP address for mounting the NFS share, and click **Next**.



Step 8 Click **Finish**.



----End

4.5.3 Creating VMs

Step 1 Log in to the VMware vSphere Web Client at the protected site and choose **Hosts and Clusters**.

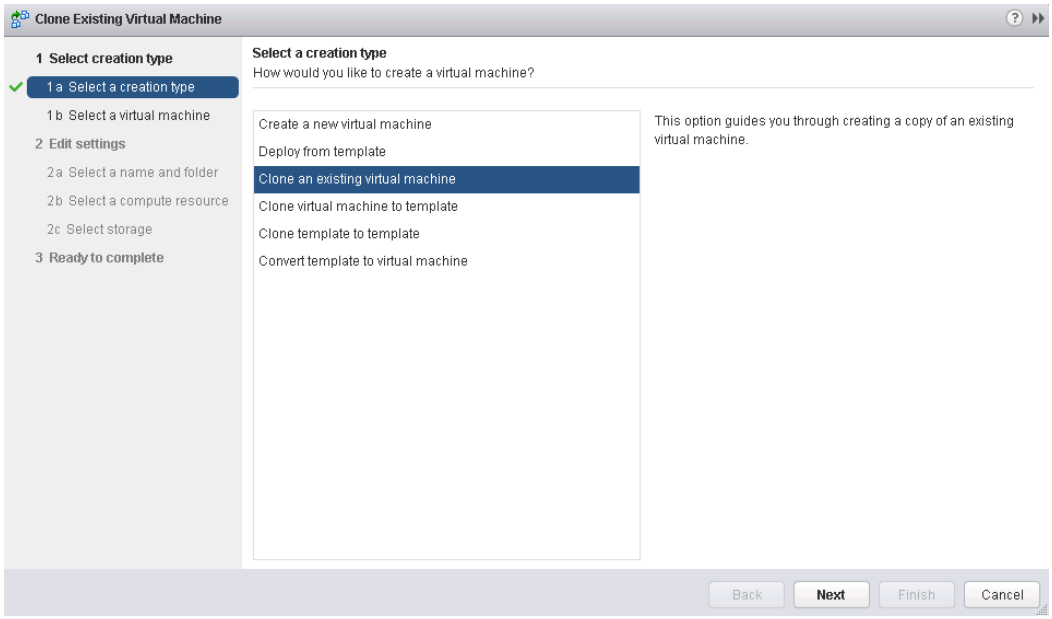
Step 2 Select the host of the protected site.

Step 3 Click to create a VM.

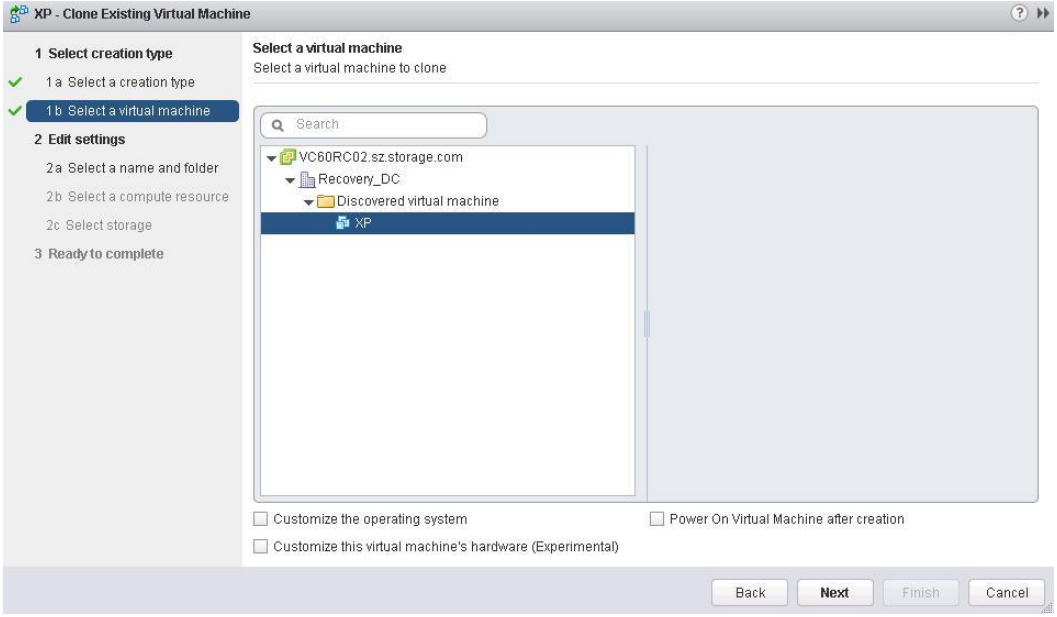
NOTE

A VM can be created in several ways. This section describes how to create a VM by cloning an existing VM.

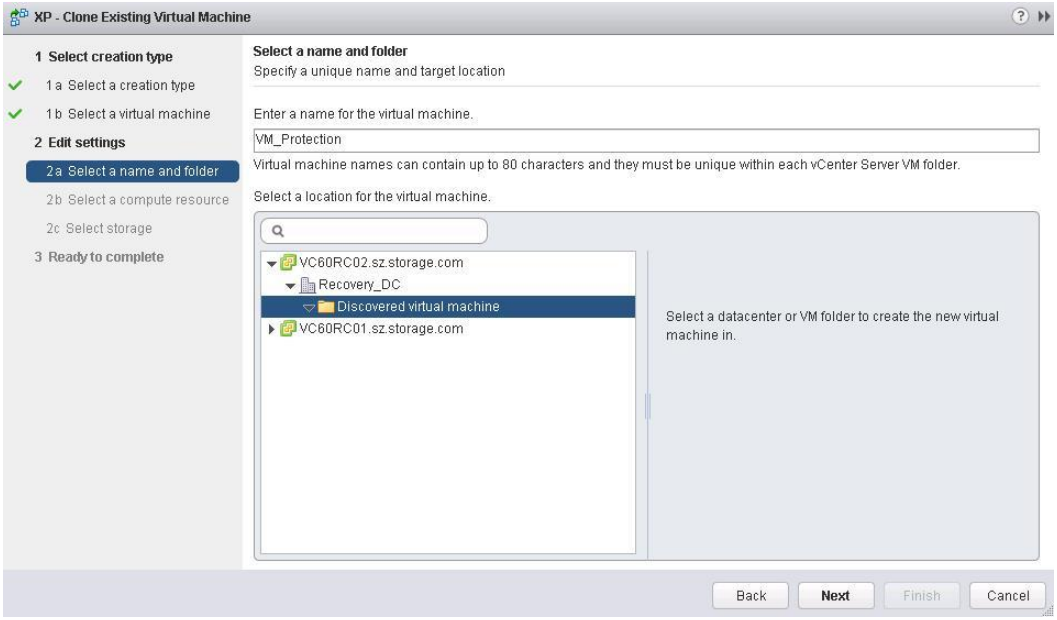
Step 4 Choose **1a Select a creation type** from the navigation tree and click **Clone an existing virtual machine**.



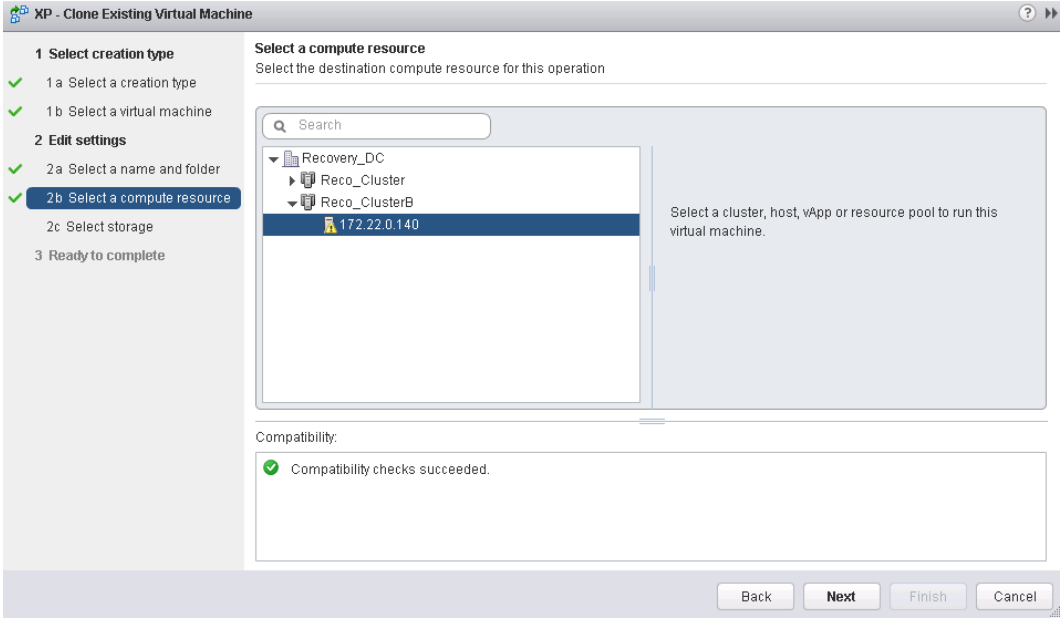
Step 5 Select the VM to be cloned and click **Next**.



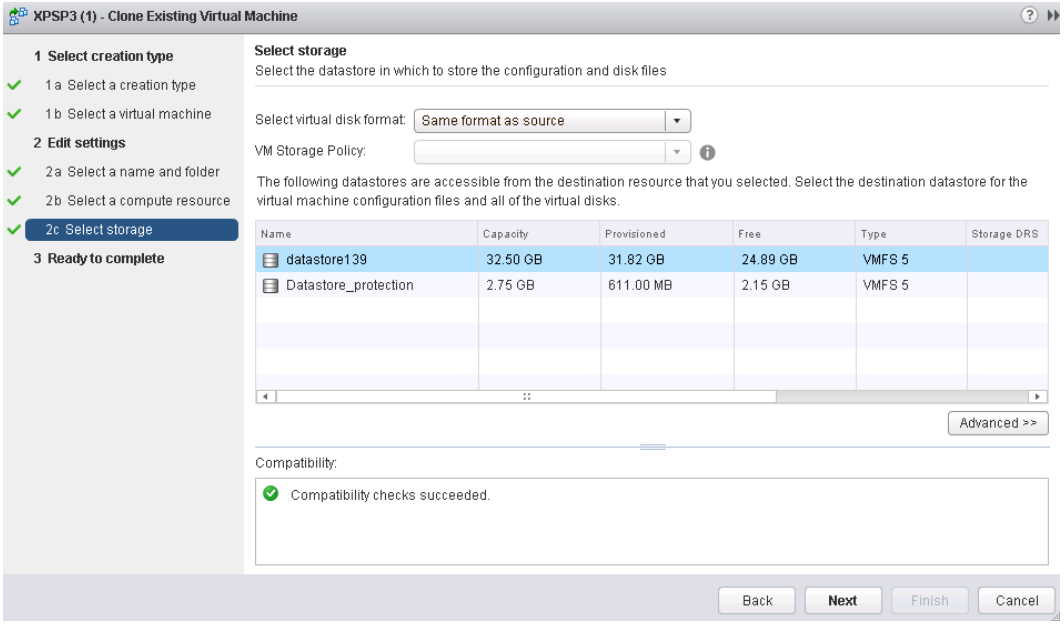
Step 6 Enter the VM name, select the **Discovered virtual machine** folder of the protected site, and click **Next**.



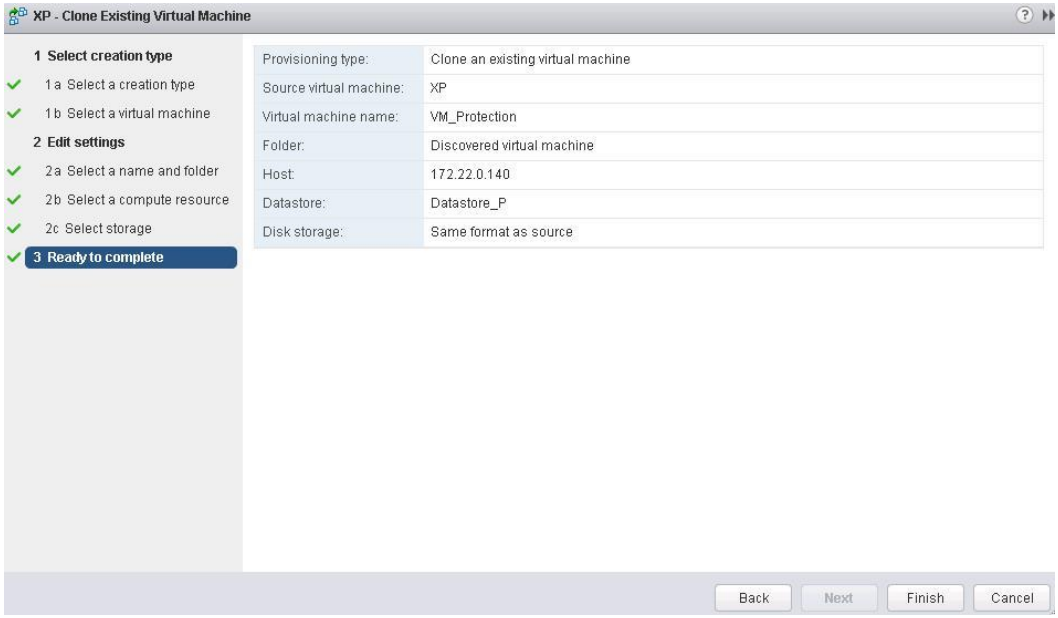
Step 7 Select the host of the protected site and click **Next**.



Step 8 Select the created data store and click **Next**.



Step 9 Click **Finish**.



Step 10 Create other VMs in the same way.

----End

4.5.4 Creating a Tag

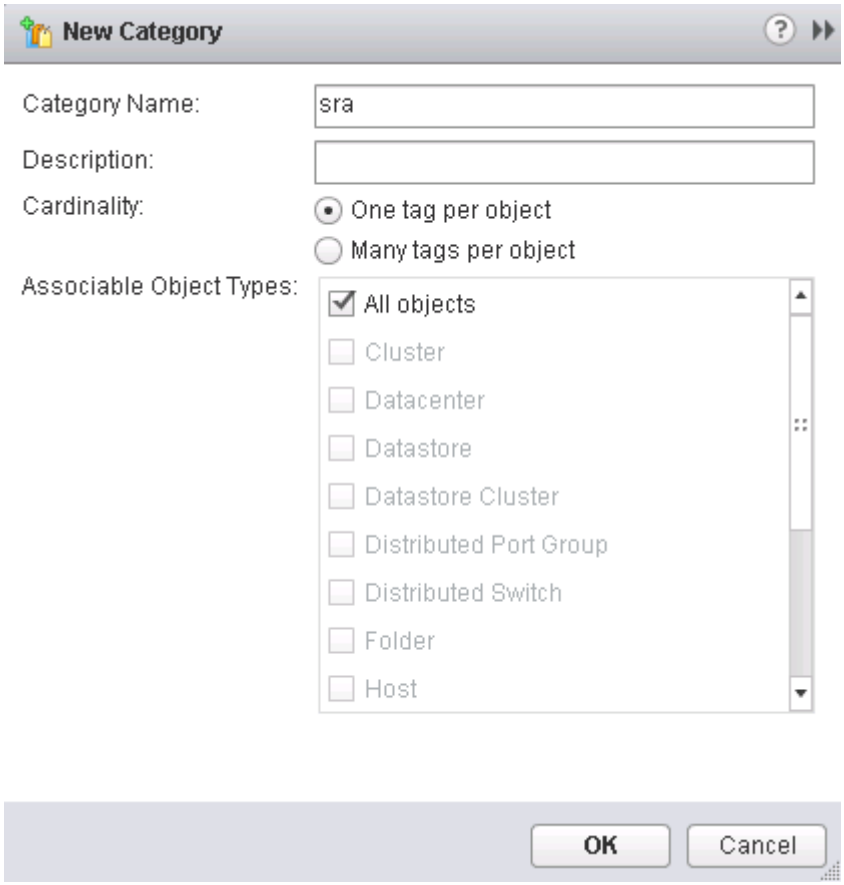
NOTE

A tag needs to be created only in the HyperMetro solution. The protected site and recovery site use the same tag.

Step 1 Log in to the VMware vSphere Web Client at the protected site and click Tags.

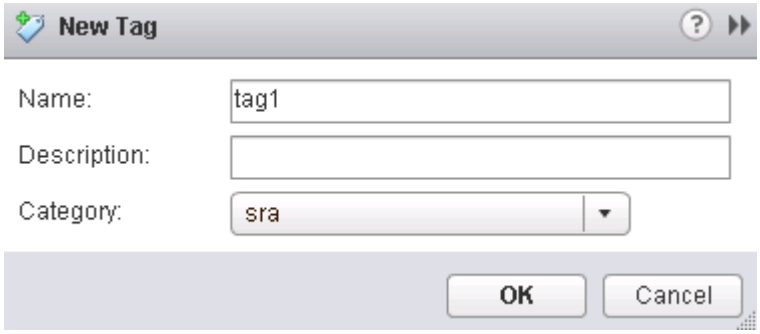
Step 2 Click to create a category.

Step 3 Set the category name and click **OK**.



Step 4 Click to create a tag.

Step 5 Set the tag name, select the created category, and click **OK**.



----End

4.5.5 Assigning the Tag to the Created Data Store

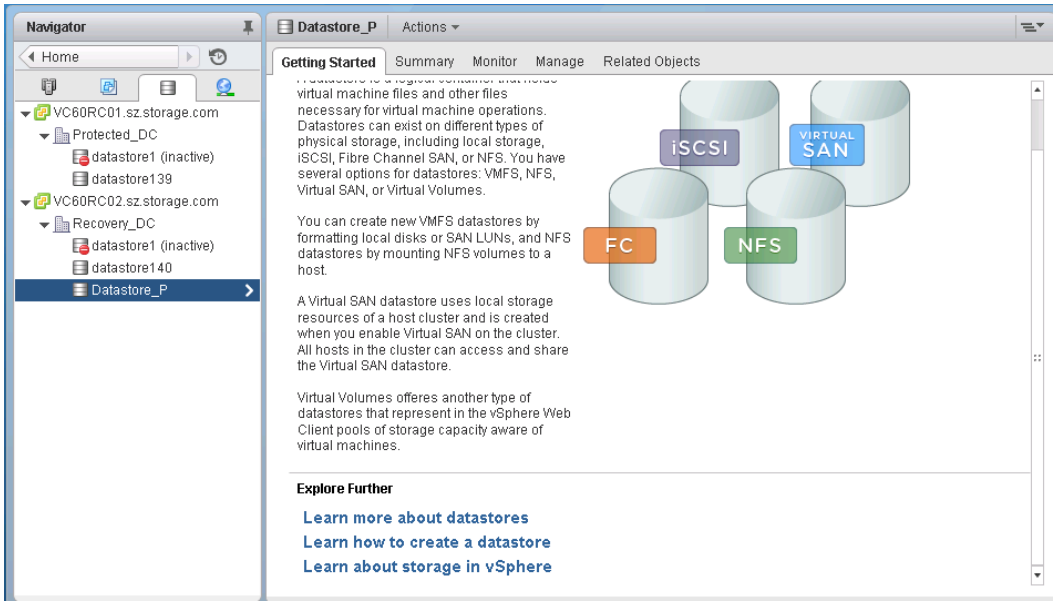
NOTE

The tag needs to be assigned to the created data store only in the HyperMetro solution. The protected site and recovery site use the same tag.

Step 1 Log in to the VMware vSphere Web Client at the protected site and choose **Hosts and Clusters**.

Step 2 Click .

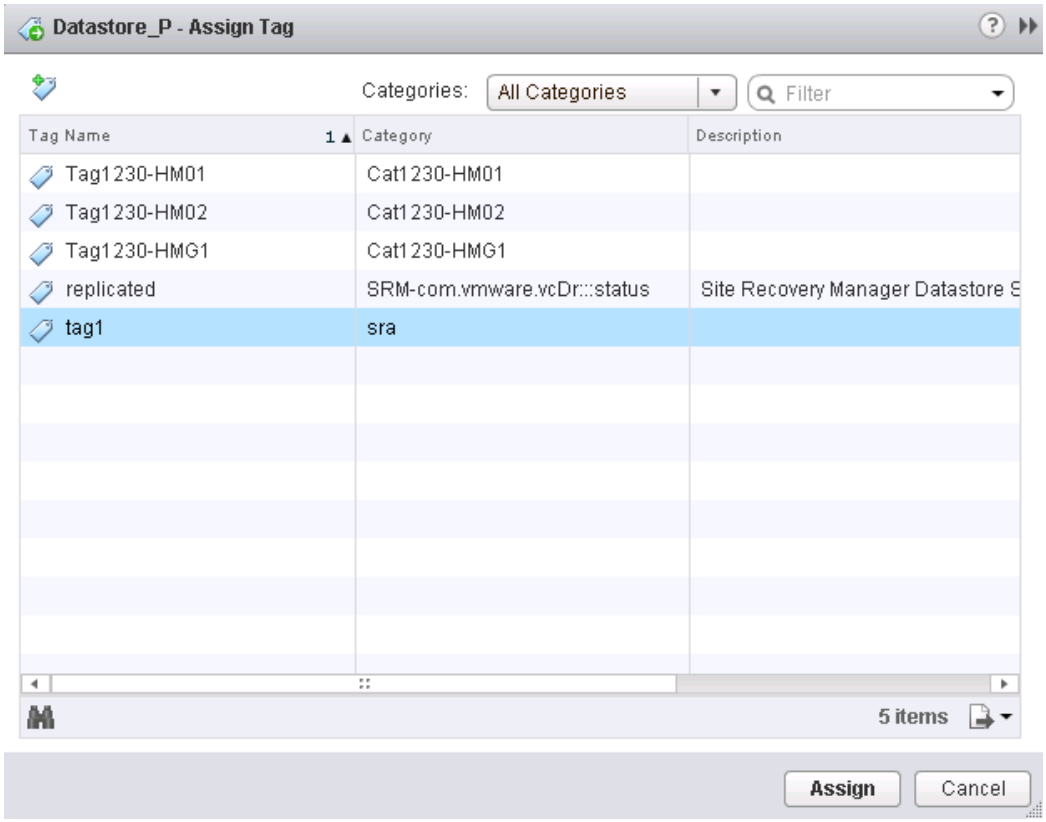
Step 3 Select the created data store.



Step 4 Choose **Manage** > **Tags**.

Step 5 Click.

Step 6 Select the created tag and click **Assign**.



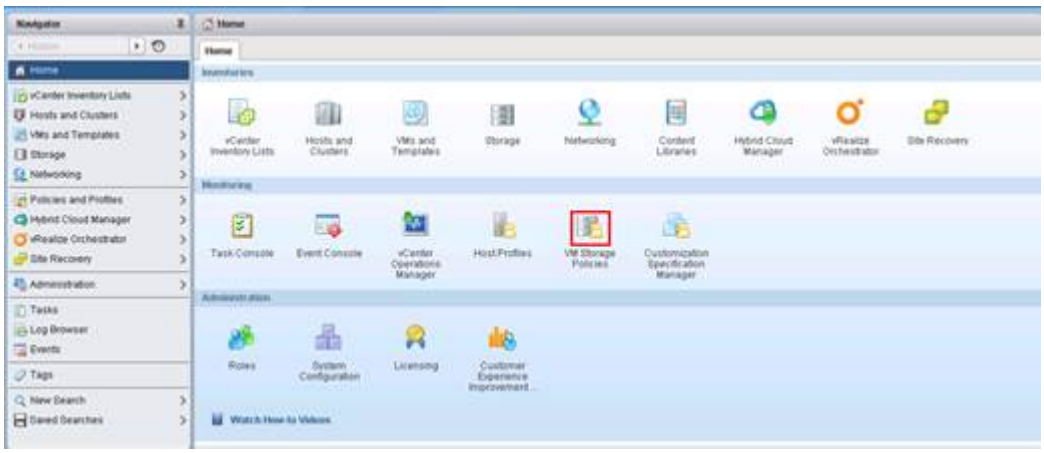
----End

4.5.6 Creating a VM Storage Policy

NOTE

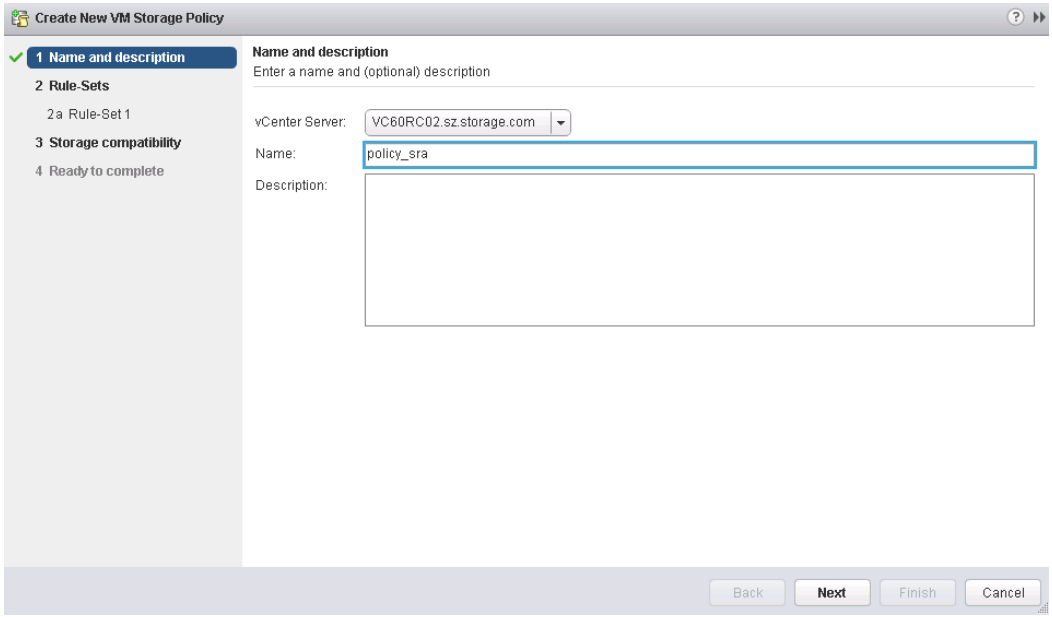
- A VM storage policy needs to be created only in the HyperMetro solution.
- The same VM storage policy must be created at both the protected site and recovery site.

Step 1 Log in to the VMware vSphere Web Client at the protected site and click **VM Storage Policies**.



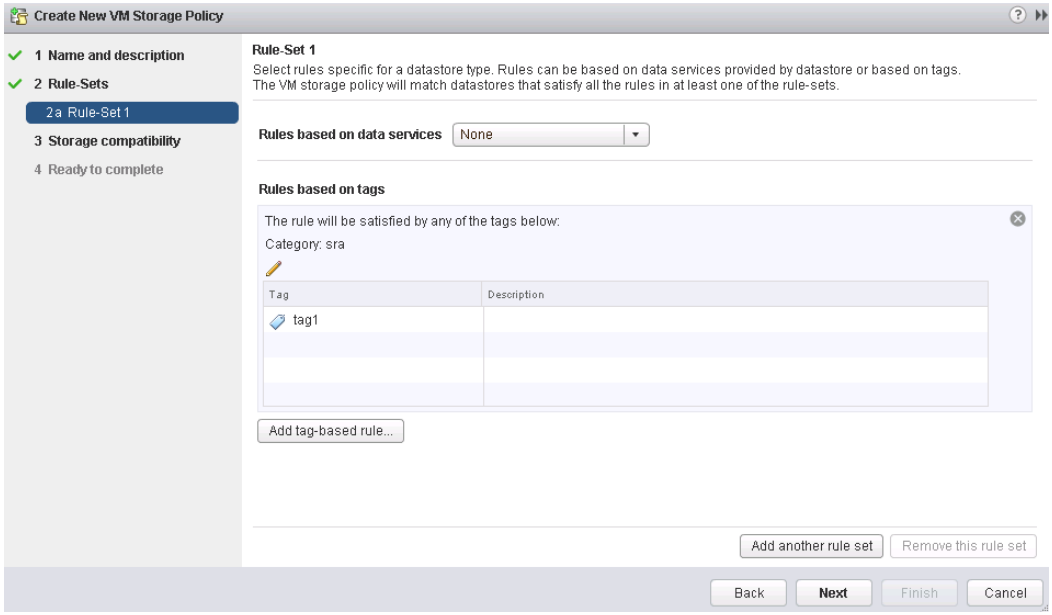
Step 2 Click to create a VM storage policy.

Step 3 Select the vCenter Server, set the VM storage policy name, and click **Next**.



Step 4 Click **Next**.

Step 5 Click **Add tag-based rule** and select the created tag.



Step 6 Always click **Next** on the displayed pages.

Step 7 Repeat steps 1 to 6 to create the same VM storage policy at the recovery site.

----End

4.5.7 Applying the VM Storage Policy to VMs

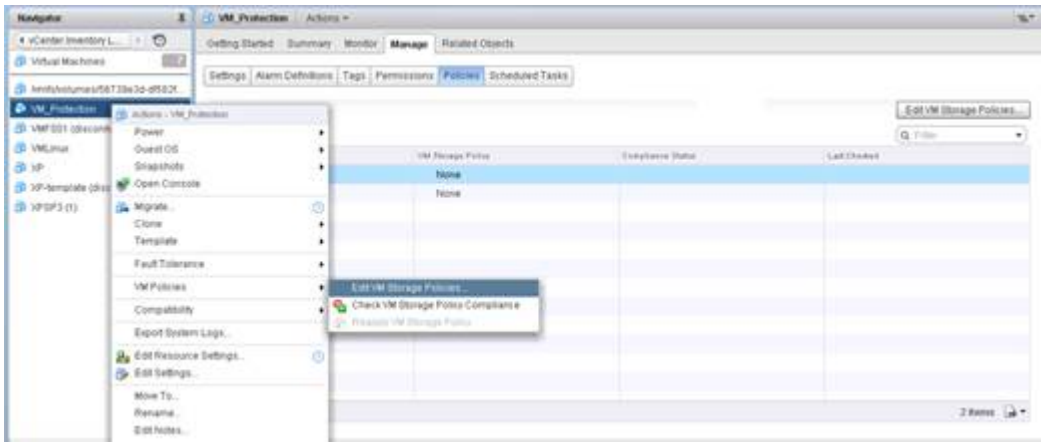
NOTE

- The VM storage policy needs to be applied to VMs only in the HyperMetro solution.
- Applying the VM storage policy to VMs needs to be performed only at the protected site.

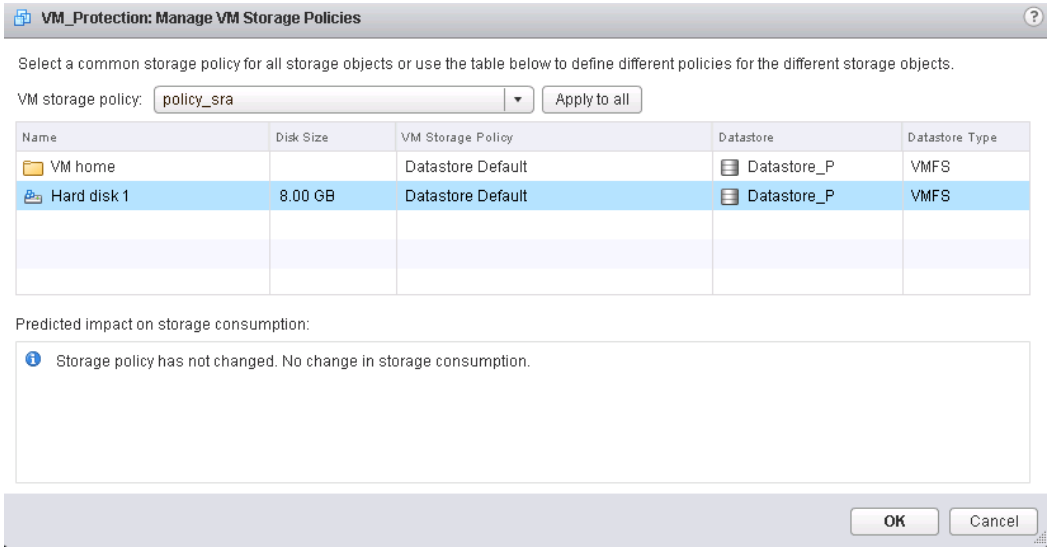
Step 1 Log in to the VMware vSphere Web Client at the protected site.

Step 2 Choose **vCenter Inventory Lists** > **Virtual Machines**.

Step 3 Right-click a VM and choose **VM Policies** > **Edit VM Storage Policies** from the shortcut menu.



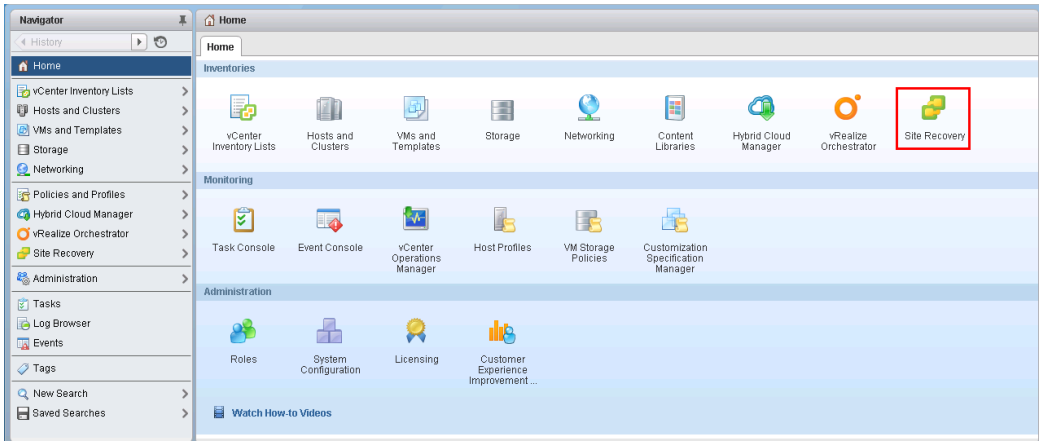
Step 4 Select the created VM storage policy from the **VM storage policy** drop-down list box, click **Apply to all**, and click **OK**.



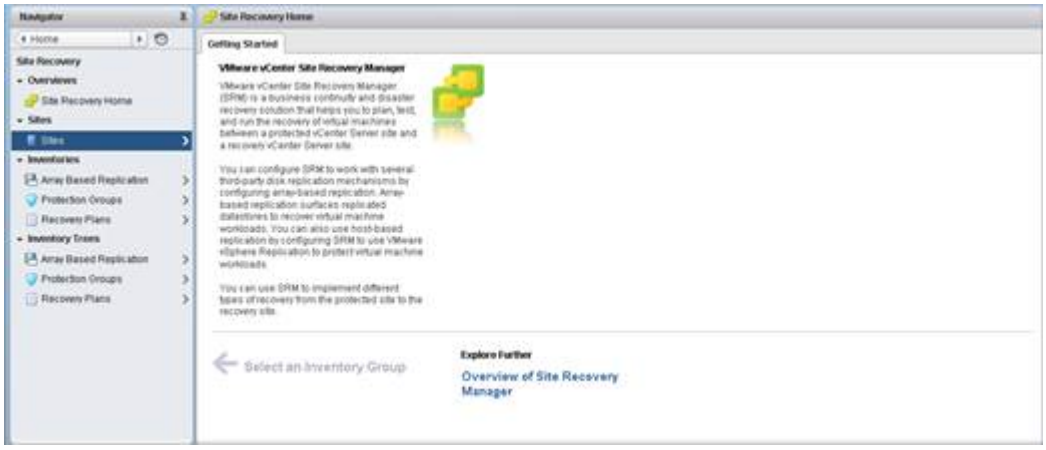
----End

4.5.8 Setting Up a Connection Between the vCenter Servers at the Protected Site and Recovery Site

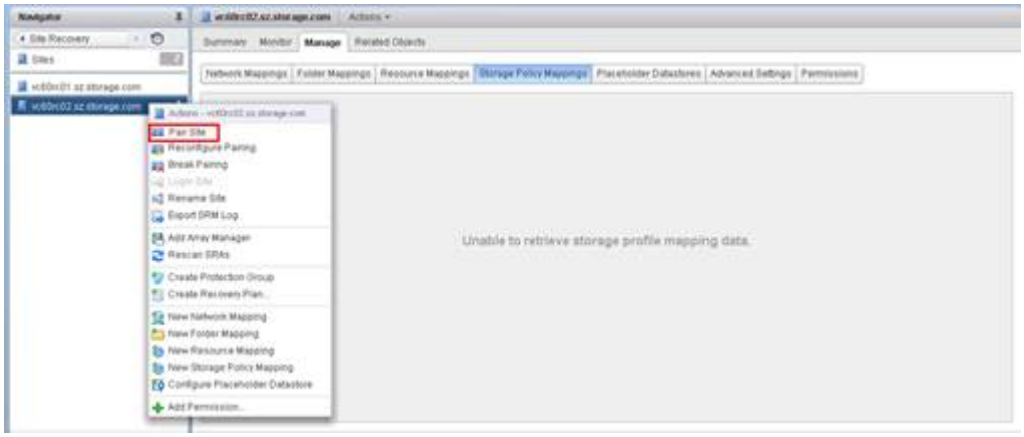
Step 1 Log in to the VMware vSphere Web Client at the protected site and click **Site Recovery**.



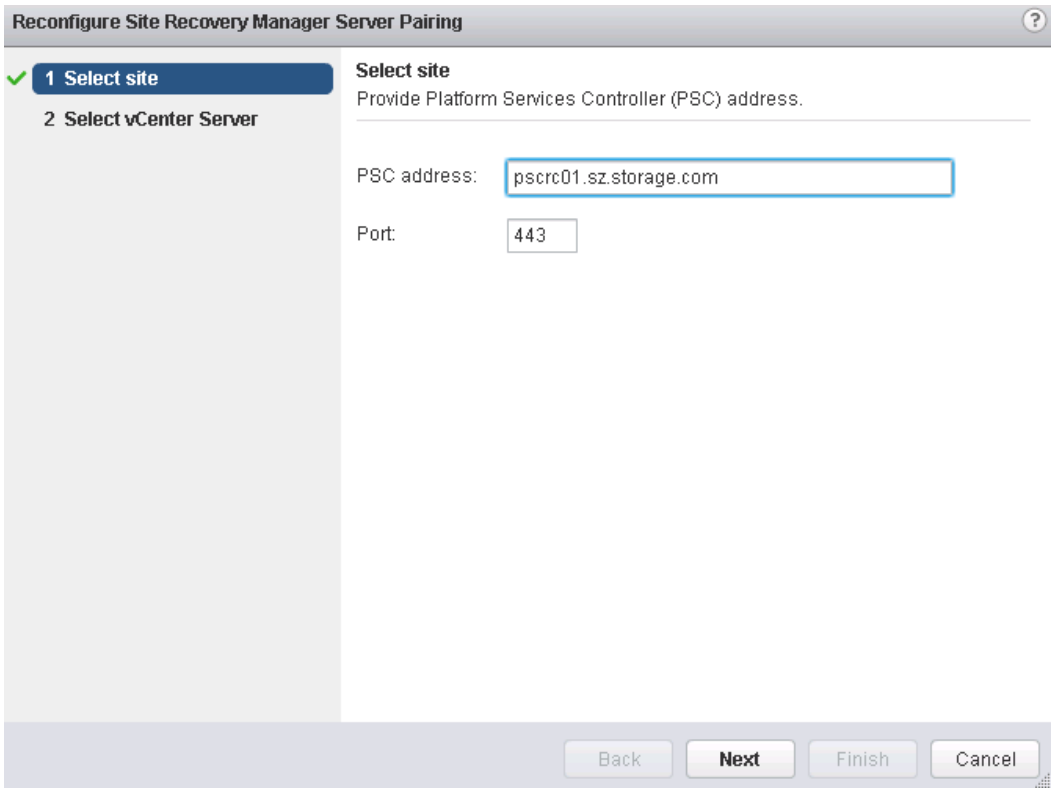
Step 2 Choose **Sites**.



Step 3 Right-click the protected site and choose **Pair Site** from the shortcut menu.



Step 4 Enter the address and port ID of the Platform Services Controller and click **Next**.



Step 5 Select the vCenter Server at the recovery site, enter the name and password of the vCenter Server, and click **Next**.

Step 6 Click **Finish**.

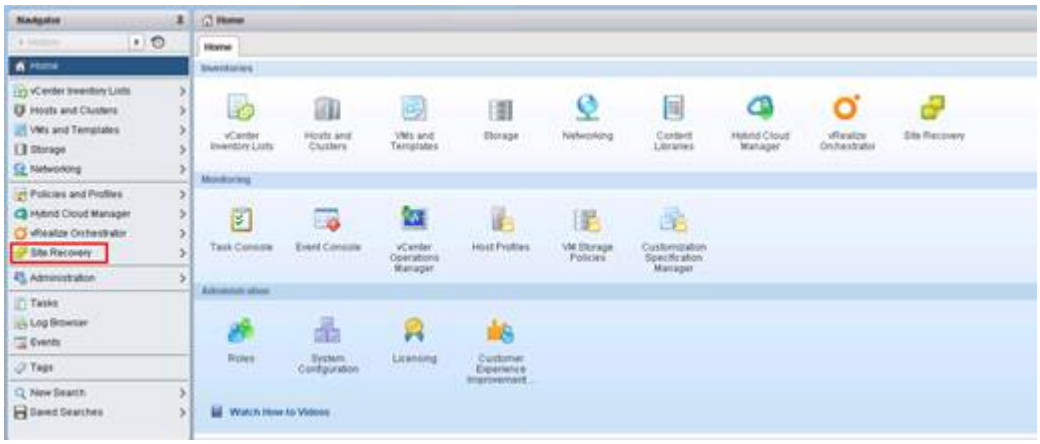
So far, the connection between the vCenter Servers at the protected site and recovery site has been set up.

----End

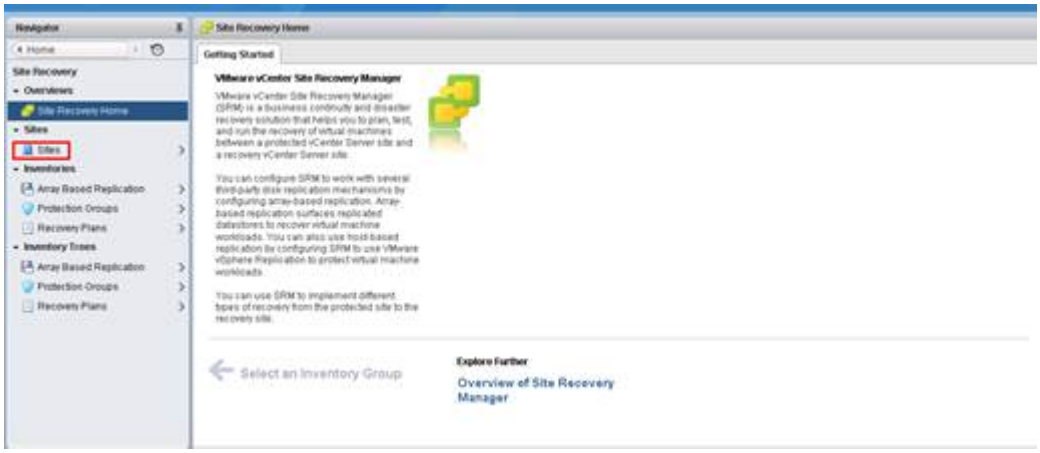
4.5.9 Configuring Mapping Between the vCenter Servers at the Protected Site and Recovery Site

Step 1 Log in to the VMware vSphere Web Client at the protected site.

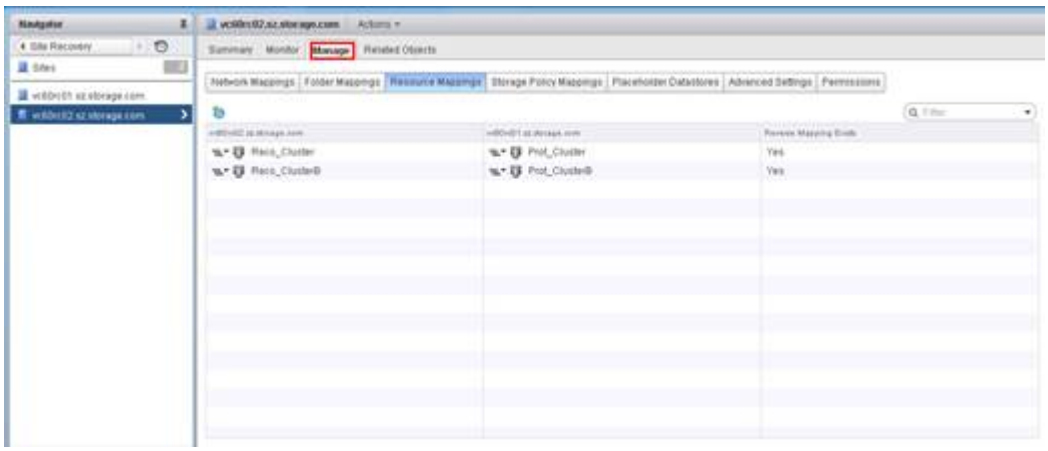
Step 2 Click **Site Recovery**.



Step 3 Choose **Sites**.



Step 4 Select the protected site and click the **Manage** tab.

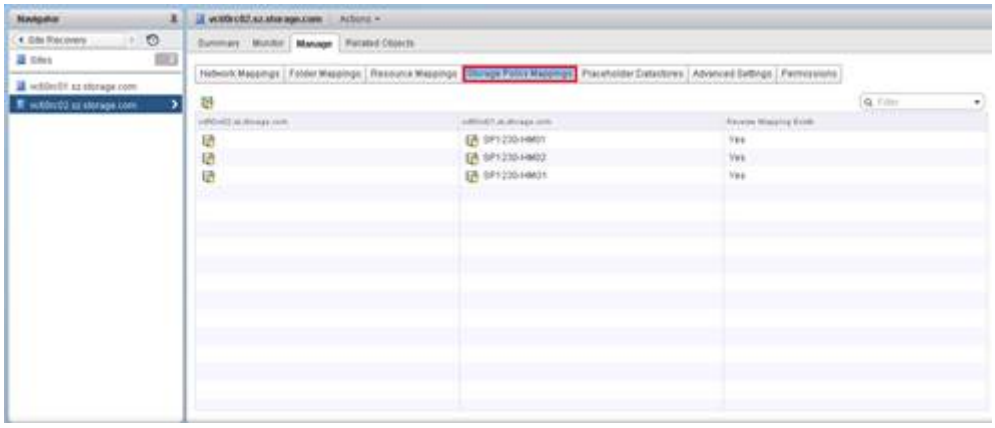


Step 5 Configure storage policy mapping.

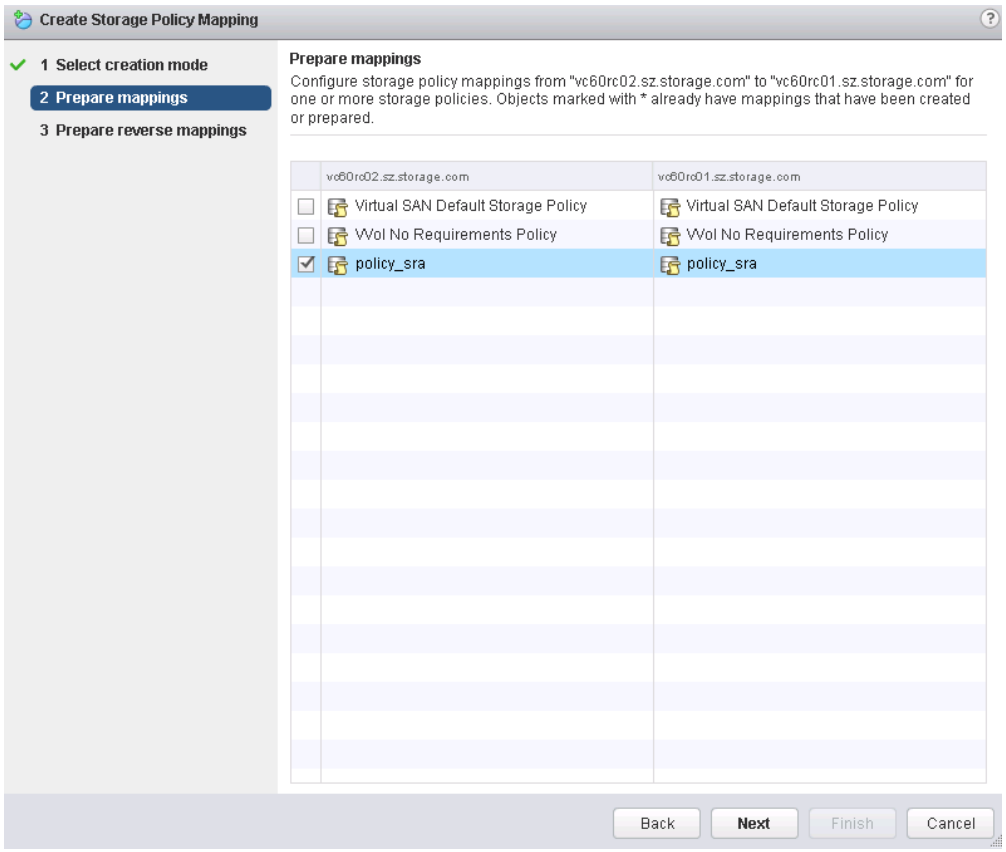
NOTE

Storage policy mapping needs to be configured only in the HyperMetro solution.

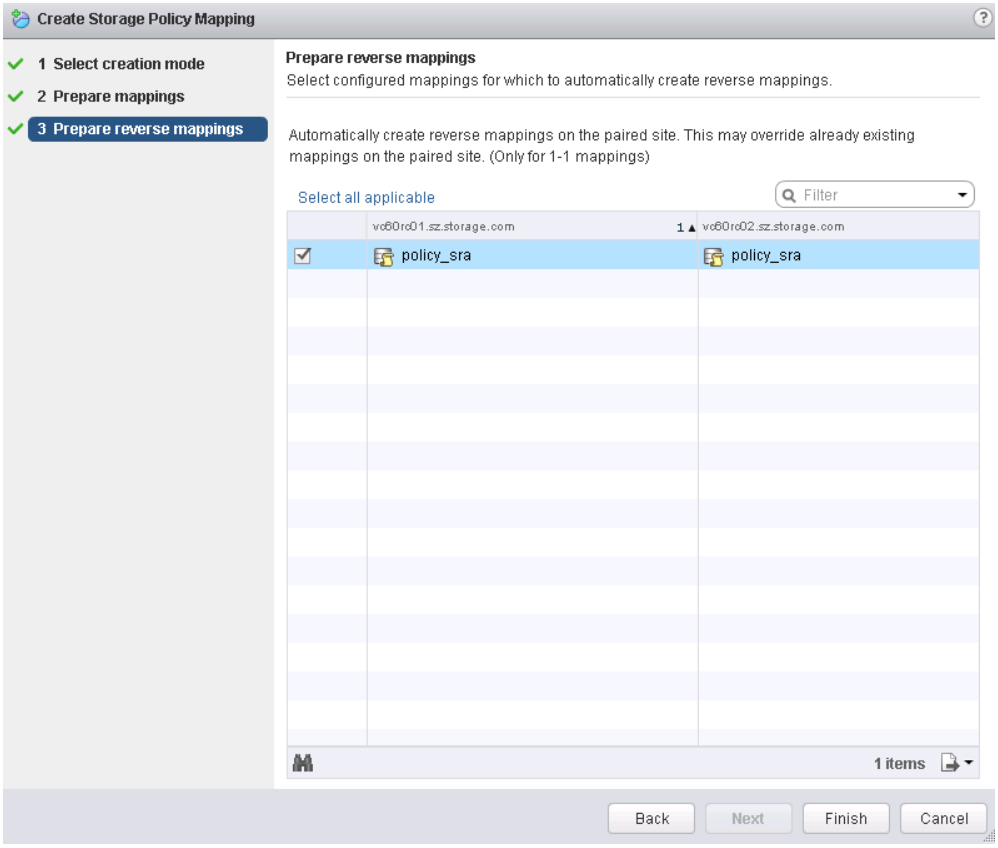
1. Click the **Storage Policy Mappings** tab.



2. Click .
3. Select **Automatically prepare mappings for storage policies with matching names** and click **Next**.
4. Select the created storage policy and click **Next**.

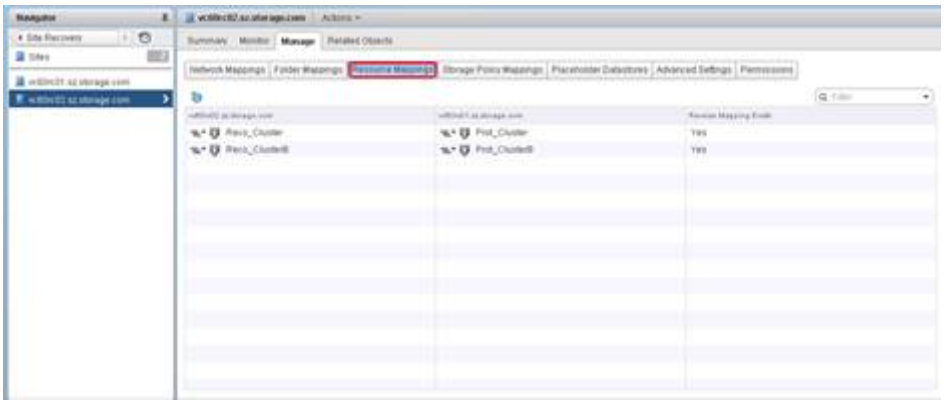


5. Select the reverse mapping policy and click **Finish**.

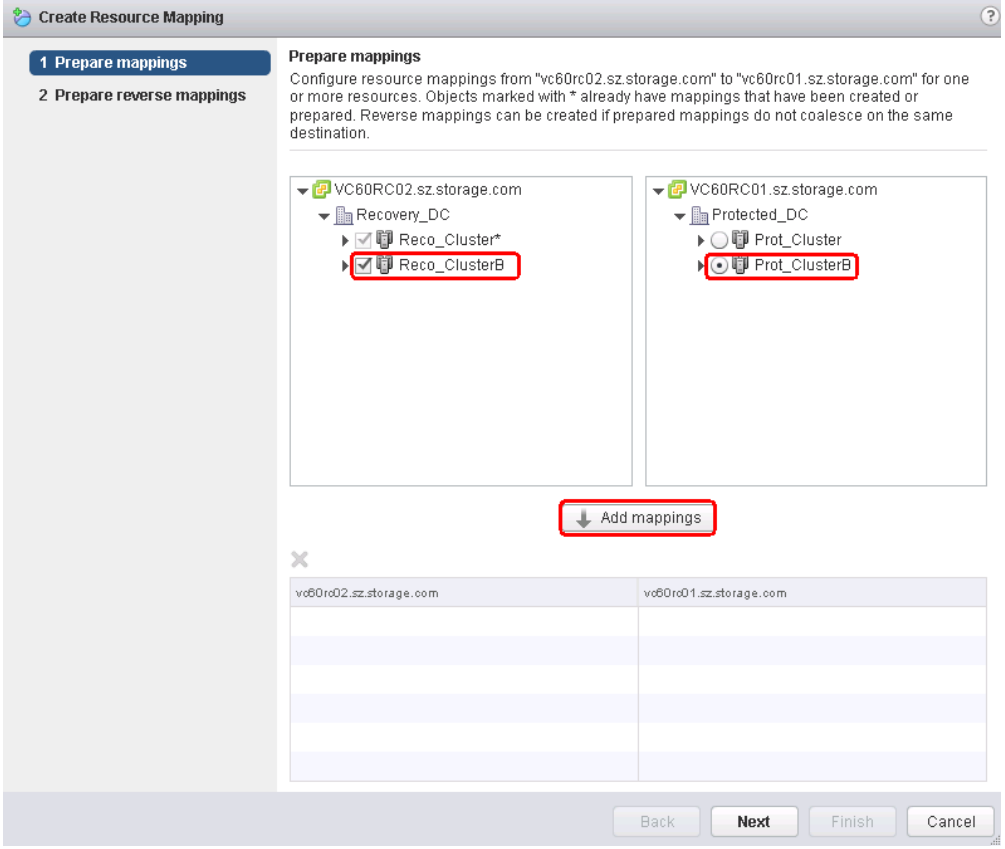


Step 6 Configure resource mapping.

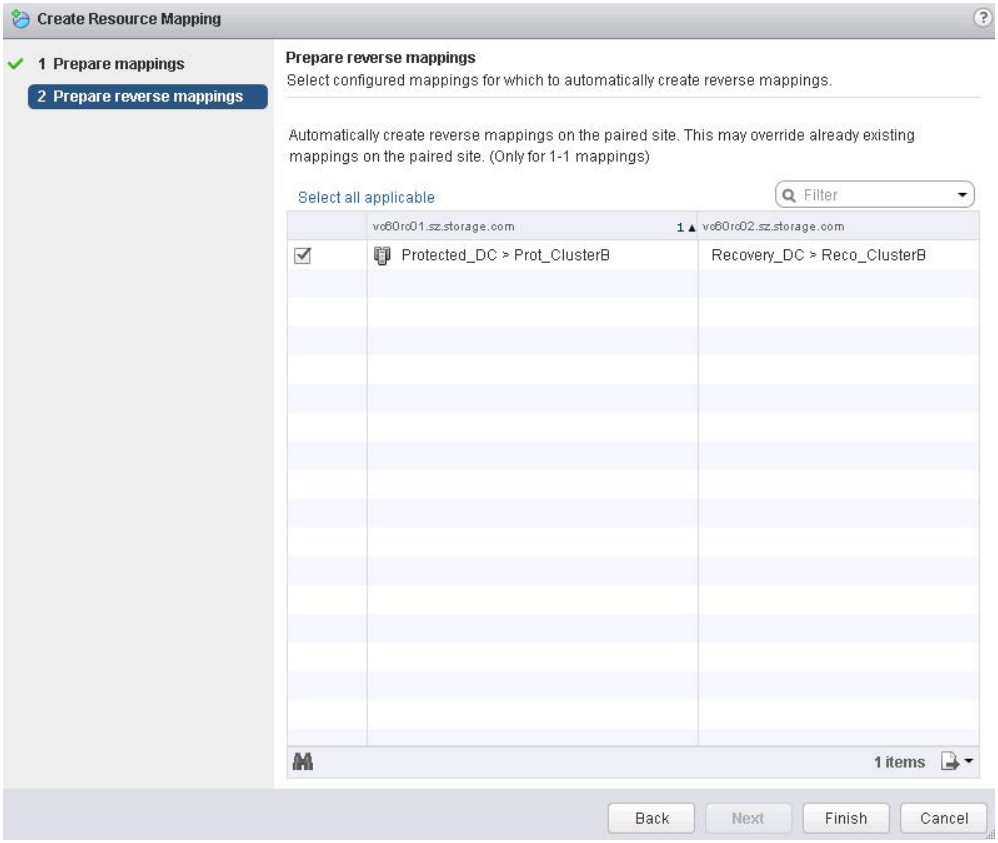
1. Click the **Resource Mappings** tab.



2. Click to create resource mapping.
3. Select the desired ESXi host and click **Add mappings**.



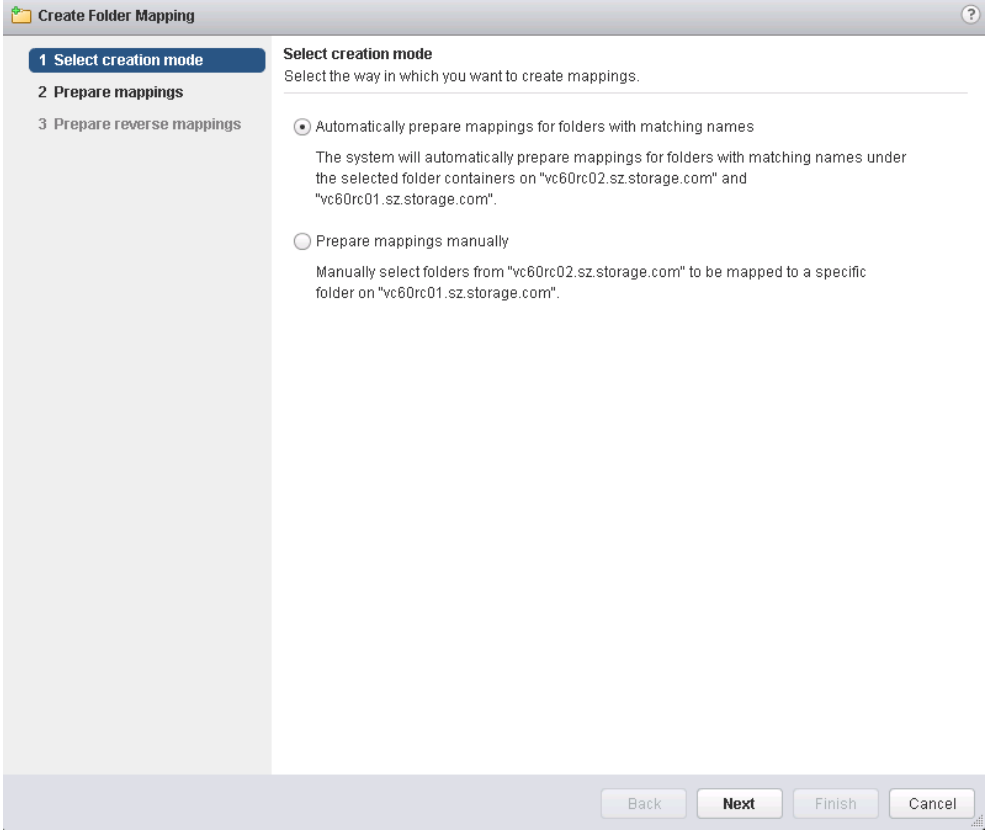
4. Click **Next**.
5. Click **Select all applicable**.



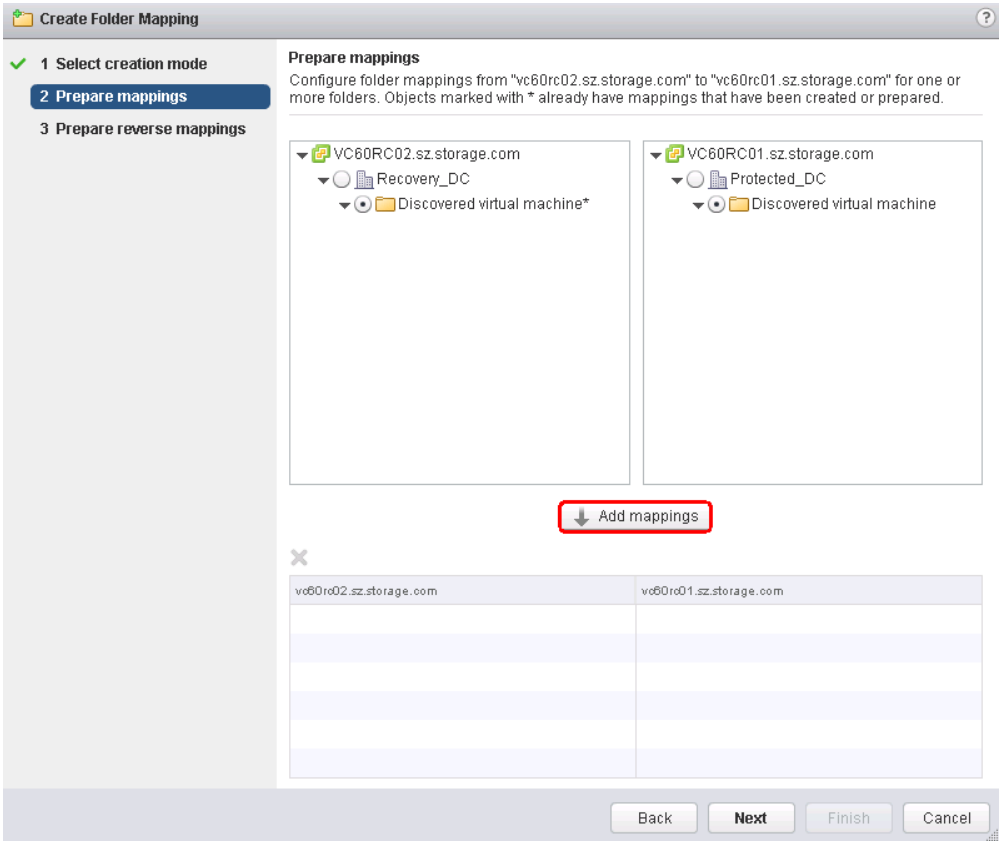
6. Click **Finish**.

Step 7 Configure folder mapping.

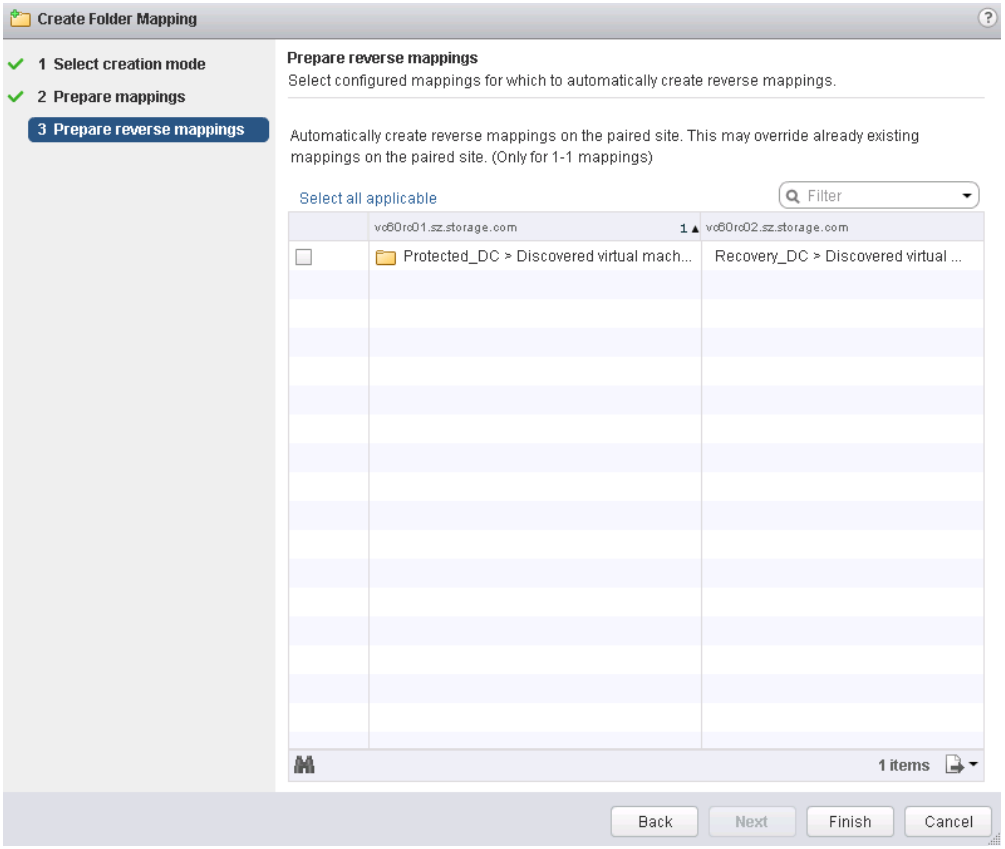
1. Click the **Folder Mappings** tab.
2. Click to create folder mapping.
3. Select **Automatically prepare mappings for folders with matching names** and click **Next**.



4. Select the desired folders at the protected site and recovery site, click **Add Mappings**, and click **Next**.



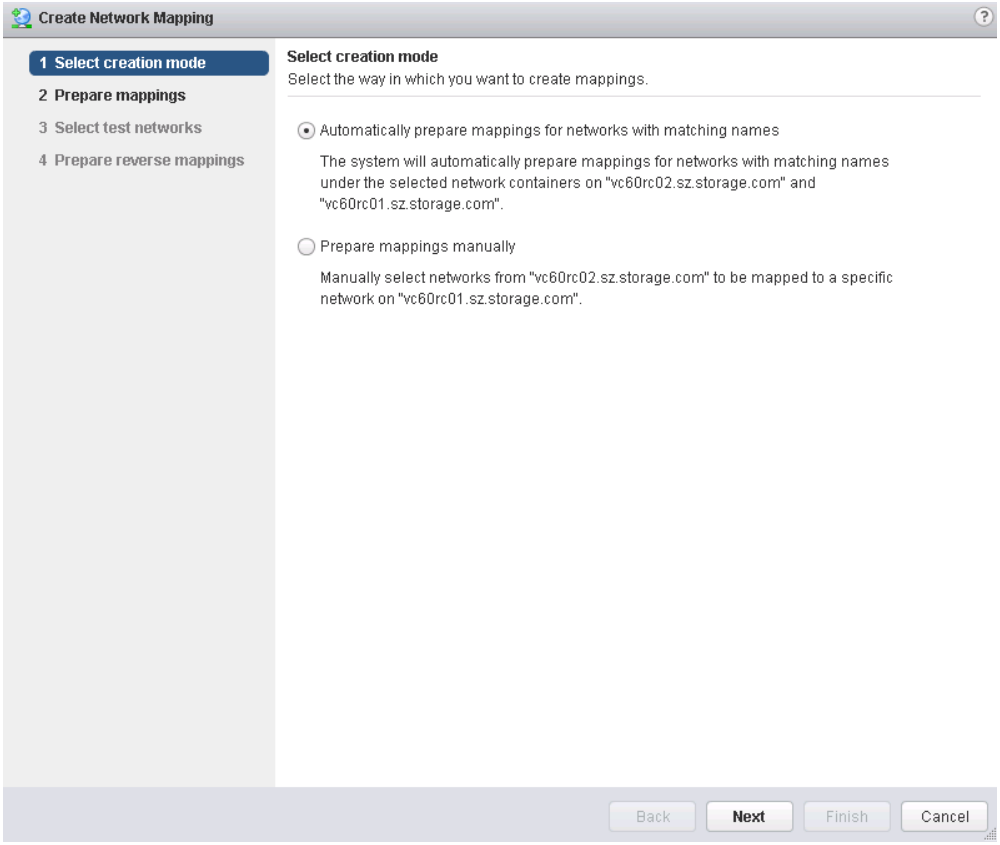
5. Click **Select all applicable**.



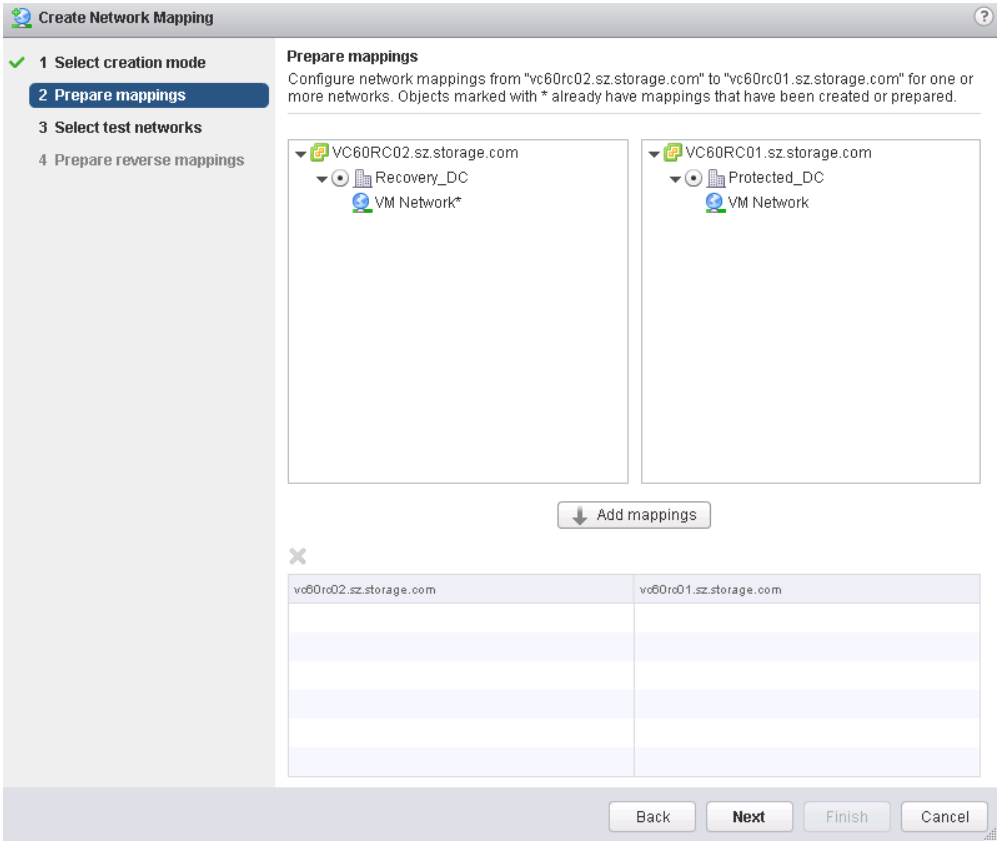
6. Click **Finish**.

Step 8 Configure network mapping.

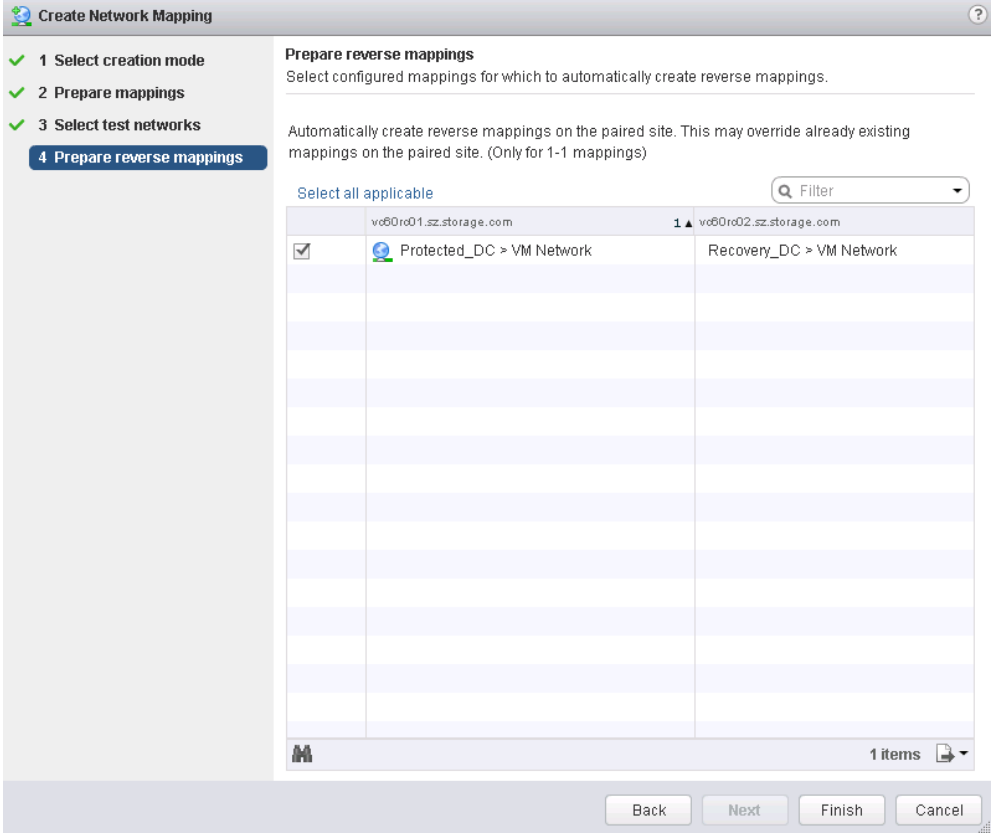
1. Click the **Network Mappings** tab.
2. Click to create network mapping.
3. Select **Automatically prepare mappings for networks with matching names** and click **Next**.



4. Select the networks at the protected site and recovery site and click **Add mappings**.



5. Click **Next**.
6. Click **Next**.
7. Click **Select all applicable**.

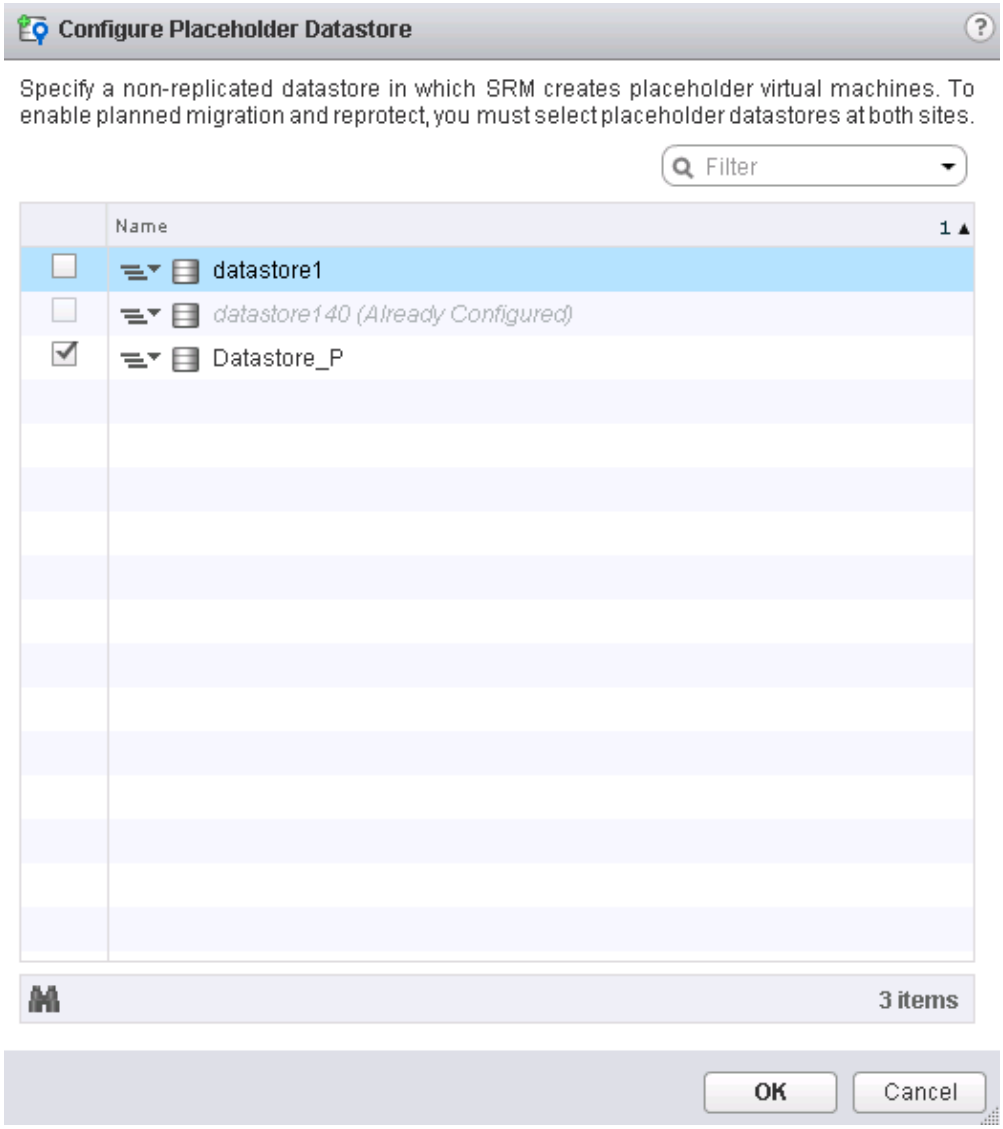


8. Click **Finish**.

Step 9 Configure a placeholder data store.

You are advised to use a data store created on a common LUN instead of a local data store on an ESX host as a placeholder data store.

1. Click the **Placeholder Datastores** tab.
2. Click to configure a placeholder data store.
3. Select the created remote placeholder data store and click **OK**.



4. Repeat the preceding steps to configure a placeholder data store at the recovery site.

NOTE

If the recovery site has no data store, create a data store and configure it as a placeholder data store.

----End

4.5.10 Creating and Configuring Placeholder Storage

You are advised to use a common LUN or datastore created on FusionSphere as placeholder storage, instead of using an ESX local datastore. For details about how to create placeholder storage, see section **4.5.1 Creating a Datastore (VMFS)** and section **4.5.2 Creating a Datastore (NFS)**.

Configuring a Placeholder Datastore

Step 1 Log in to the VMware vSphere Web Client at the protected site.

Step 2 Choose v**Center Inventory Lists** > **Datastores**.

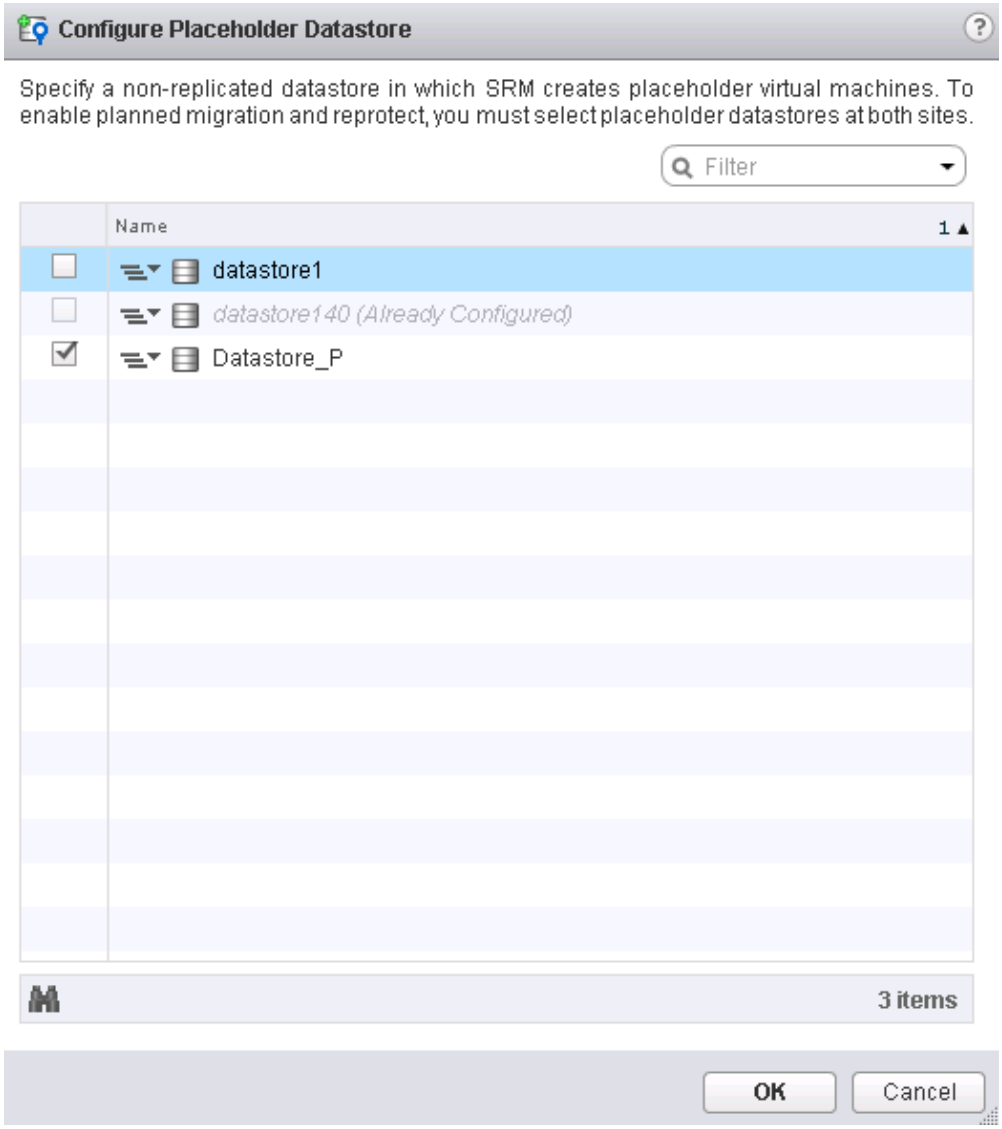
1. Select the protected site and click the **Manage** tab.

Step 3 Click the **Placeholder Datastore** tab.

Step 4 Click to configure a placeholder datastore.

Step 5 Select the created remote placeholder datastore and click **OK**.

----End



----End

4.5.11 Adding Array Managers

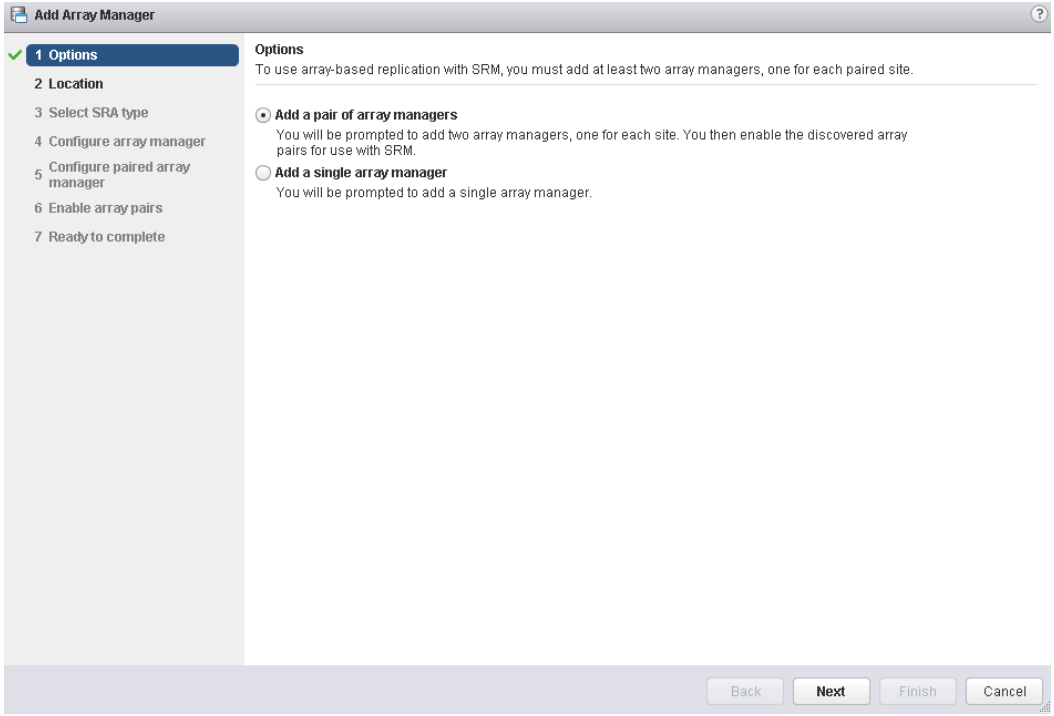
Step 1 Log in to the VMware vSphere Web Client at the protected site, and click **Site Recovery**.

Step 2 Select **Inventories** > **Array Based Replication**.

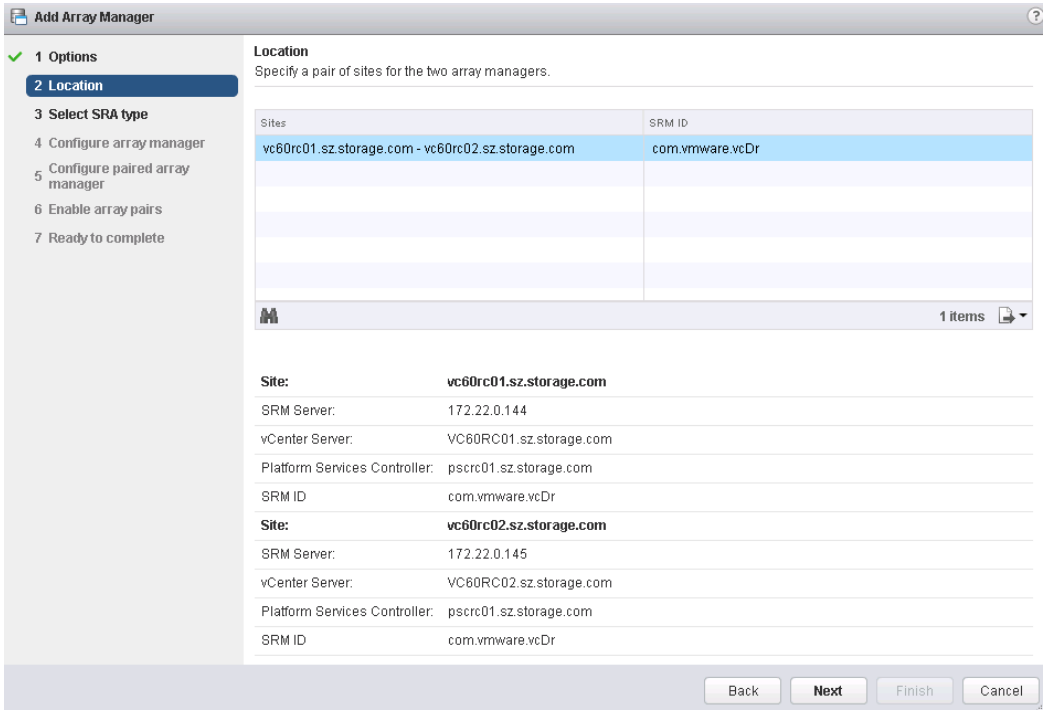
Step 3 Click (**Add Array Manager**).

The array manager configuration wizard is displayed.

Step 4 Click **Add a pair of array managers** and click **Next**.



Step 5 Select a site and click **Next**.



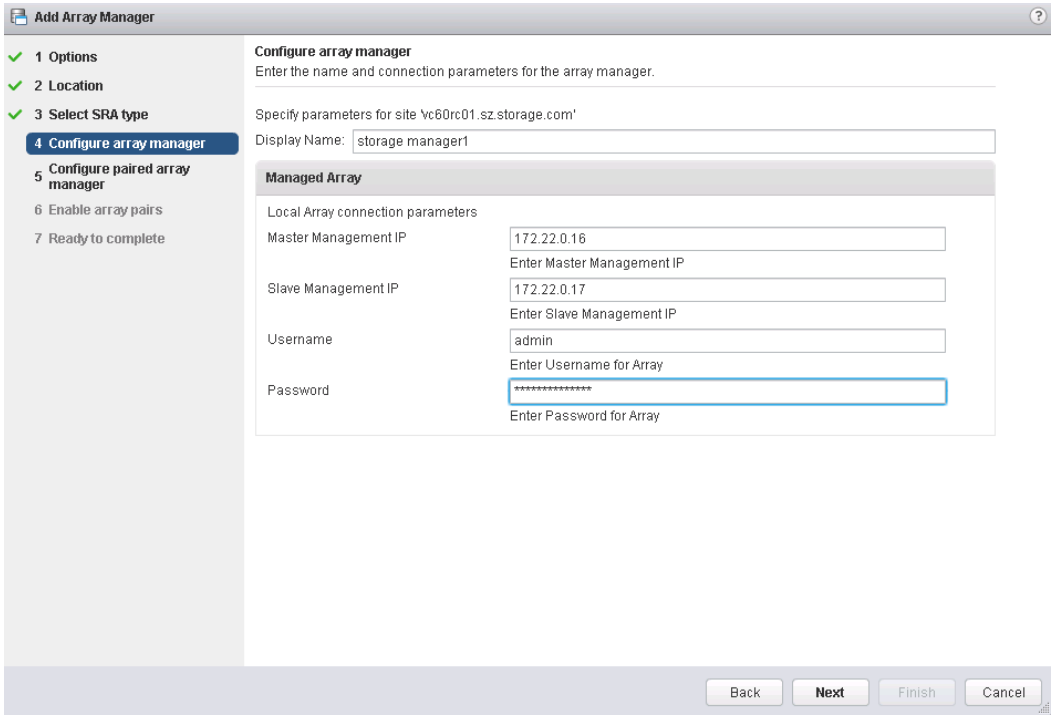
Step 6 Set the SRA type and click **Next**.

NOTE

Currently, many storage vendors provide different SRA software for different SRM environments. In this step, set the SRA type to **Huawei eSDK_Storage_SRA**.

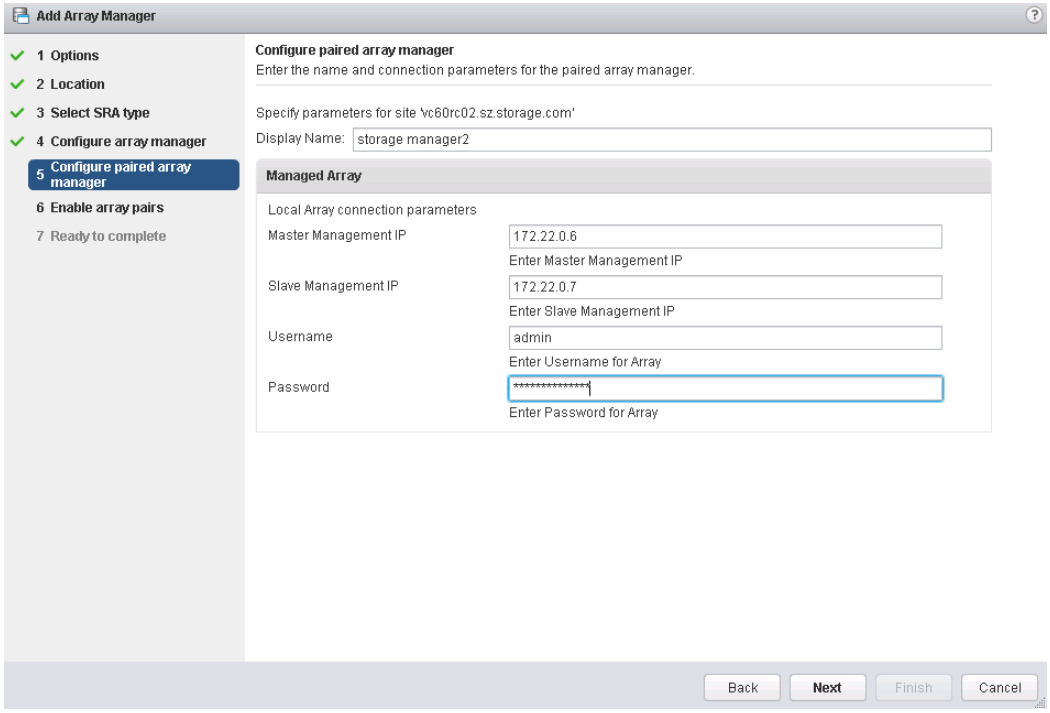
Step 7 Configure an array manager and click **Next**.

- **Display Name**: name of the array manager, which can be defined by users
- **Master Management IP**: management IP address of controller A on the storage array at the local site (example: vs6001-sra.sz.strorage.com)
- **Slave Management IP**: management IP address of controller B on the storage array at the local site (example: vs6001-sra.sz.strorage.com)
- **Username**: user name of the storage array at the local site
- **Password**: password of the storage array at the local site

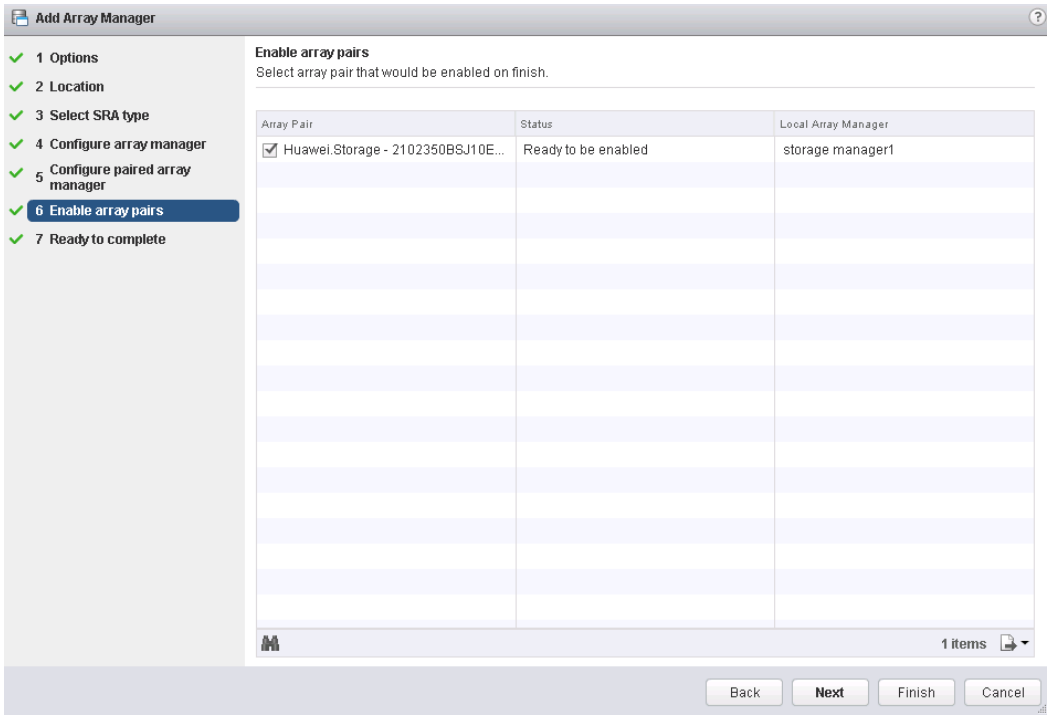


Step 8 Configure the paired array manager and click **Next**.

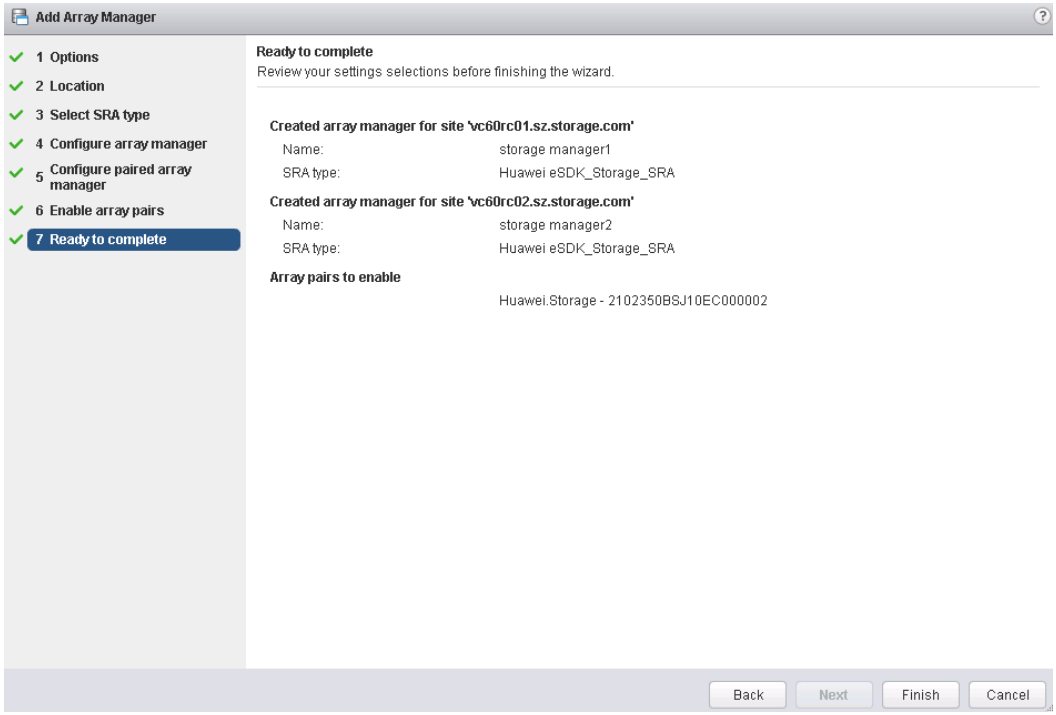
- **Display Name**: name of the array manager, which can be defined by users
- **Master Management IP**: management IP address of controller A on the storag array at the peer site (example: vs6002-sra.sz.strorage.com)
- **Slave Management IP**: management IP address of controller B on the storage array at the peer site (example: vs6002-sra.sz.strorage.com)
- **Username**: user name of the storage array at the peer site
- **Password**: password of the storage array at the peer site



Step 9 Select the storage array pair and click **Next**.



Step 10 Click **Finish**.

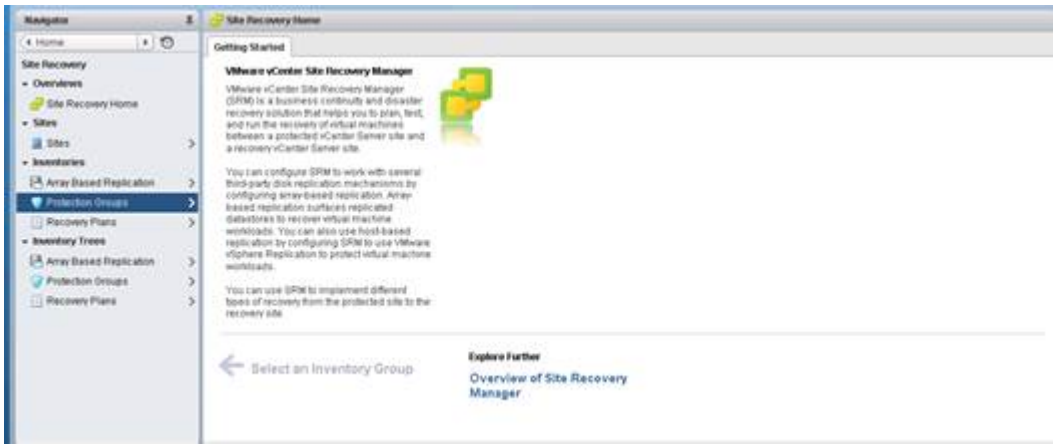


----End

4.5.12 Creating a Datastore-Based Protection Group

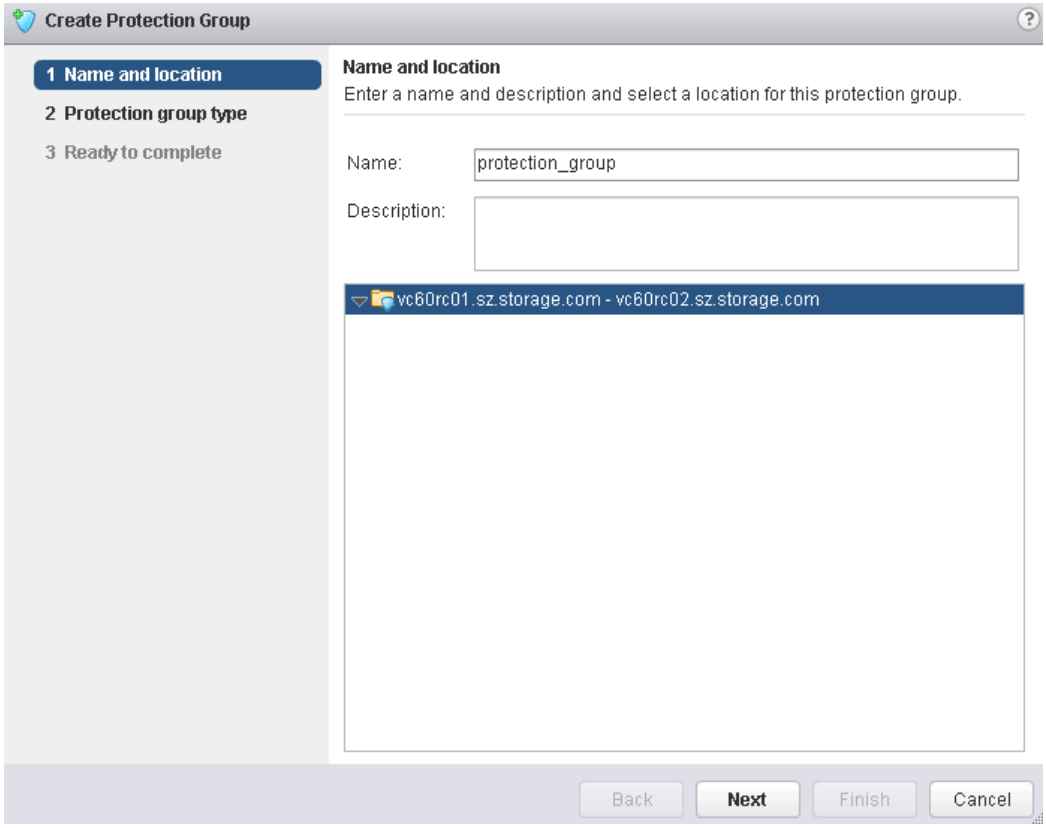
Step 1 Log in to the VMware vSphere Web Client at the protected site, and click **Site Recovery**.

Step 2 Choose **Inventories** >**Protection Groups**.



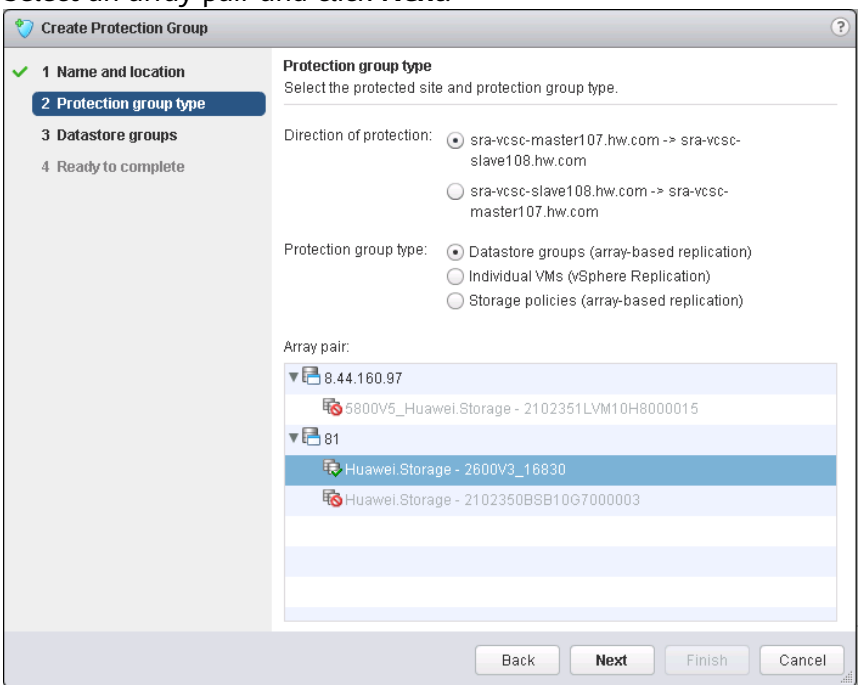
Step 3 Click to create a protection group.

Step 4 Set the protection group name and click **Next**.

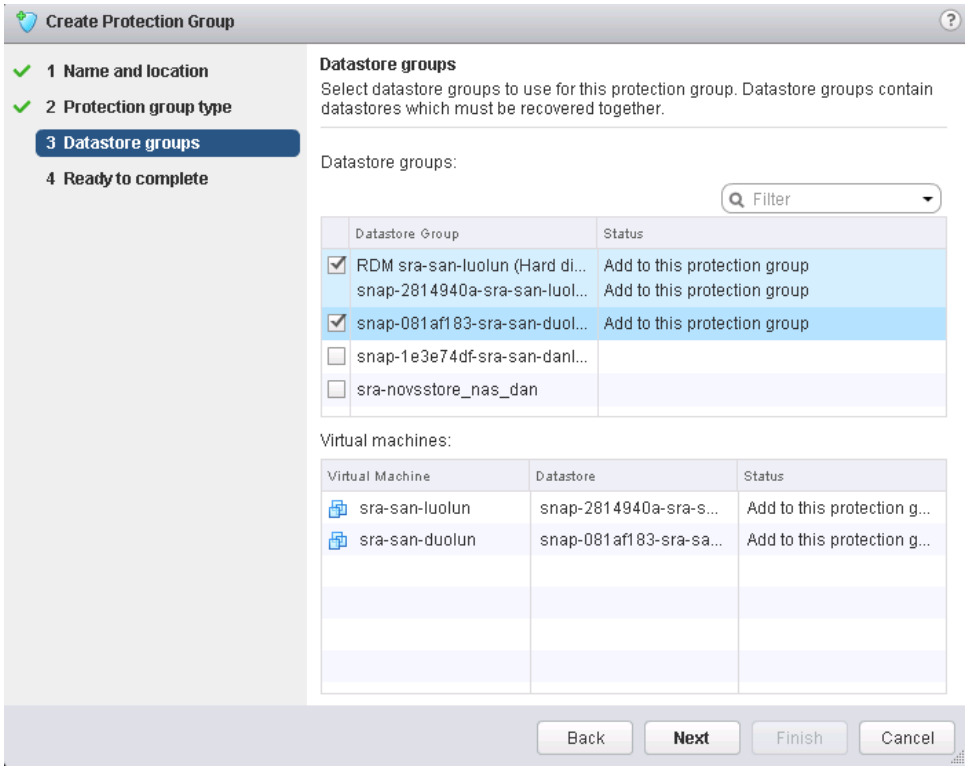


Step 5 Set the protection group type.

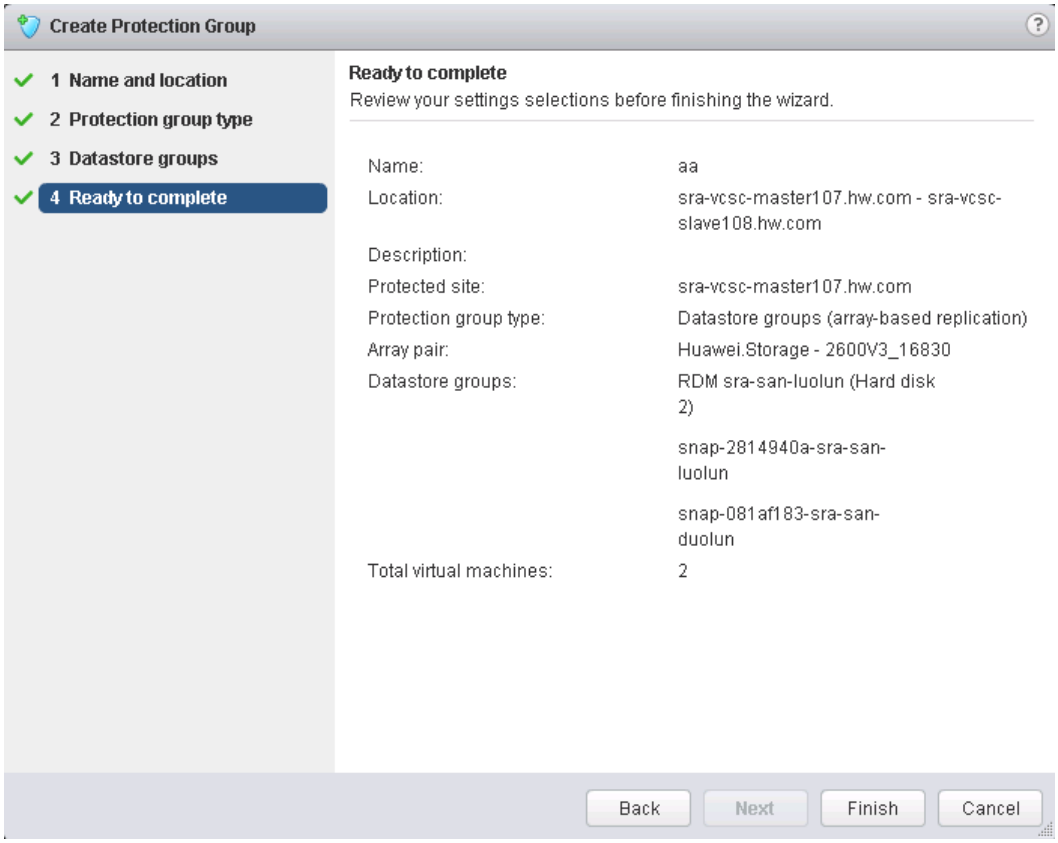
- **Direction of protection**: protected site -> recovery site.
- **Protection group type**: Select **Datastore groups (array-based replication)**. Select an array pair and click **Next**.



Step 6 Select desired datastore groups and click **Next**.



Step 7 Click **Finish**.



----End

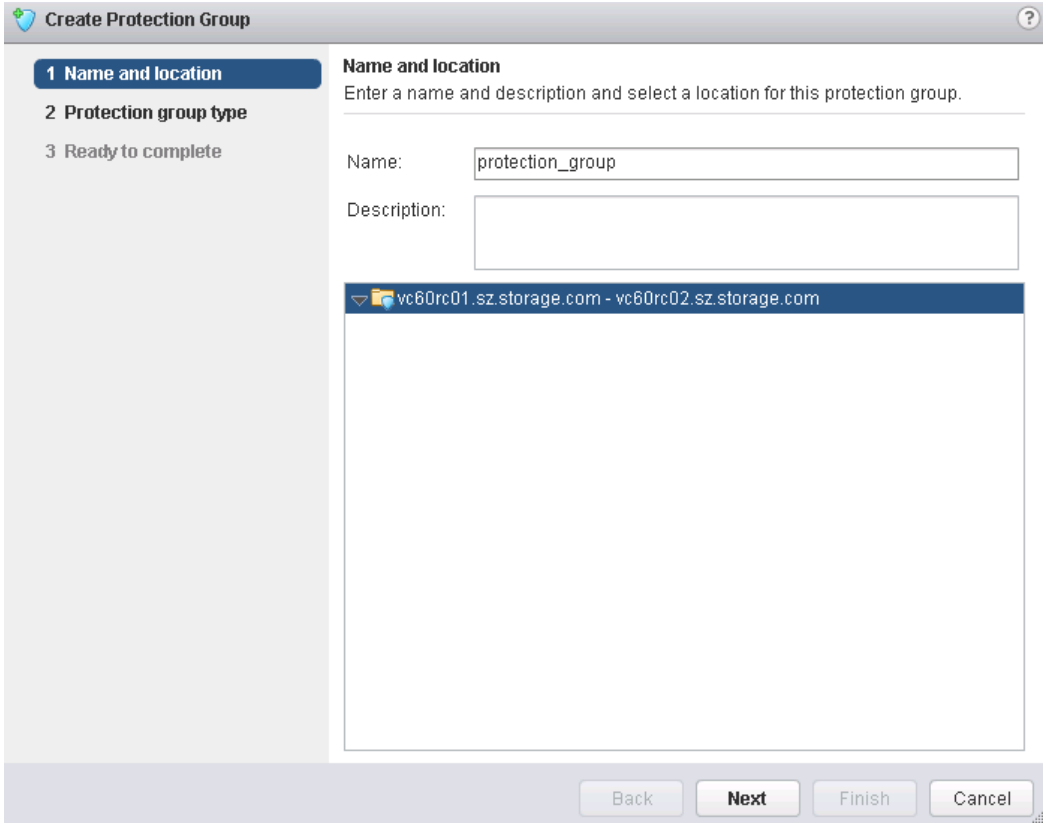
4.5.13 Creating a Policy-Based Protection Group

Step 1 Log in to the VMware vSphere Web Client and click **Site Recovery**.

Step 2 Choose **Inventories** >**Protection Groups**.

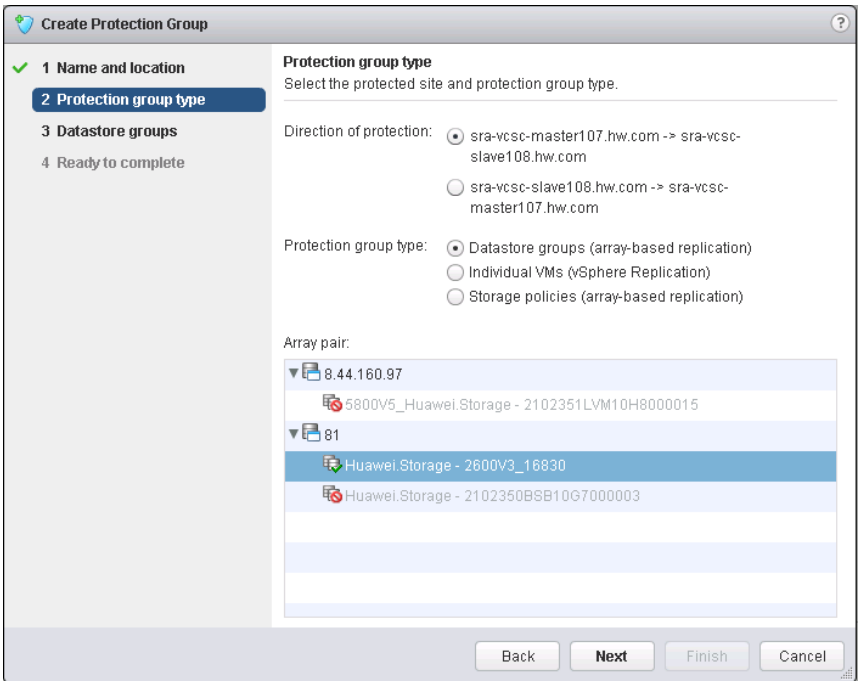
Step 3 Click to create a protection group.g

Step 4 Set the protection group name and click **Next**.

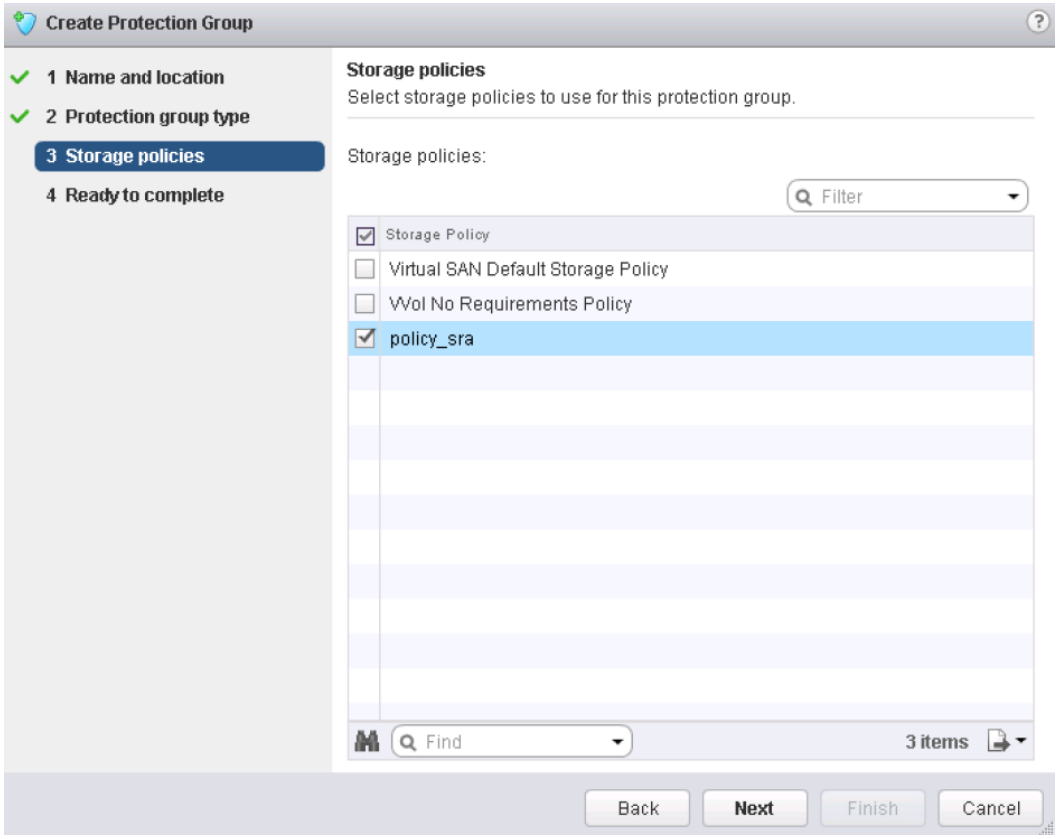


Step 5 Set the protection group type.

- **Direction of protection**: protected site > recovery site.
- **Protection group type**: Select **Storage policies (array-based replication)**.



Step 6 Select **Storage policy** and click **Next**.



Step 7 Click **Finish**.

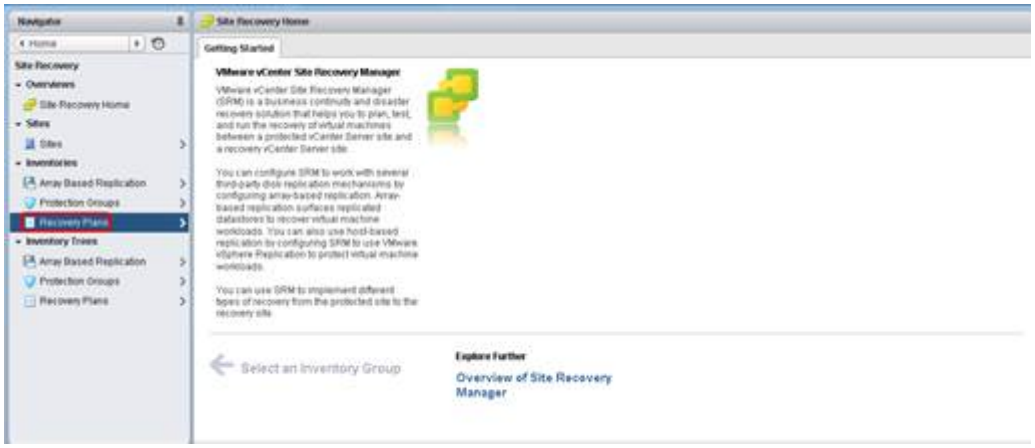
----End

4.5.14 Creating a Recovery Plan (Based on VM Protection Groups)

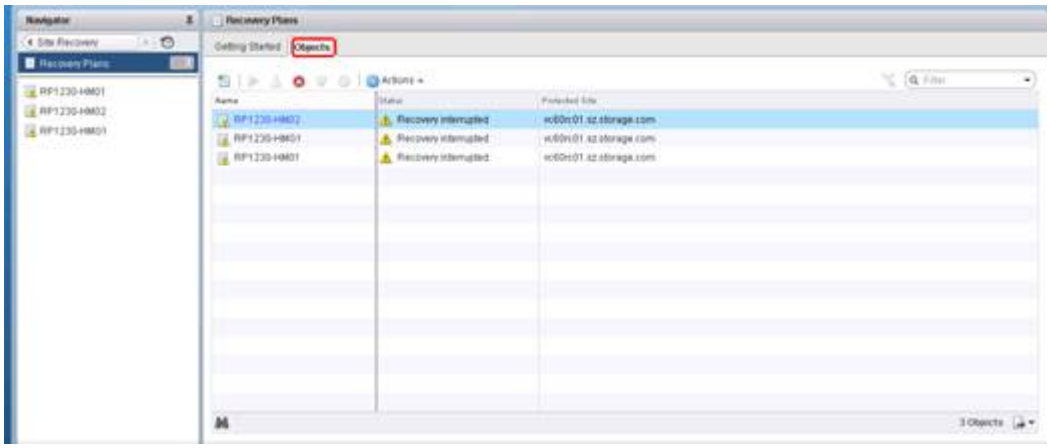
Step 1 Log in to the VMware vSphere Web Client at the protected site.

Step 2 Click **Site Recovery**.

Step 3 Select **Recovery Plans**.

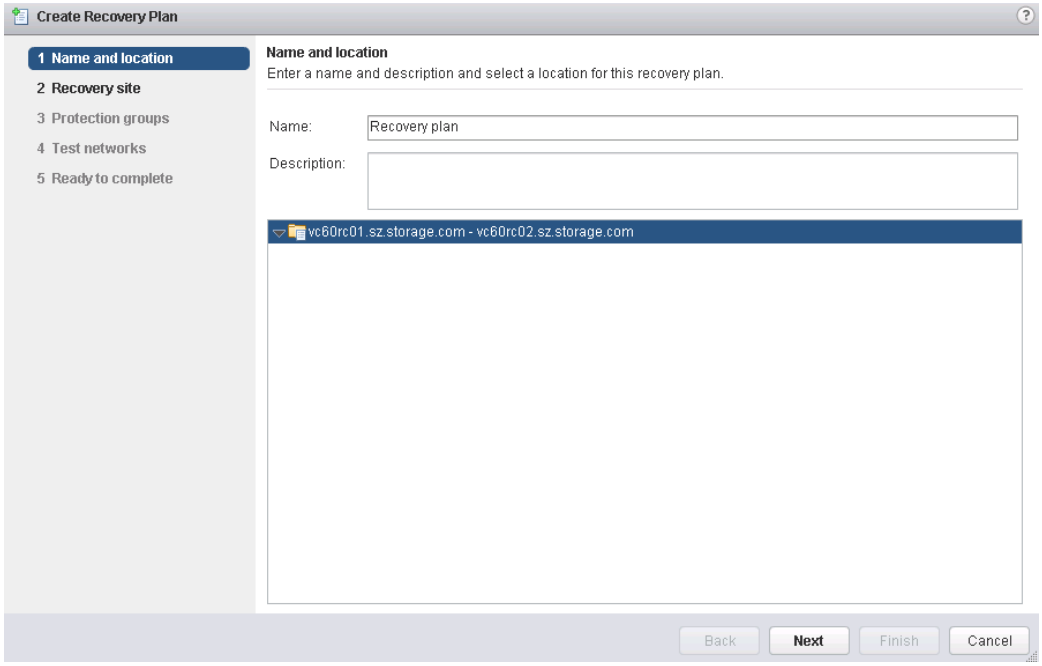


Step 4 Click the **Objects** tab.

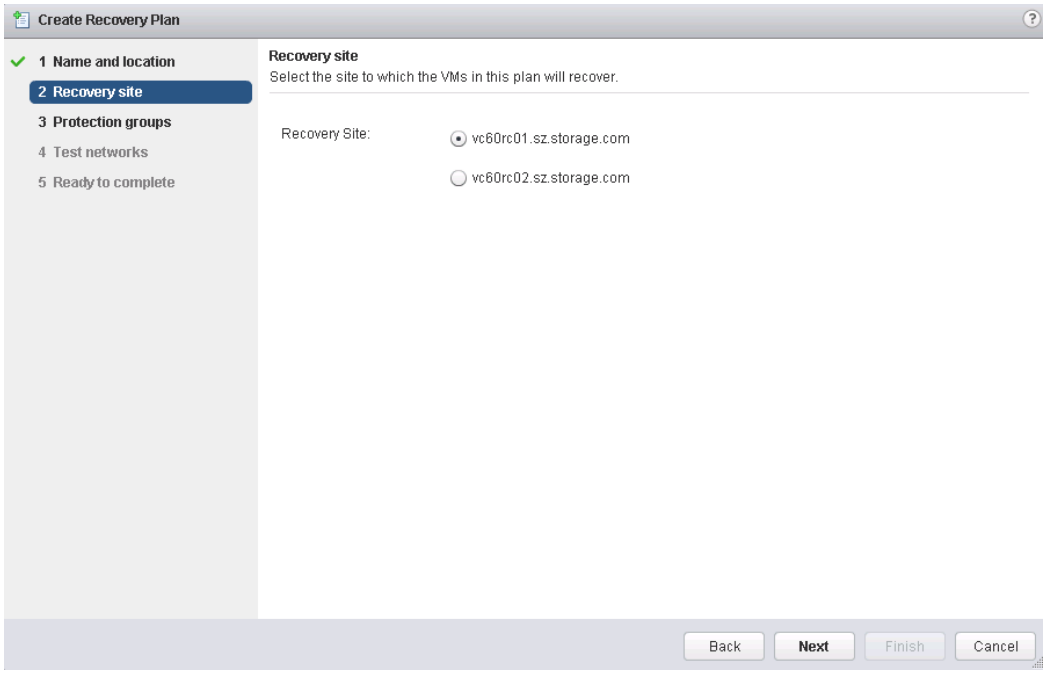


Step 5 Click .

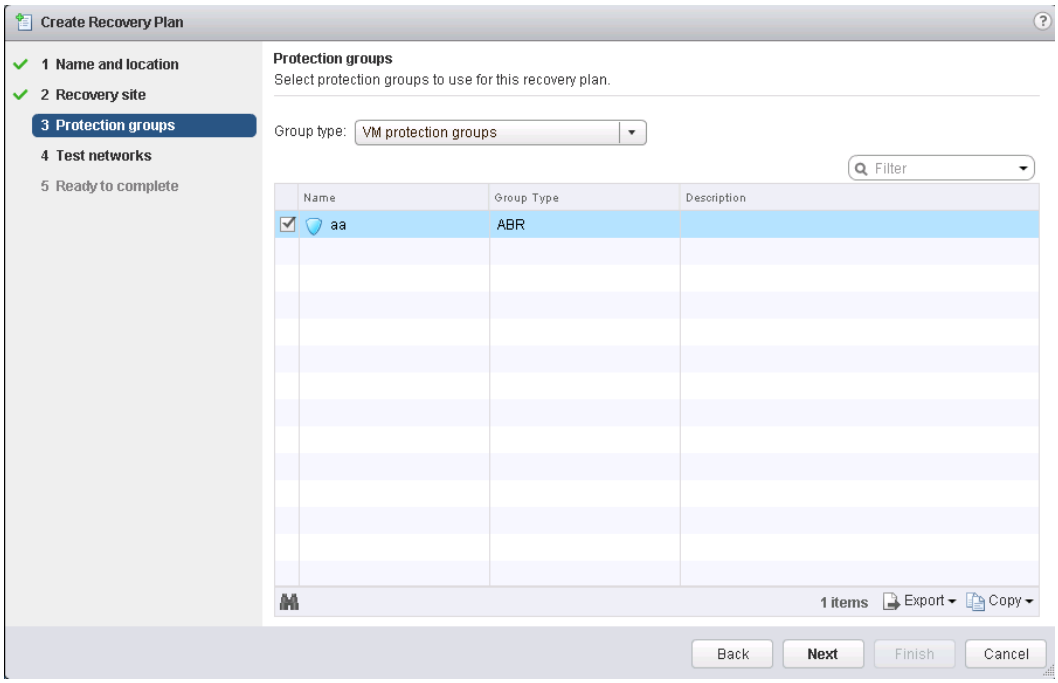
Step 6 Set the recovery plan name and click **Next**.



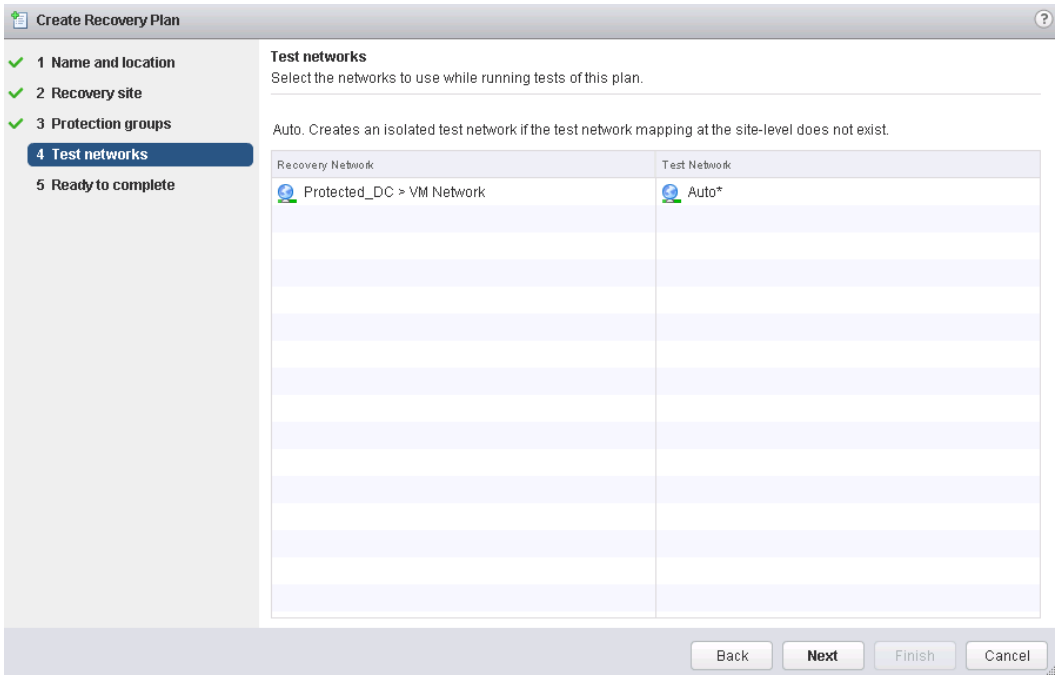
Step 7 Select the recovery site and click **Next**.



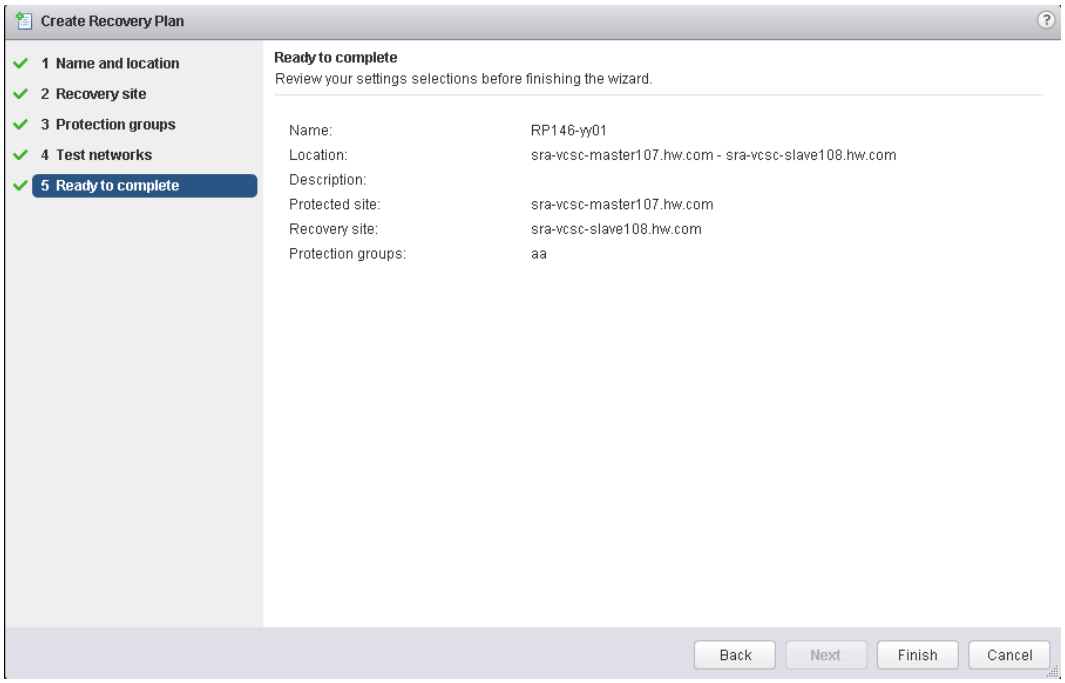
Step 8 Select VM protection groups from the **Group type** drop-down list. Then, click **Next**.



Step 9 Click **Next**.



Step 10 Click **Finish**.



----End

4.5.15 Creating a Recovery Plan (Based on a Storage Policy for a Protection Group)

Step 1 Log in to the VMware vSphere Web Client and click **Site Recovery**.

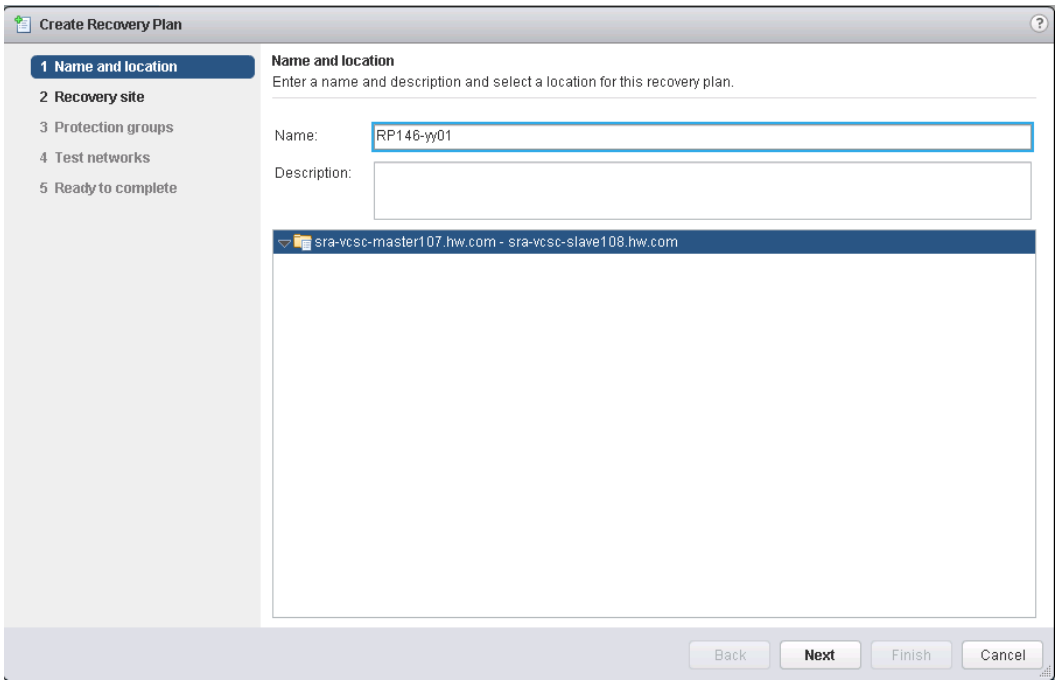
Step 2 Select **Recovery Plan**.

Step 3 Click the **Objects** tab.

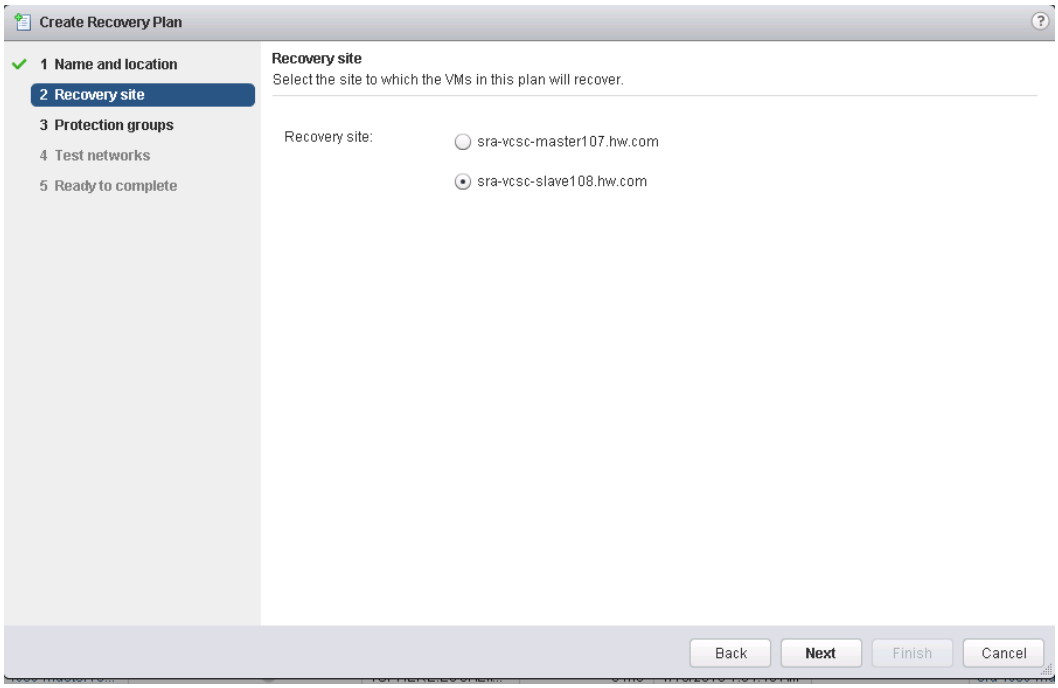
Step 4 Select the **Recovery Plan** tab.

Step 5 Click.

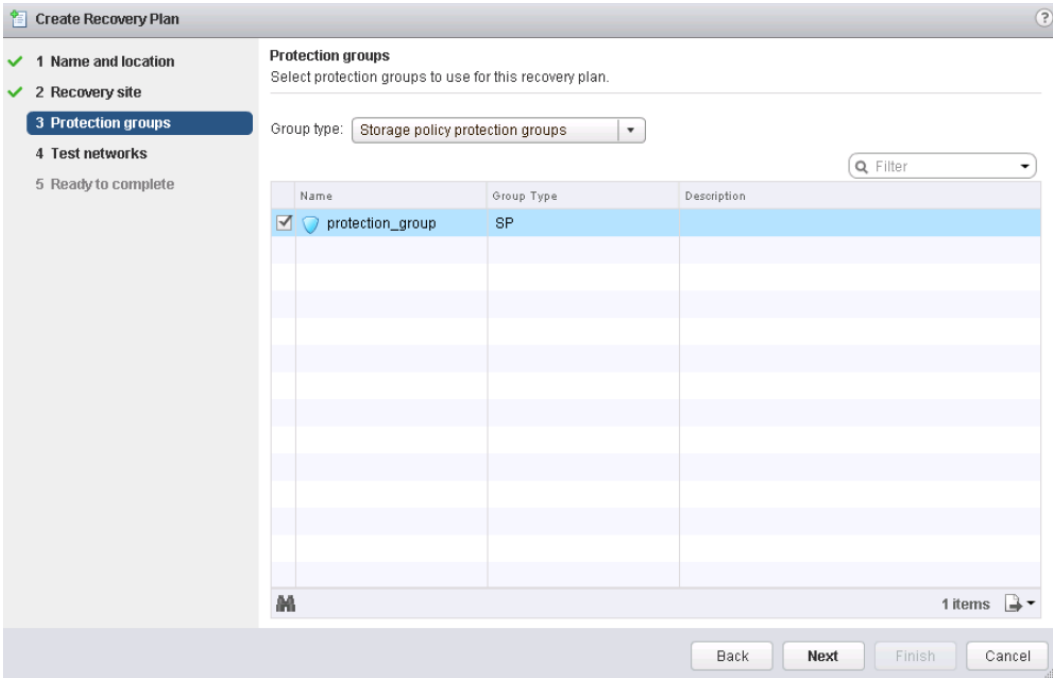
Step 6 Set the recovery plan name and click **Next**.



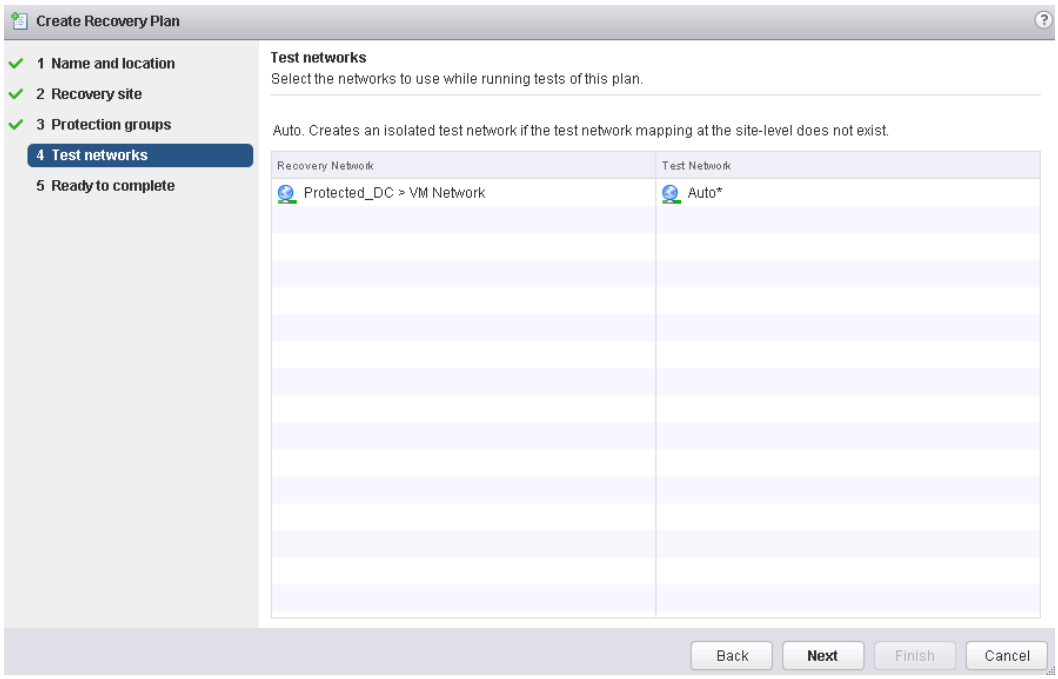
Step 7 Select the recovery site and click **Next**.



Step 8 Select **Storage policy protection groups** from the drop-down list of **Group Type**. Then, select a protection group, such as **protection_group**, and click **Next**.



Step 9 Click **Next**.



Step 10 Click **Finish**.

----End

5 Fault Recovery Scenarios

NOTE

After a recovery task is executed successfully, you are advised to wait for 2 minutes before you perform reprotection.

5.1 Recovery Plan Test

5.2 Planned Migration

5.3 Disaster Recovery

5.4 Switchback

5.1 Recovery Plan Test

Scenario Identification

A disaster recovery test is used to verify the availability of disaster recovery and estimate the required time. Customers should test disaster recovery periodically to ensure that the disaster recovery process is available. In addition, periodic tests and audit result recording are required by most regulations.

Scenario Analysis

VMs on the active-active devices will be started in an independent network. SRM will test the compatibility of vMotion hosts and run the **testFailoverStart** command so that write snapshots can be created at the recovery site. The SRM will load the snapshots and start the corresponding VMs from the snapshots. After the test is complete, the **testFailoverStop** command needs to be run to delete these writable snapshots. The two commands are optional.

NOTICE

When creating a snapshot, do not use **snapshot_for_vssra** as the prefix of the snapshot name.

 Copyright © Huawei Technologies Co., Ltd.

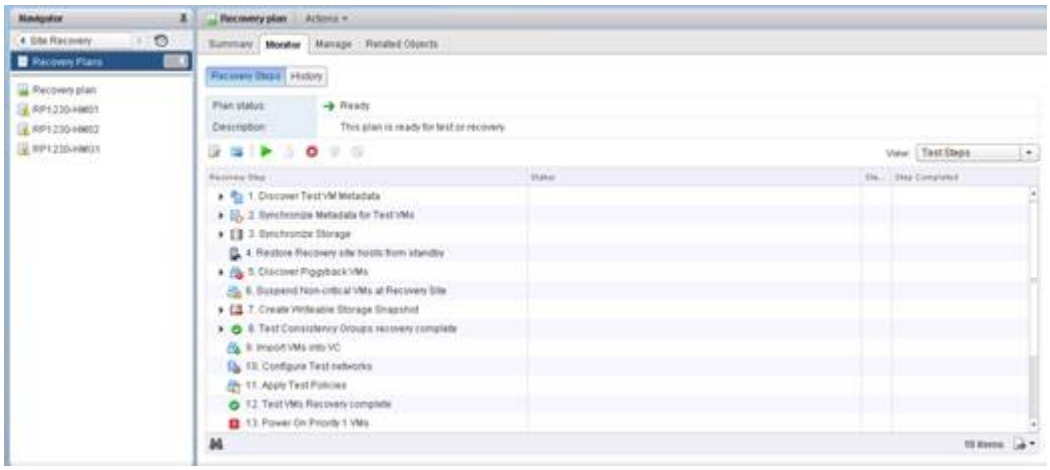
Procedure

Step 1 Log in to the VMware vSphere Web Client at the protected site and click **Site Recovery**.

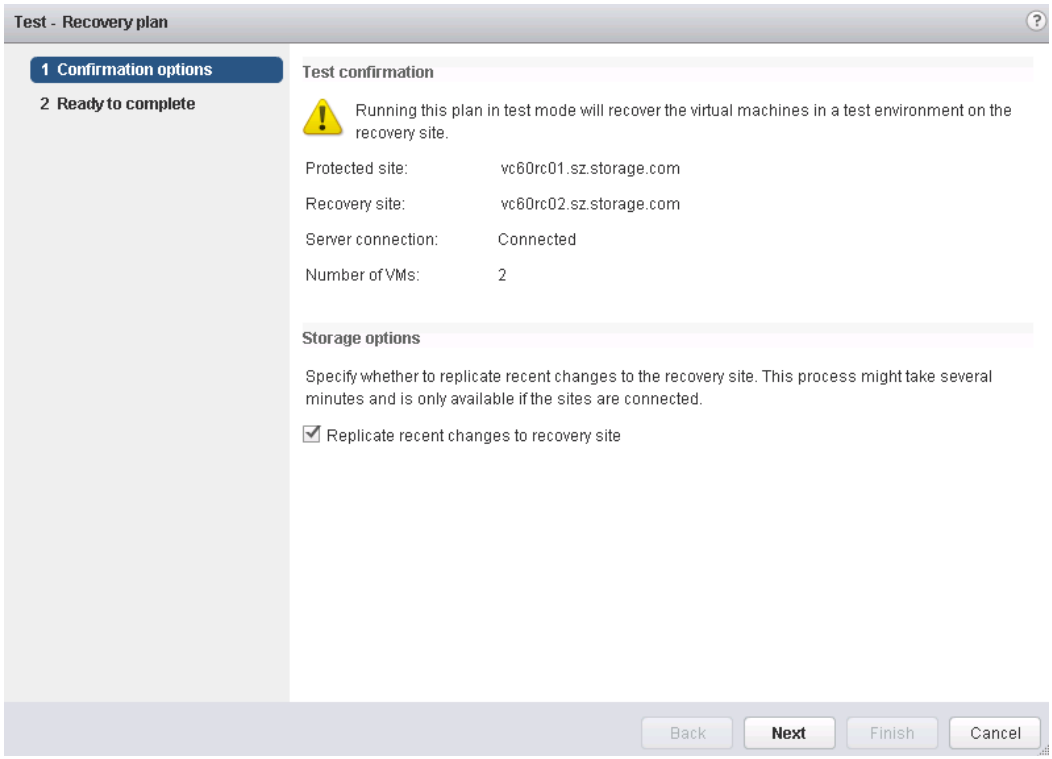
Step 2 Choose **Recovery Plans** from the navigation tree.

Step 3 Select the desired recovery plan.

Step 4 Click the **Monitor** tab and then the **Recovery Steps** tab.



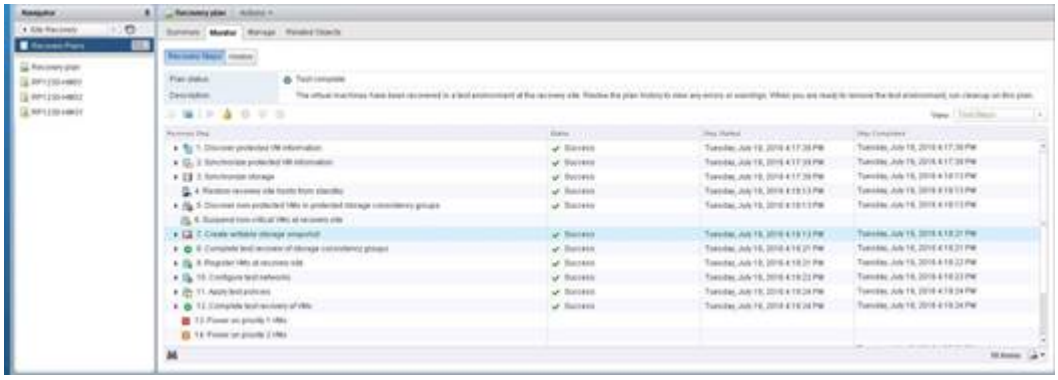
Step 5 Click ▶.



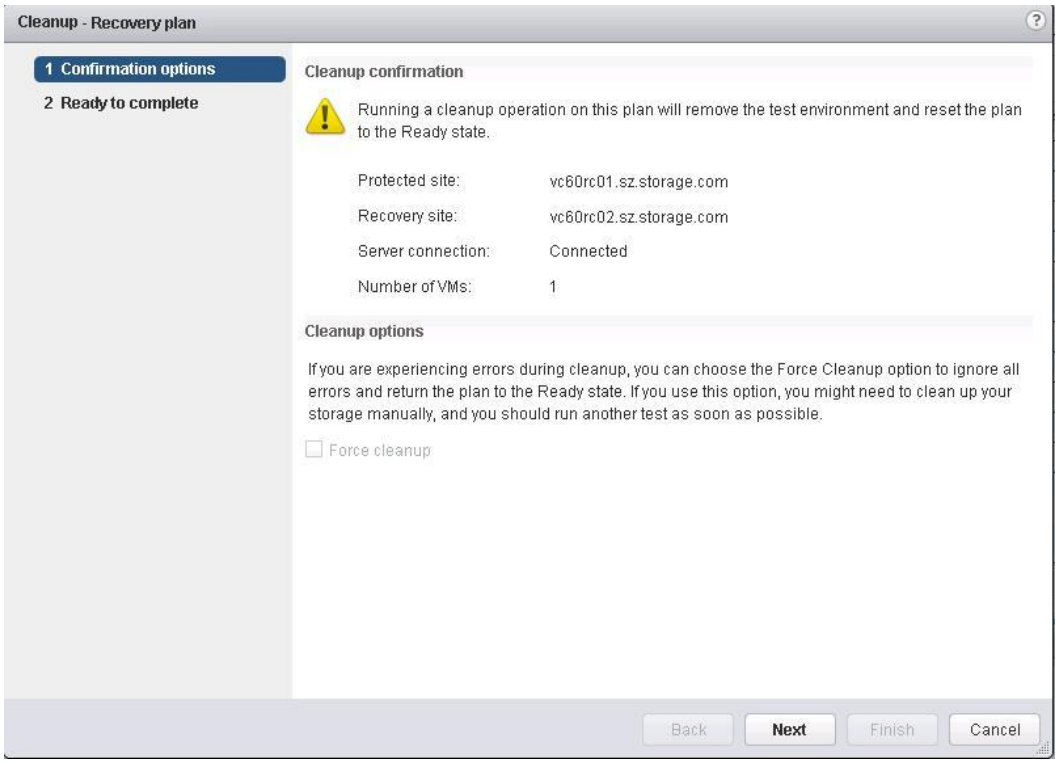
Step 6 Click **Next**.

Step 7 Click **Finish**.

After a recovery plan test is completed, the page shown in the following figure is displayed.



Step 8 Click to remove the test environment and restore the recovery plan to the ready state.

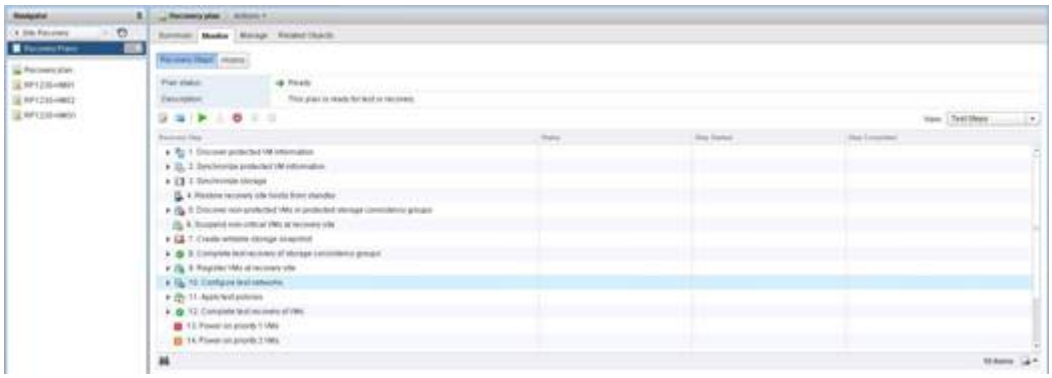


Step 9 Click **Next**.

Step 10 Click **Finish**.

----End

After the cleanup operation on the recovery plan is completed, the page shown in the following figure is displayed.



5.2 Planned Migration

Scenario Identification

A planned migration is performed for system maintenance or is manually performed by users to protect services against potential disasters. The planned migration ensures service consistency and data integrity.

The purposes of and requirements for planned migrations are as follows:

- To tackle foreseeable potential disasters, such as typhoons, floods, and forcible evacuation, planned migrations are performed to prevent storage systems from breaking down and to achieve zero data loss.
- Planned migrations are performed for planned data center maintenance. During planned maintenance, services must keep running, and application owners and end users do not notice the maintenance. After the maintenance is complete, applications can be switched back.
- Planned migrations are performed to achieve global load balancing because SRM Stretch does not support dynamic global load balancing. (For storage arrays, some LUNs are migrated as instructed by the SRA to achieve global load balancing.)

Scenario Analysis

Based on whether VMs support SRM Stretch, the process is as follows:

- If VMs do not support SRM Stretch, VMs interrupt host I/Os at the protected site. After data is replicated to the recovery site, VMs are started at the recovery site. Services are interrupted during the process.
- If VMs support SRM Stretch, the SRM sets stretch storage from the protected site to the recovery site. Then, the SRM uses the vSphere vMotion function to migrate protected VMs in the SPPG to the recovery site. The services of the protected VMs are not interrupted during the process.

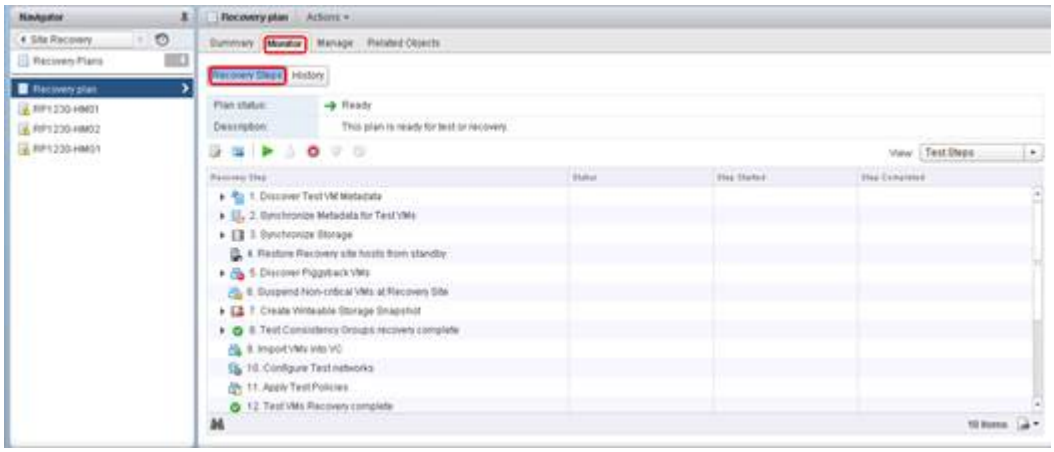
Procedure

Step 1 Log in to the VMware vSphere Web Client at the protected site and click **Site Recovery**.

Step 2 Choose **Recovery Plans** from the navigation tree.

Step 3 Select the desired recovery plan.

Step 4 Click the **Monitor** tab and then the **Recovery Steps** tab.



Step 5 Click .

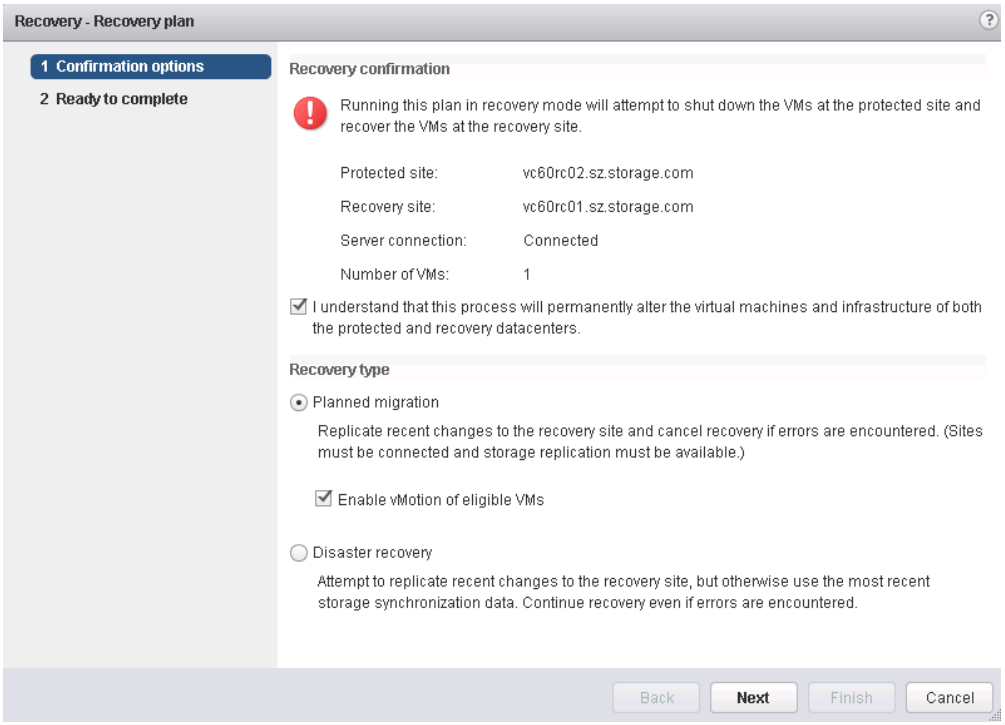
Step 6 Set parameters.

- Select **I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datascenters**.
- Select **planned migration**.
- Select **Enable vMotion of eligible VMs**.

  If **Enable vMotion of eligible VMs** is not selected, the following error message will be displayed when the recovery plan is being executed:

  Failed to sync data on replica devices. Cannot process device '2102350BSJ10EC0000002_31_MP_643e8c32a9540000' with role 'target' when expected device with role 'source'

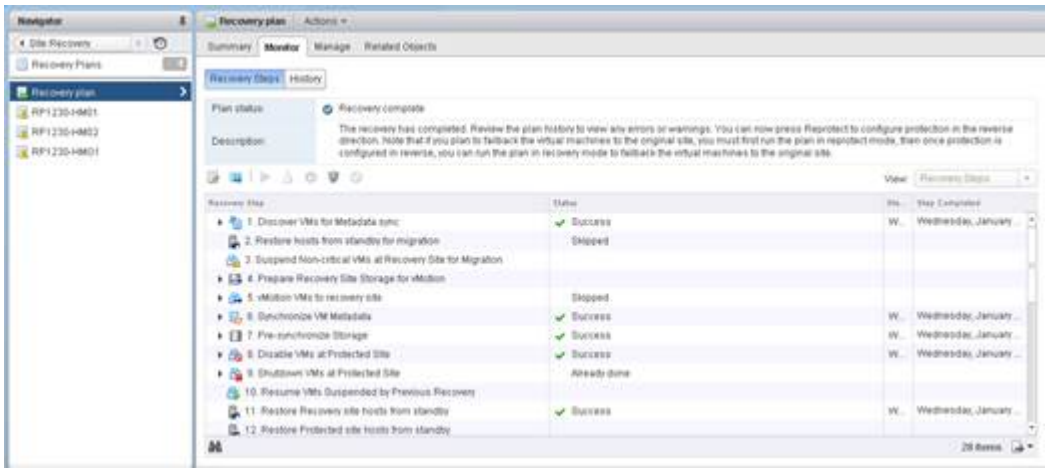
  For the solution, see section 1.1 "System Displays an Error Message During a Planned Migration."



Step 7 Click **Next**.

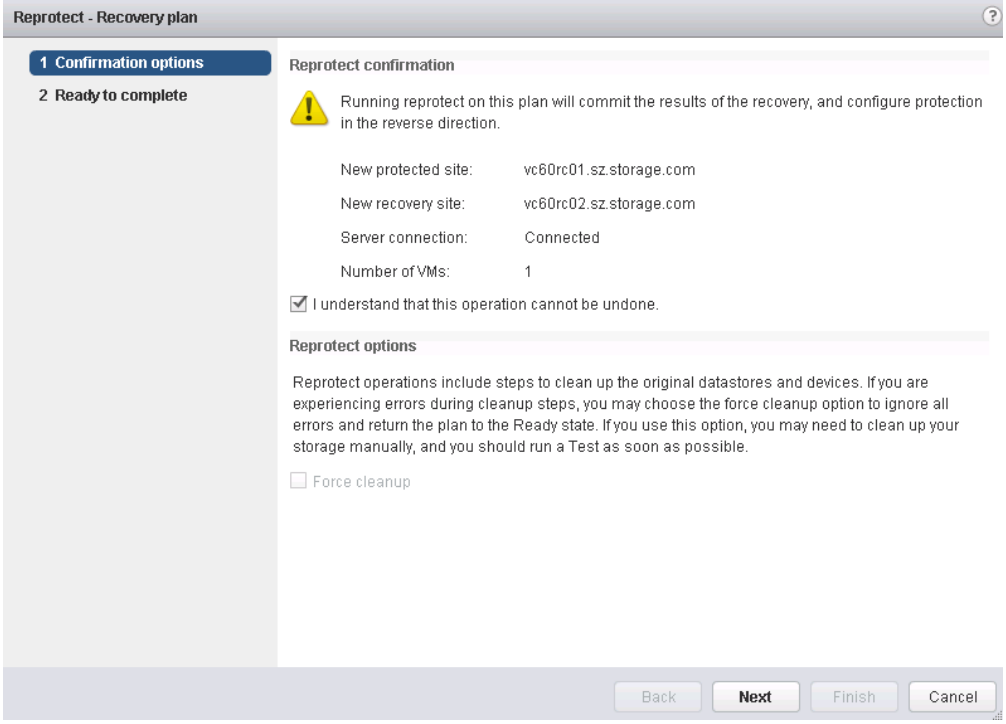
Step 8 Click **Finish**.

After the planned migration is completed, the page shown in the following figure is displayed.



Step 9 After the planned migration is completed, click to reprotect the recovery site as the protected site.

1. Select **I understand that this operation cannot be undone** and click **Next**.



2. Click **Finish**.

----End

NOTICE

In SRM Stretch scenarios, if the planned recovery fails, the primary/secondary relationship of the HyperMetro pair may change, resulting in an inconsistency between the primary/secondary relationship of the HyperMetro pair and that of the sites. An administrator needs to decide whether to perform prior/non-prior switchover on the HyperMetro pair.

5.3 Disaster Recovery

Scenario Identification

Disaster recovery is performed when services are interrupted due to a disaster, component fault, or network interruption. During the disaster recovery, services are interrupted.

Disaster recovery is performed in the following cases:

- An unforeseeable disaster (such as an earthquake) happens, causing damage to a data center site.
- An unplanned power system or network breakdown of a data center causes the data center site to become unavailable.
- A key component of the protected site, such as the ESXi host (vCenter), SRM server, or storage array, is faulty.

Scenario Analysis

There are two cases based on whether VMs support SRM Stretch:

- If VMs do not support SRM Stretch, VMs in a protection group restart at the recovery site.
- If VMs support SRM Stretch, the SRM sets stretch storage from the protected site to the recovery site. Then, VMs in a protection group restart at the recovery site.

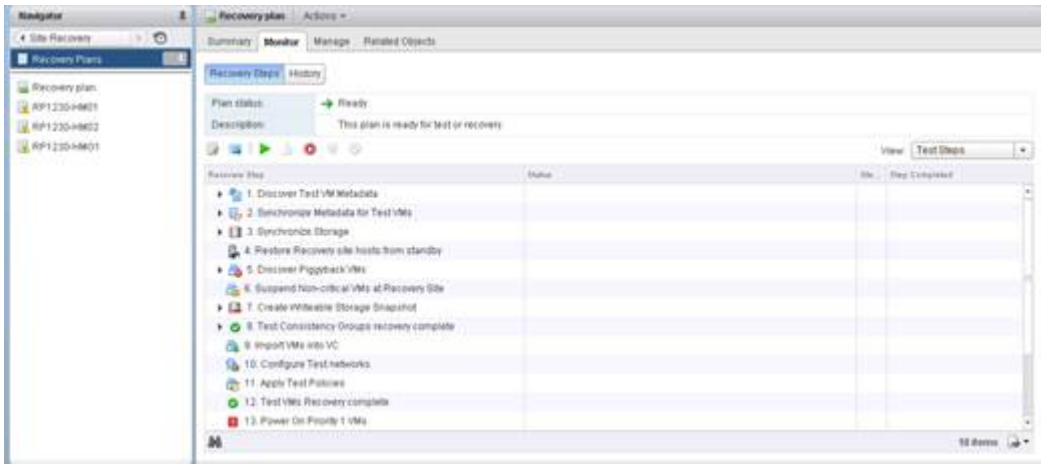
Procedure

Step 1 Log in to the VMware vSphere Web Client at the protected site and click **Site Recovery**.

Step 2 Choose **Recovery Plans** from the navigation tree.

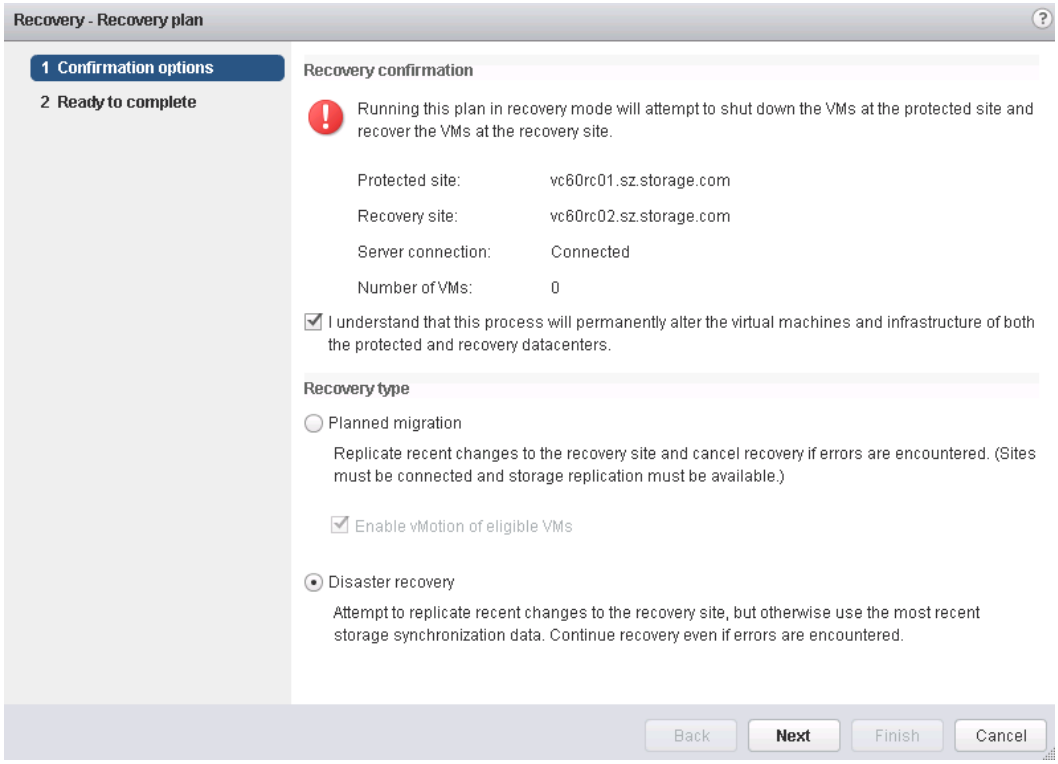
Step 3 Select the desired recovery plan.

Step 4 Click the **Monitor** tab and then the **Recovery Steps** tab.



Step 5 Click .

Step 6 Select **I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datascenters** and **Disaster recovery**.



Step 7 Click **Next**.

Step 8 Click **Finish**.

Step 9 After the disaster recovery is complete, click to reprotect the recovery site as the protected site.

NOTICE

- Before reprotecting the recovery site as the protected site, refresh device information on the storage array manager. Otherwise, the reprotection task may fail.
- In the geo-redundant DR scenario, if data center B is faulty and users forcibly switch services from data center A to data center C, data loss may occur.

----End

5.4 Switchback

Scenario Identification

A switchback means that users perform recovery operations to switch services back to the original protected site when the protected site recovers.

Scenario Analysis

There are two cases based on whether storage arrays support SRM Stretch:

- If storage arrays do not support SRM Stretch, the SRM shuts down all VMs at the protected site. After data synchronization is complete, all VMs are restarted at the original protected site.
- If storage arrays support SRM Stretch, the SRM sets stretch storage from the protected site to the recovery site. Then, the SRM uses the vSphere vMotion function to migrate protected VMs in the SPPG to the protected site. The services of the protected VMs are not interrupted during the process.

Prerequisites

A planned migration or disaster recovery is complete.

Procedure

Step 1 Switch services from the current protected site back to the original protected site. For details, see section **6.2 "Planned Migration**."

Step 2 Click to reprotect the original protected site.

----End

6 Uninstalling SRA

6.1 Uninstalling SRA in a Windows Environment

6.2 Uninstalling SRA in the SRM VA Environment

6.1 Uninstalling SRA in a Windows Environment

Prerequisites

SRM does not use any resources of the storage system. To check whether RSM uses any resources of the storage system, log in to the VMware vSphere Web Client and check the SRM running information.

Context

The SRA software of both the production site and DR site must be uninstalled.

Procedure

Step 1 Log in to the SRA server as an administrator.

Step 2 Choose **Start** > **Huawei** and click **Uninstall eSDK_Stroage_SRA**.

The operating system enters the SRA uninstallation process.

The SRA uninstallation takes 1 to 3 minutes.

----End

6.2 Uninstalling SRA in the SRM VA Environment

Prerequisites

SRM does not use any resources of the storage system. To check whether RSM uses any resources of the storage system, log in to the VMware vSphere Web Client and check the SRM running information.

 Copyright © Huawei Technologies Co., Ltd.

Context

The SRA software of both the production site and DR site must be uninstalled.

Procedure

Step 1 Log in to the SRM management GUI as user **admin**. The login address is **https://** *<SRM server IP address>***:5480**.

Step 2 Click **Storage Replicaiton Adapters**. The SRA plug-in management GUI is displayed.

Step 3 Select the SRA plug-in to be deleted and click **Delete**.

----End

 Copyright © Huawei Technologies Co., Ltd.

7 Troubleshooting

SRA Logs in a Windows Environment

- SRA logs are stored in directory **C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\logs\SRAs\eSDK_Storage_SRA**.

  NOTICE

  ProgramData is a hidden folder. Before obtaining logs, unhide **ProgramData**.

- Log description: The current log file is **log.txt** and the historical log file is **log.txt***N*, where *N* can be **1**, **2**, **3**, or **4**. A maximum of four SRA log files can be retained. The bigger the value of *N* is, the earlier the corresponding log file is generated.
- Log size: The maximum size of a log file is 100 MB.
- SRM logs are stored in directory **C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\logs**.

SRA Logs in the SRM VA Environment

- SRA logs are stored in directory **/var/log/vmware/srm/SRAs/**.
- Log description: The current log file is **log.txt** and the historical log file is **log.txt***N*, where *N* can be **1**, **2**, **3**, or **4**. A maximum of four SRA log files can be retained. The bigger the value of *N* is, the earlier the corresponding log file is generated.
- Log size: The maximum size of a log file is 100 MB.
- SRM logs are stored in directory **/var/log/vmware/srm**.

 Copyright © Huawei Technologies Co., Ltd.

8 FAQ

8.1 System Displays an Error Message During a Planned Migration

8.2 Cleanup Lock Failure

8.3 Reprotection Failure

8.4 A Reprotection Task Fails During Remote Replication

8.5 Shutting Down the VM at the Protected Site Fails

8.6 vCenter Cannot Detect the Installed SRA Plug-in

8.7 No Result Is Returned for a Planned Migration

8.8 Failed to Execute Planned Fault Recovery or Test a Recovery Plan

8.9 "Recovered device xxx not found after HBA rescan" Is Displayed When the Recovery Plan Fails to Be Tested

8.10 A File Copy Error Is Displayed During a Planned Migration or DR

8.11 No Datastore Can Be Found During Data Center Switchback in the Geo-redundant DR Scenario

8.12 A Placeholder Error Occurs During Reprotection

8.1 System Displays an Error Message During a Planned Migration

Symptom

During a planned migration, **Enable vMotion of eligible VMs** is not selected. The system displays the error message "Failed to sync data on replica devices. Cannot process device '2102350BSJ10EC0000002_31_MP_643e8c32a9540000' with role 'target' when expected device with role 'source'."

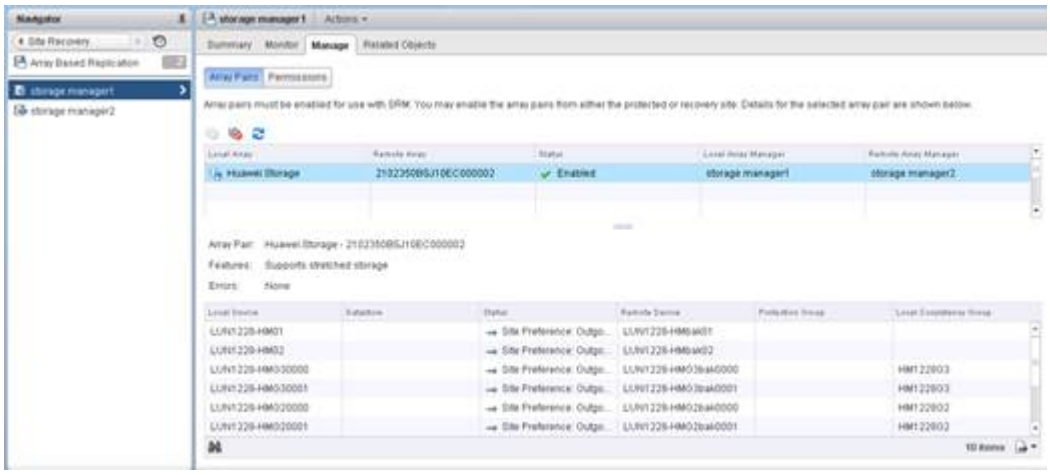
 Copyright © Huawei Technologies Co., Ltd.

Solution

Step 1 Log in to the VMware vSphere Web Client and click **Site Recovery**.

Step 2 Choose **Array Based Replication** from the navigation tree.

Step 3 Select the array manager and click.



----End

8.2 Cleanup Lock Failure

Symptom

In an active/standby disaster recovery solution, cleanup lock failure information appears in the task list of a disaster recovery test, planned migration, or disaster-triggered migration.

Solution

Ignore the failure information because it does not affect the disaster recovery test, planned migration, or disaster-triggered migration.

8.3 Reprotection Failure

Symptom

In an active/standby disaster recovery solution, the storage array at the protected site is faulty and is restarted. After the disaster recovery is complete, the recovery site fails to be reprotected as the protected site. The following figure shows the failure information.

Recovery Step	Result
1. Restore Protected site hosts from standby	Success
2. Configure Storage to Reverse Direction	Error - Failed to reverse replication for failed over devices. Cannot process device '2102350BSJ10EC000002_46_RP_643e8c40e36d0015' with role 'target' when expected device with role 'promotedTarget'.
2.1. Protection Group PG226-P02	Error - Failed to reverse replication for failed over devices. Cannot process device '2102350BSJ10EC000002_46_RP_643e8c40e36d0015' with role 'target' when expected device with role 'promotedTarget'.
2.1.1. Configure Array-based Storage	Error - Failed to reverse replication for failed over devices. Cannot process device '2102350BSJ10EC000002_46_RP_643e8c40e36d0015' with role 'target' when expected device with role 'promotedTarget'.

Solution

Update the storage array manager and execute reprotection again. The procedure is as follows:

Step 1 Log in to the VMware vSphere Web Client and click **Site Recovery**.

Step 2 Choose **Array Based Replication** from the navigation tree.

Step 3 On the **Object** tab page, click.

----End

8.4 A Reprotection Task Fails During Remote Replication

Symptom

During remote replication, a network fault occurs between the storage arrays at the protected site and recovery site. After the environment is recovered and disaster recovery is complete, a reprotection task is executed with the device information on the storage array manager being not refreshed. The following error message is displayed:

"A storage operation requested on unknown consistency group 'XXX'. Failed to reverse replication for failed over device."

Solution

- For SRM 5.5 devices, re-create a recovery plan as follows:
  a. On the VMware vSphere Web Client, delete the existing recovery plan.
  b. On a storage array, perform a switchover between the primary and secondary ends in the remote replication pair to change the original recovery site to the protected site, and synchronize data.
  c. On the VMware vSphere Web Client, re-create a recovery plan.
- For SRM 6.1 devices, refresh the storage array manager and execute the reprotection task again.

8.5 Shutting Down the VM at the Protected Site Fails

Symptom

A VM is deployed in a data store that contains multiple LUNs. The service network is disconnected between the protected site and the ESX server. During disaster

recovery, shutting down the VM at the protected site times out. After the environment is recovered, disaster recovery is performed again. Shutting down the VM at the protected site fails during the disaster recovery. The system displays a message indicating that VMware tools are not running on the VM.

Solution

Manually shut down the VM at the protected site, and continue with the disaster recovery.

8.6 vCenter Cannot Detect the Installed SRA Plug-in

Symptom

The SRA plug-in has been installed. However, when a user attempts to manually refresh SRA information on the VMware vSphere Web Client, the system displays the message "No SRAs have been installed.".

Solution

Restart the vCenter Server.

8.7 No Result Is Returned for a Planned Migration

Symptom

During a planned migration, the servers where the vCenter Server and SRM are located shut down unexpectedly. Consequently, no result is returned for the planned migration.

Solution

Cancel the planned migration. After the environment is recovered, perform the planned migration again.

8.8 Failed to Execute Planned Fault Recovery or Test a Recovery Plan

Symptom

During the execution of planned fault recovery or recovery plan testing, "Failed to recover datastore XXX, VMFS volume residing on recovered devices XXX cannot be found." is displayed, as shown in the following figure.

```
Error - Failed to recover datastore "Datastore-duolun" ⌄  VMFS volume residing on recovered
devices ""258qaz963wsx741edc01_3013_RP_84ad589336ae0002",
"258qaz963wsx741edc01_3014_RP_84ad589336ae0009",
"258qaz963wsx741edc01_3015_RP_84ad589336ae0003",
"258qaz963wsx741edc01_3016_RP_84ad589336ae0004",
"258qaz963wsx741edc01_3017_RP_84ad589336ae0005",
"258qaz963wsx741edc01_3018_RP_84ad589336ae0006",
"258qaz963wsx741edc01_3019_RP_84ad589336ae0007",
"258qaz963wsx741edc01_3020_RP_84ad589336ae0008"" cannot be found⌄
```

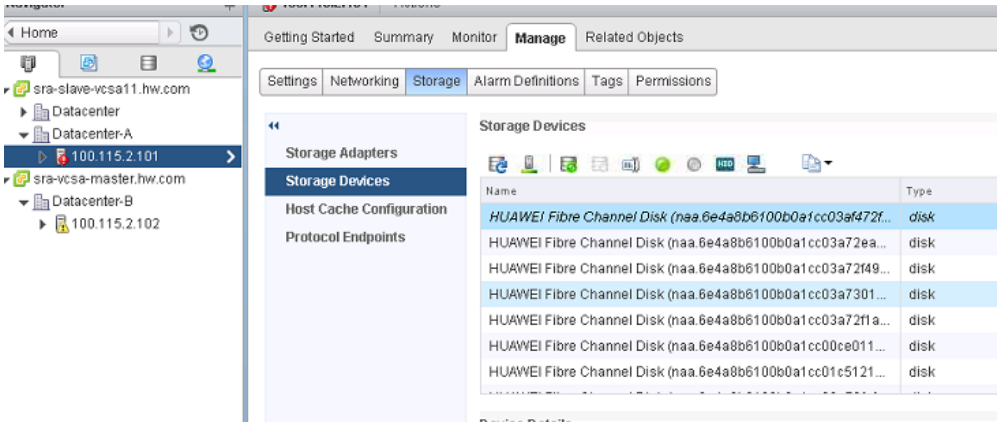
Solution

Re-scan the HBA of the storage and perform the planned recovery or test the recovery plan.

Step 1 Log in to the VMware vSphere Web Client and choose **Hosts and Clusters**.

Step 2 In the navigation tree, select the host at the recovery site.

Step 3 Click **Manage**, and choose **Storage** > **Storage Devices**, and click.



Step 4 Perform the planned recovery or test the recovery plan again.

----End

8.9 "Recovered device xxx not found after HBA rescan" Is Displayed When the Recovery Plan Fails to Be Tested

Symptom

During a recovery plan test, an error is displayed indicating that datastore xxx cannot be restored, the VMFS volume residing on the restored device xxx cannot be detected, and the to-be-restored device cannot be found after HBA card rescan, as shown in the following figure.

Error - Failed to recover datastore 'danlun-2'. VMFS volume residing on recovered devices '"123adb456sd789ad789f_53_MP_8038bc1866540000"' cannot be found. Recovered device '123adb456sd789ad789f_53_MP_8038bc1866540000' not found after HBA rescan.

Solution

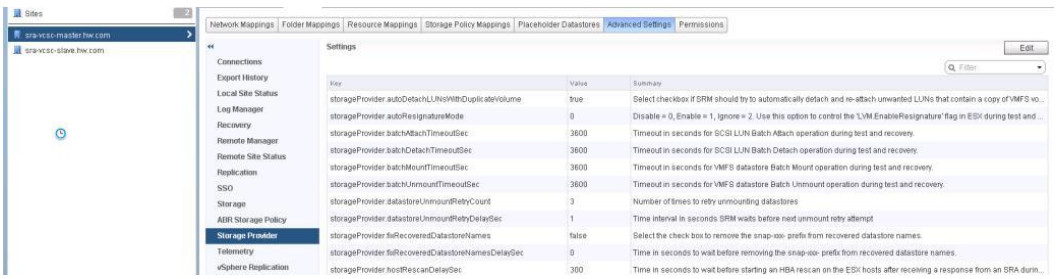
Reconfigure **storageProvider.hostRescanTimeoutSec** (scanning timeout duration of the host managed by SRM) and test the recovery plan again.

Step 1 Log in to the VMware vSphere Web Client and click **Site Recovery**.

Step 2 In the navigation tree, select **Sites**.

Step 3 In the navigation tree, select a protected site, for example, sra-vcsc-master.hw.com.

Step 4 On the page that is displayed, click **Manage**, choose **Advanced Settings** > **Storage Provider**, and click **Edit**



Step 5 Set **storageProvider.hostRescanTimeoutSec**. The recommended value is **500.**

Step 6 Click **OK** to save the settings.

Step 7 Repeat steps 2 to 6 on the other site.

Step 8 Test the recovery plan again.

----End

8.10 A File Copy Error Is Displayed During a Planned Migration or DR

Symptom

During a planned migration or DR, an error indicating that "Failed to copy file xxxx.vmx" is displayed, as shown in the following figure..

Error - Failed to copy file '[danlun-2] danlun-2/danlun-2.vmx' to 'C:\Windows\TEMP\vmware-SYSTEM\danlun-2.vmx-ps-5.tmp85': 4 - A file error was encountered.

Solution

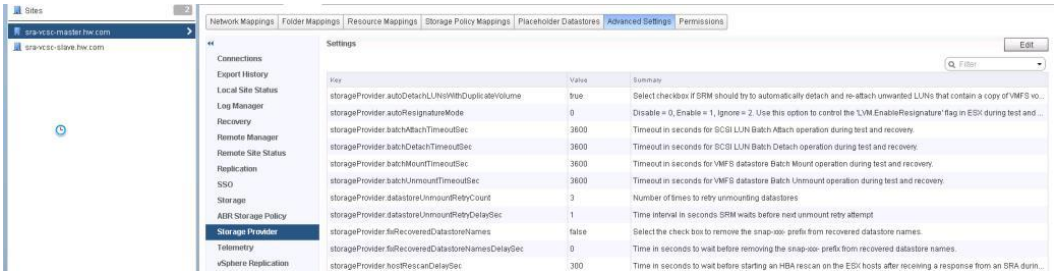
Reconfigure **storageProvider.hostRescanDelaySec** and **storageProvider.hostRescanRepeatCnt**, and perform the planned migration or DR again.

Step 1 Log in to the VMware vSphere Web Client and select **Site Recovery**.

Step 2 In the navigation tree, select **Sites**.

Step 3 In the navigation tree, select a protected or recovery site, for example, sra-vcsc-master.hw.com.

Step 4 On the page that is displayed, click **Manage**, choose **Advanced Settings > Storage Provider**, and click **Edit**.



Step 5 Set **storageProvider.hostRescanDelaySec** and **storageProvider.hostRescanRepeatCnt.** The recommended values are 300 and 2, respectively.

Step 6 Click **OK** to save the settings.

Step 7 Repeat steps 2 to 6 on the other site.

Step 8 Perform the planned recovery or DR again.

----End

8.11 No Datastore Can Be Found During Data Center Switchback in the Geo-redundant DR Scenario

Symptom

In the geo-redundant DR scenario, when data center C is switched back to data center B, a message is displayed indicating that no datastore cannot be found. The error message is as follows:

```
Error-Some virtual machines in the protection group 'xxx-group' could not be recovered Failed to recover
datastore 'snap-05e8bc88-datastore'. VMFS volume residing on recovered devices
'"xxxxxxxxxxxxxxxx_xx_RP_xxxxxxxxx"' cannot be found.
```

Solution 1

Perform the following operations on storage arrays:

Step 1 Log in to **https://support.huawei.com** and search for **HyperMetro Configuration Guide for Huawei SAN Storage Using OS Native Multipathing Software**.

Step 2 Configure VMware multipathing by referring to chapter "VMware."

----End

Solution 2

Perform the following operations on VMs. In this solution, multipathing is fixed at data center B. The procedure is as follows:

Step 1 Find **Storage Devices** corresponding to snap-05e8bc88-datastore in host cluster A.

Step 2 Click the **Properties** tab.

Step 3 Click **Edit Multipathing**.

Step 4 Set **Path selection policy**.

By default, By default, VMware supports the following path selection policies: If a third-party PSP is installed on the host, its policy is also displayed in the list.

- Fixed (VMware)
- Most Recently Used (VMware)
- Round Robin (VMware)

Step 5 Select **Fixed (VMware)** and specify the preferred path to data center B.

Step 6 Click **OK** to save the settings and exit the dialog box.

----End

8.12 A Placeholder Error Occurs During Reprotection

Symptom

In the active/standby redundancy, "Protection group '***' has protected VMs with placeholders which need to be repaired" is reported during reprotection.

Solution

Perform the reprotection operation again and select the items you want to forcibly clear.

 Copyright © Huawei Technologies Co., Ltd.