Configuring SRM 8.7 Stretched Storage Certification with Hitachi Ops Center Protector SRA 5.0.1 on a VSP Storage System using GAD

v1.0

Implementation Guide

This guide provides instructions for configuring and implementing a stretched storage certification using Hitachi SRA 5.0.1 to certify VMware SRM 8.7 on VMware ESXi using Hitachi Global-Active Device (GAD), managed through Ops Center Protector.

MK-SL-354-00

Hitachi Vantara

June 2025

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at https://support.HitachiVantara.com/ en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and
2) Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

Table of Contents

Preface

About this document

This guide shows how to set up VMware Site Recovery Manager (SRM) 8.7 using Storage Replication Adapter (SRA) 5.0.1 on VMware ESXi hosts with Hitachi Global-Active Device (GAD) managed through Hitachi Ops Center Protector.

Intended audience

This document is intended for technical audiences responsible for configuring and managing disaster recovery solutions using SRA and SRM to automate failover, failback, and replication management.

To use this document, you must be familiar with VMware vSphere, SRM, SRA, GAD, and VSP storage systems.

Revision History

Revision	Changes	Date
v1.0	Initial Release	June 2025

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: https://support.hitachivantara.com/.

Log in and select Product Downloads to access the most current downloads, including updates that may have been made after the release of the product.

Getting Help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to GPSE-Docs-Feedback@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Introduction

VMware Site Recovery Manager (SRM) automates disaster recovery by replicating and recovering virtual machines across data centers. Paired with Hitachi Global-Active Device (GAD), SRM enables zero-downtime failover.

Purpose

The purpose of this document is to provide step-by-step instructions for SRM 8.7 with Storage Replication Adapter (SRA) 5.0.1 on VMware ESXi, using GAD managed through Ops Center Protector. This setup is designed for organizations seeking a reliable disaster recovery solution that minimizes downtime and data loss across geographically dispersed sites.

Connectivity Block Diagram

The following connectivity diagram illustrates the setup of SRM for a stretched storage certification, using SRA on VMware ESXi hosts with GAD managed through Ops Center Protector.

The setup includes two ESXi Hosts, one for primary host A and another for secondary host B, along with Ops Center Protector connected to both the Virtual Storage Platform (VSP) primary and secondary sites. An external VSP storage system is configured with GAD to enable real-time data replication, ensure high availability, and support disaster recovery between the primary and secondary storage systems.

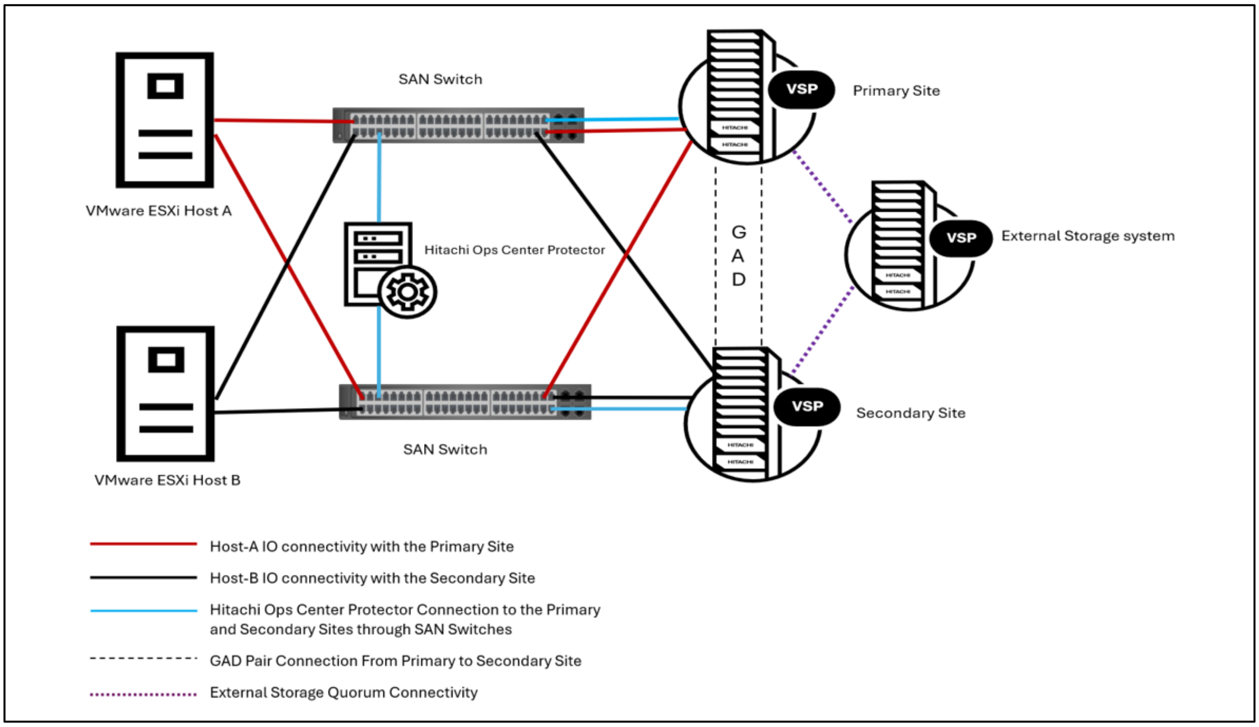

SAN Switch
VSP
Primary Site
VMware ESXi Host A
Hitachi Ops Center Protector
G
A
D
VSP
External Storage system
VSP
Secondary Site
SAN Switch
VMware ESXi Host B
Host-A IO connectivity with the Primary Site
Host-B IO connectivity with the Secondary Site
Hitachi Ops Center Protector Connection to the Primary and Secondary Sites through SAN Switches
GAD Pair Connection From Primary to Secondary Site
External Storage Quorum Connectivity

Figure 1: SRM 8.7 with SRA and GAD connectivity overview

Hardware Requirements

The following lists the hardware requirements:

- Two compatible VSP storage systems with support for GAD configuration, and an external VSP storage system for replicating data.
- VMware ESXi servers at both primary and secondary sites.
- Supported Fibre Channel (FC) HBA.
- High-speed network connectivity between the primary and secondary sites for replication and failover operations.
- Enterprise-grade FC/Ethernet switches (such as Cisco or Brocade) that support high-speed, low-latency connections between the host and storage sites.

Software Requirements

The following lists the software requirements:

- vSphere client version: Version 6.7.0
- VMware VCSA: Version 8.0.1-21560480 compatible with SRM 8.7
- VMware SRM: Version 8.7, including license information and supported features
- Hitachi SRA: Version 5.0.1, with installation requirements and version compatibility
- Hitachi Ops Center Protector: Version 7.8.0
- OS install media: ESXi 8.0U1

Installing VMware vCenter Server Appliance (VCSA)

The VMware vCenter Server Appliance (VCSA) is a preconfigured Linux-based virtual machine optimized for managing VMware ESXi hosts. This section shows how to deploy and configure VCSA as part of the SRM 8.7 environment setup.

Prerequisites

- VMware ESXi host running version 7.x or later
- Network connectivity with DNS, NTP, and IP configurations
- VCSA ISO file from VMware official website - VCSA Download URL
- Administrator access to the ESXi host for deployment
- Properly configured DNS records for forward and reverse lookup of the vCenter Server hostname
- The following three VCSAs had been configured in this test environment with the respective names as follows:
    - vcsaext.vmcert.com → Master VCSA
    - vcsapro81.vmcert.com → Protected Site A VCSA
    - vcsarec81.vmcert.com → Recovery Site B VCSA

Preparing the Environment

1. Configure DNS:
    a. Ensure that a fully qualified domain name (FQDN) is resolvable by DNS.
    b. Verify forward and reverse DNS lookups for the vCenter hostname and IP address.
2. Download VCSA ISO. Obtain the ISO image of VCSA from the VMware Customer Connect portal: https://tap.broadcom.com/docs/-/certkit/Storage-Certification/8.0-8.0U1-8.0U3.
3. Verify NTP configuration. Use a reliable NTP server for time synchronization to avoid clock drift issues.

Deploying and Configuring VCSA

For deploying and configuring the VCSA, refer to the official Broadcom documentation. The process includes:

1. Deploying VCSA on the ESXi host.

2. Accepting the EULA, configuring the target ESXi host, selecting the deployment size, and providing network settings.

3. Configuring the vCenter Server with SSO domain information and setting up the administrator password.

4. Completing the configuration and starting the vCenter services.

Installing VMware Site Recovery Manager

This section shows how to install VMware SRM 8.7 with GAD and Ops Center Protector.

Prerequisites

- VMware vCenter Server installed and configured on both the protected and recovery sites.
- Fully qualified domain names (FQDN) and static IP addresses for SRM servers.
- Ensure SRM servers can communicate with vCenter servers on both sites.
- Open required ports:
    - TCP 443: For vCenter communication
    - TCP 902: For ESXi communication

Installing SRM

For detailed instructions on installing and configuring VMware SRM, see the official VMware installation guide. The process includes:

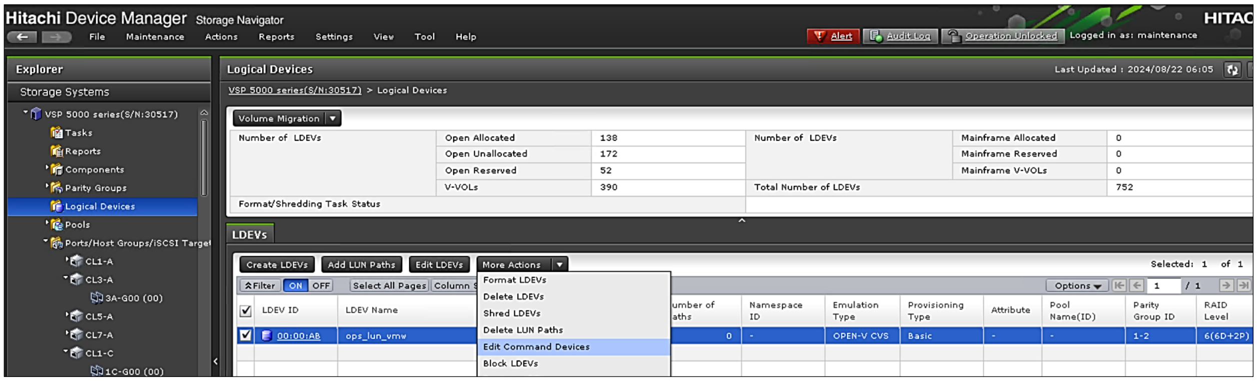
1. Downloading the SRM installer and selecting the appropriate version from the VMware site.
2. Mounting the SRM ISO and accessing the OVF files in the bin directory.
3. Deploying the SRM OVF template through the vSphere Client by selecting the target host and providing necessary configuration details, including VM name, storage, network settings, and password.
4. Completing the installation and powering on the VM.
5. Deploying SRM on the Protected and Recovery Sites (Site A and Site B), ensuring both sites are properly configured with the vCenter Server and necessary SRM appliance settings.

Configuring the Storage System

This section shows how to configure the storage system for installing VMware SRM 8.7 with SRA 5.0.1.

Configuring Command Device

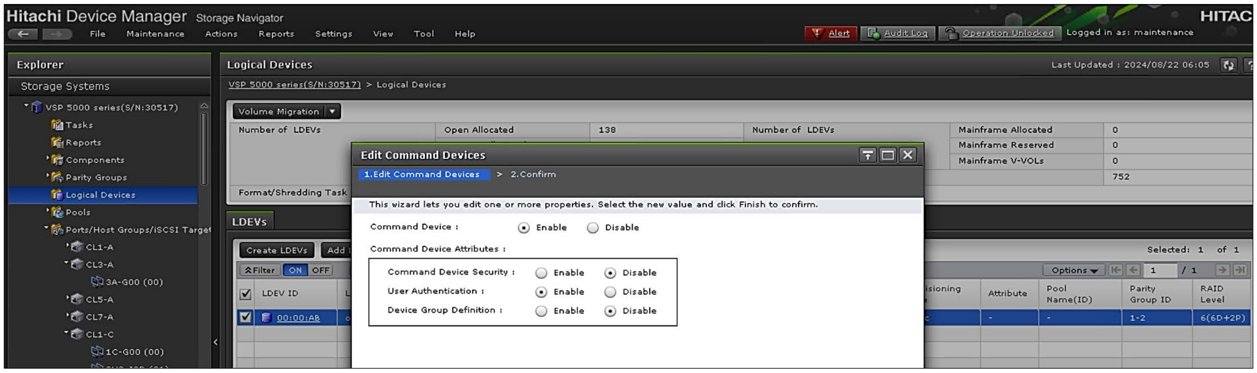
1. Create host groups for all ports on both storage systems.
2. Create two basic 50GB LDEVs on both storage systems for command device.
3. Select the LDEV, navigate to More Actions click Edit Command Devices and edit the LDEVs.



Number of LDEVs	Open Allocated	138	Number of LDEVs	Mainframe Allocated	0
	Open Unallocated	172		Mainframe Reserved	0
	Open Reserved	52		Mainframe V-VOLs	0
	V-VOLs	390	Total Number of LDEVs		752
Format/Shredding Task Status					

☑	LDEV ID	LDEV Name	umber of aths	Namespace ID	Emulation Type	Provisioning Type	Attribute	Pool Name(ID)	Parity Group ID	RAID Level
☑	00:00:AB	ops_lun_vmw	0	-	OPEN-V CVS	Basic	-	-	1-2	6(6D+2P)

4. In the Edit Command Devices window, select **Enable** for Command Device.



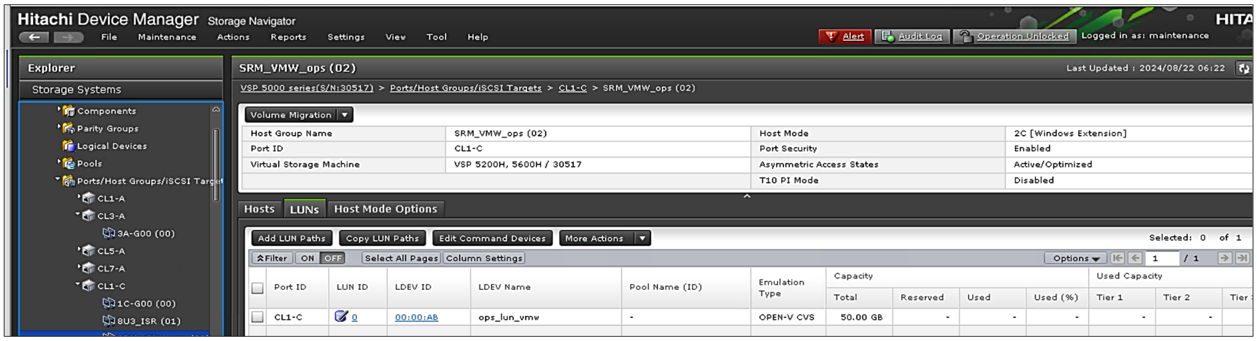
This wizard lets you edit one or more properties. Select the new value and click Finish to confirm.

Command Device : ● Enable ○ Disable

Command Device Attributes :

Command Device Security : ○ Enable ● Disable
User Authentication : ● Enable ○ Disable
Device Group Definition : ○ Enable ● Disable

5. Add the command device to the Host Group that you created.



SRM_VMW_ops (02)

Last Updated : 2024/08/22 06:22

VSP 5000 series(S/N:30517) > Ports/Host Groups/iSCSI Targets > CL1-C > SRM_VMW_ops (02)

Host Group Name	SRM_VMW_ops (02)	Host Mode	2C [Windows Extension]
Port ID	CL1-C	Port Security	Enabled
Virtual Storage Machine	VSP 5200H, 5600H / 30517	Asymmetric Access States	Active/Optimized
		T10 PI Mode	Disabled

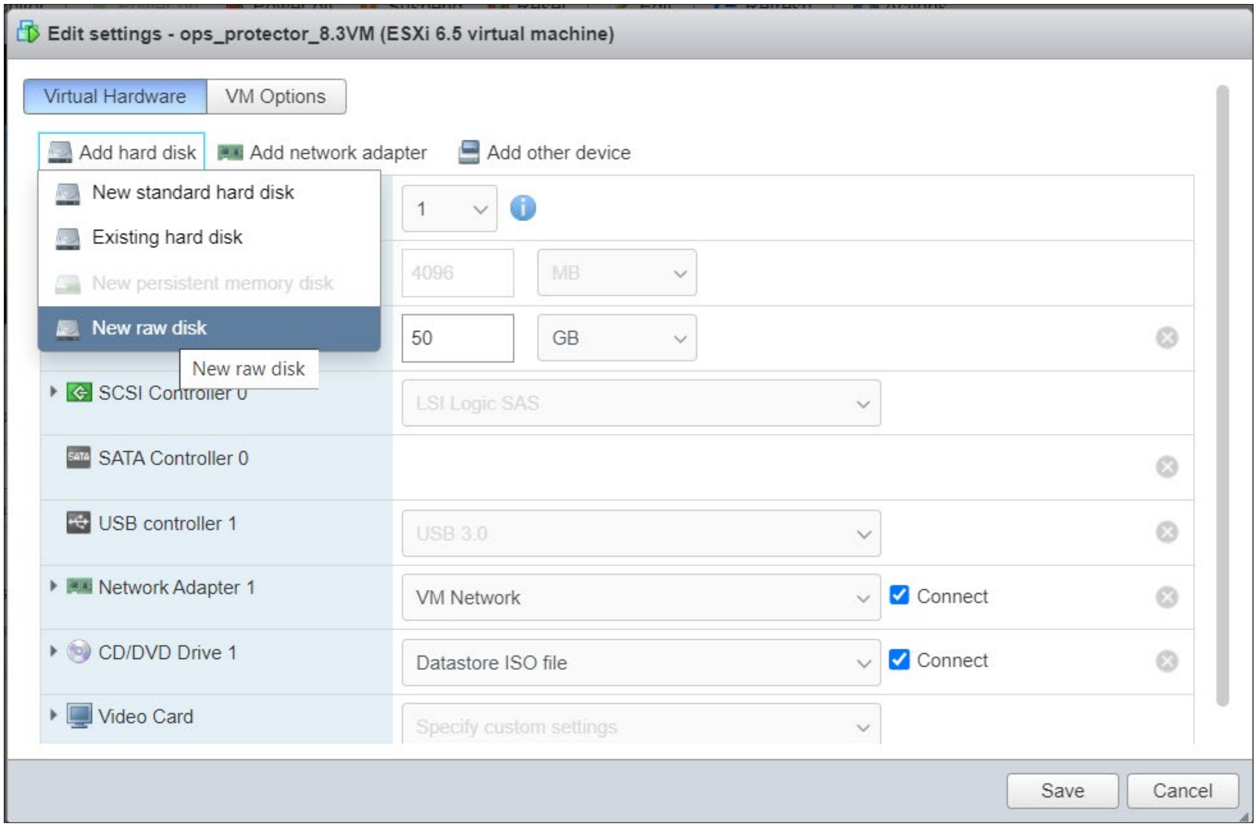
Selected: 0 of 1

□	Port ID	LUN ID	LDEV ID	LDEV Name	Pool Name (ID)	Emulation Type	Capacity				Used Capacity		
							Total	Reserved	Used	Used (%)	Tier 1	Tier 2	Tier
□	CL1-C	0	00:00:AB	ops_lun_vmw	-	OPEN-V CVS	50.00 GB	-	-	-	-	-	

6. Ensure that the command device is zoned to the Ops Center Protector server on a SAN switch.

7. Verify zoning and connectivity between the storage and the ESXi host or management server.

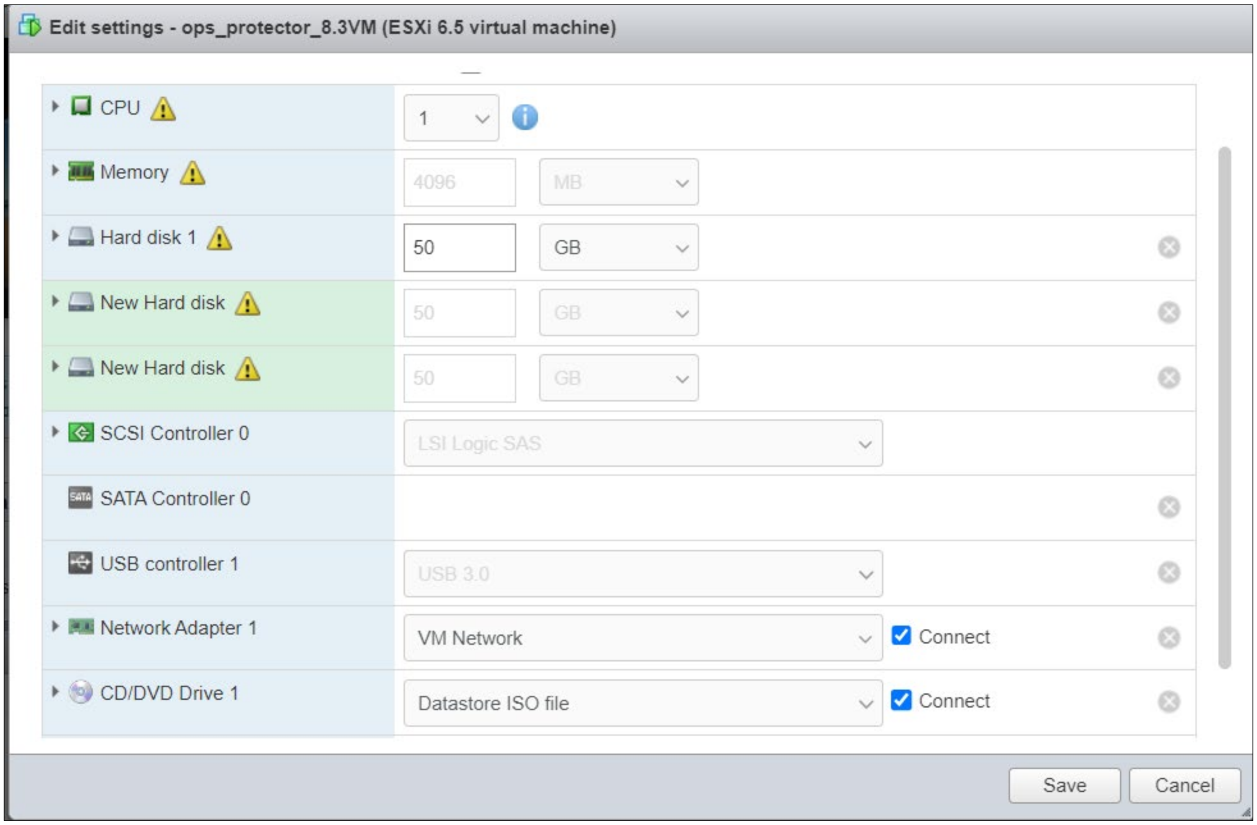
8. Add a new raw Hard Disk to the Ops Center Protector VM based on the configured LUN. Select **Edit Settings** > **Virtual Hardware**, and then click **New raw disk**.



Edit settings - ops_protector_8.3VM (ESXi 6.5 virtual machine)

	1	
	4096 MB	
	50 GB	
SCSI Controller 0	LSI Logic SAS	
SATA Controller 0		
USB controller 1	USB 3.0	
Network Adapter 1	VM Network	☑ Connect
CD/DVD Drive 1	Datastore ISO file	☑ Connect
Video Card	Specify custom settings	

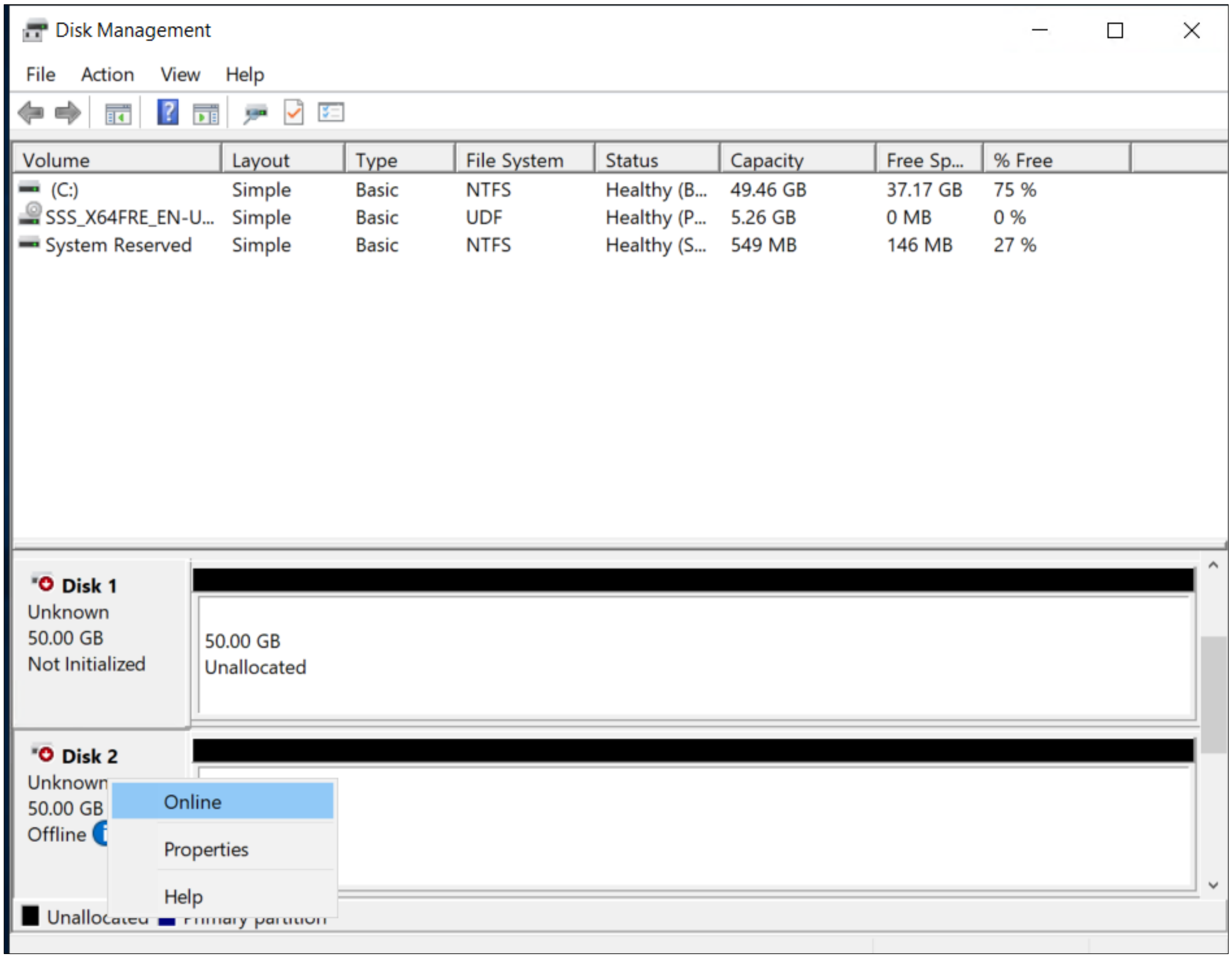
The hard disk is added.



Edit settings - ops_protector_8.3VM (ESXi 6.5 virtual machine)

CPU ⚠	1		
Memory ⚠	4096	MB	
Hard disk 1 ⚠	50	GB	
New Hard disk ⚠	50	GB	
New Hard disk ⚠	50	GB	
SCSI Controller 0	LSI Logic SAS		
SATA Controller 0			
USB controller 1	USB 3.0		
Network Adapter 1	VM Network		☑ Connect
CD/DVD Drive 1	Datastore ISO file		☑ Connect

9. Log in to the VM, select the disk, right click on it, and then click **Online**.



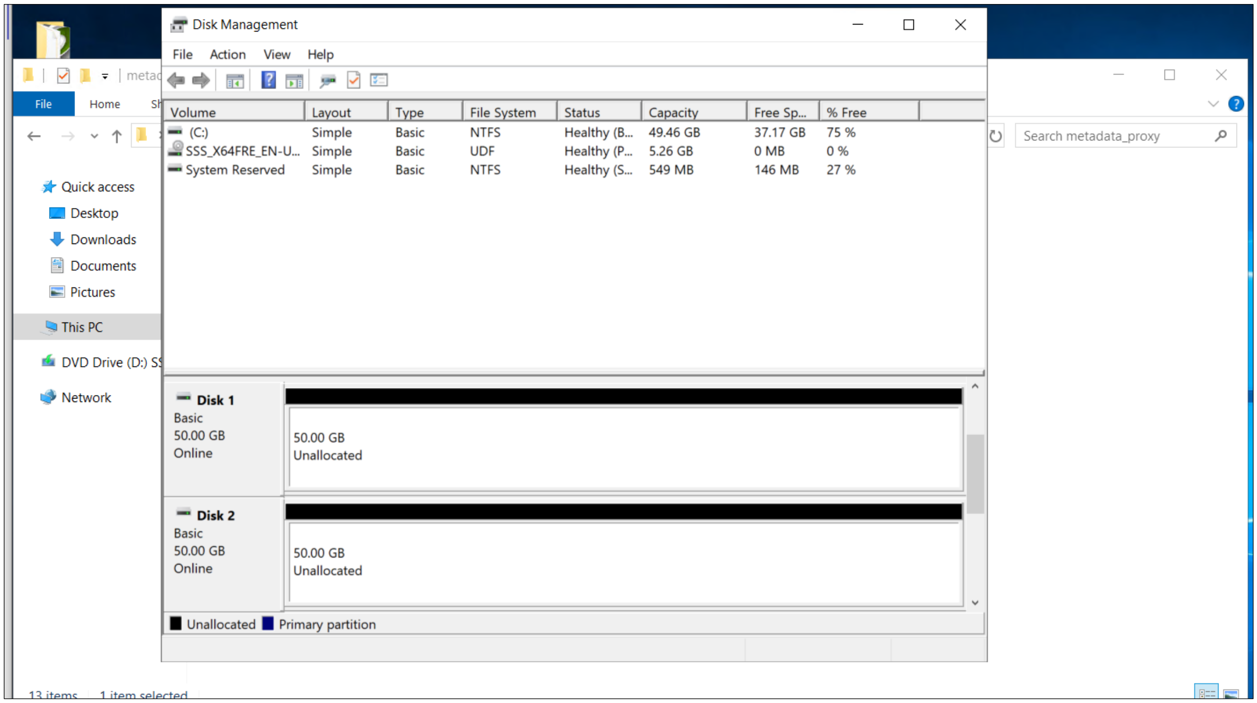
Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	49.46 GB	37.17 GB	75 %
SSS_X64FRE_EN-U...	Simple	Basic	UDF	Healthy (P...	5.26 GB	0 MB	0 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	549 MB	146 MB	27 %

Disk 1
Unknown
50.00 GB
Not Initialized

50.00 GB
Unallocated

Disk 2
Unknown
50.00 GB
Offline

■ Unallocated ■ Primary partition



Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	49.46 GB	37.17 GB	75 %
SSS_X64FRE_EN-U...	Simple	Basic	UDF	Healthy (P...	5.26 GB	0 MB	0 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	549 MB	146 MB	27 %

Disk 1
Basic
50.00 GB
Online

50.00 GB
Unallocated

Disk 2
Basic
50.00 GB
Online

50.00 GB
Unallocated

■ Unallocated ■ Primary partition

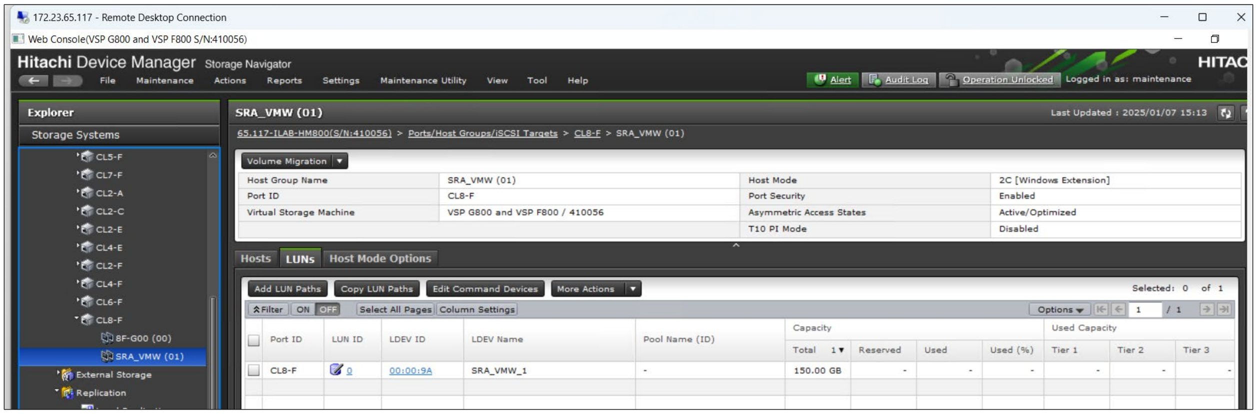
Note: Dynamic Pools must be created on both the primary and secondary storage systems. Verify that zoning is configured on both switches. Set up Host Groups and LUNs to allow each host to access the designated storage system (primary or secondary) through both available paths from both hosts (primary and secondary).

Configuring the External Storage System and Quorum Disk

For detailed instructions, see the Hitachi guide on adding the external storage system for the quorum disk.

1. Map an LDEV from the external storage to the host group of the storage system and set it as a quorum disk. For more details, see the Hitachi documentation for configuring a quorum disk.

2. Create host groups and add them on both the ports of the external storage system. The LDEV is added to the respective host groups, as shown in the following screenshots:



SRA_VMW (01)

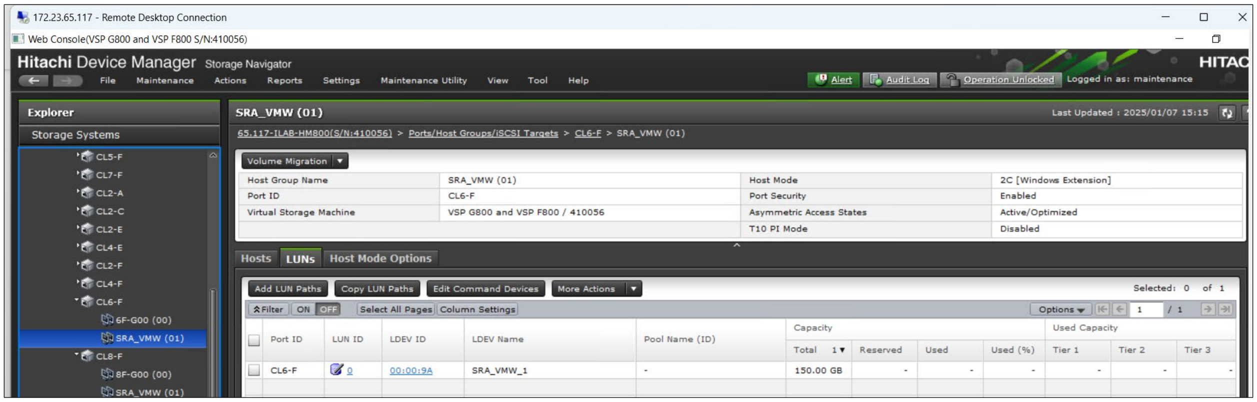
Last Updated : 2025/01/07 15:13

65.117-ILAB-HM800(S/N:410056) > Ports/Host Groups/iSCSI Targets > CL8-F > SRA_VMW (01)

Host Group Name	SRA_VMW (01)	Host Mode	2C [Windows Extension]
Port ID	CL8-F	Port Security	Enabled
Virtual Storage Machine	VSP G800 and VSP F800 / 410056	Asymmetric Access States	Active/Optimized
		T10 PI Mode	Disabled

Selected: 0 of 1

□	Port ID	LUN ID	LDEV ID	LDEV Name	Pool Name (ID)	Capacity				Used Capacity		
						Total 1▼	Reserved	Used	Used (%)	Tier 1	Tier 2	Tier 3
□	CL8-F	0	00:00:9A	SRA_VMW_1	-	150.00 GB	-	-	-	-	-	-



SRA_VMW (01)

Last Updated : 2025/01/07 15:15

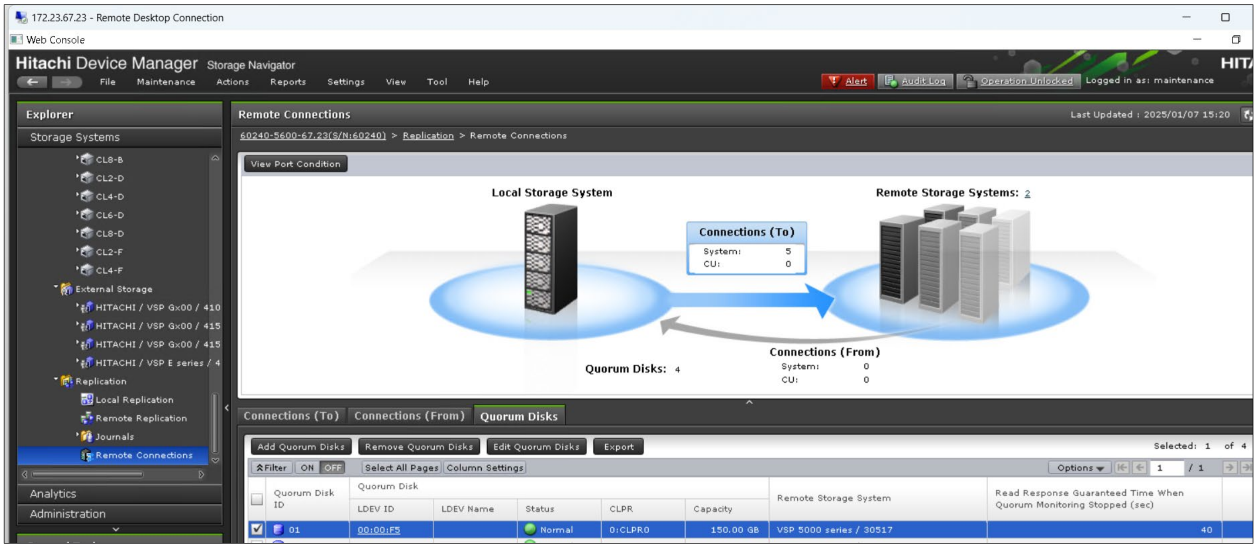
65.117-ILAB-HM800(S/N:410056) > Ports/Host Groups/iSCSI Targets > CL6-F > SRA_VMW (01)

Host Group Name	SRA_VMW (01)	Host Mode	2C [Windows Extension]
Port ID	CL6-F	Port Security	Enabled
Virtual Storage Machine	VSP G800 and VSP F800 / 410056	Asymmetric Access States	Active/Optimized
		T10 PI Mode	Disabled

Selected: 0 of 1

□	Port ID	LUN ID	LDEV ID	LDEV Name	Pool Name (ID)	Capacity				Used Capacity		
						Total 1▼	Reserved	Used	Used (%)	Tier 1	Tier 2	Tier 3
□	CL6-F	0	00:00:9A	SRA_VMW_1	-	150.00 GB	-	-	-	-	-	-

3. Create and specify the quorum disk in the primary storage system.

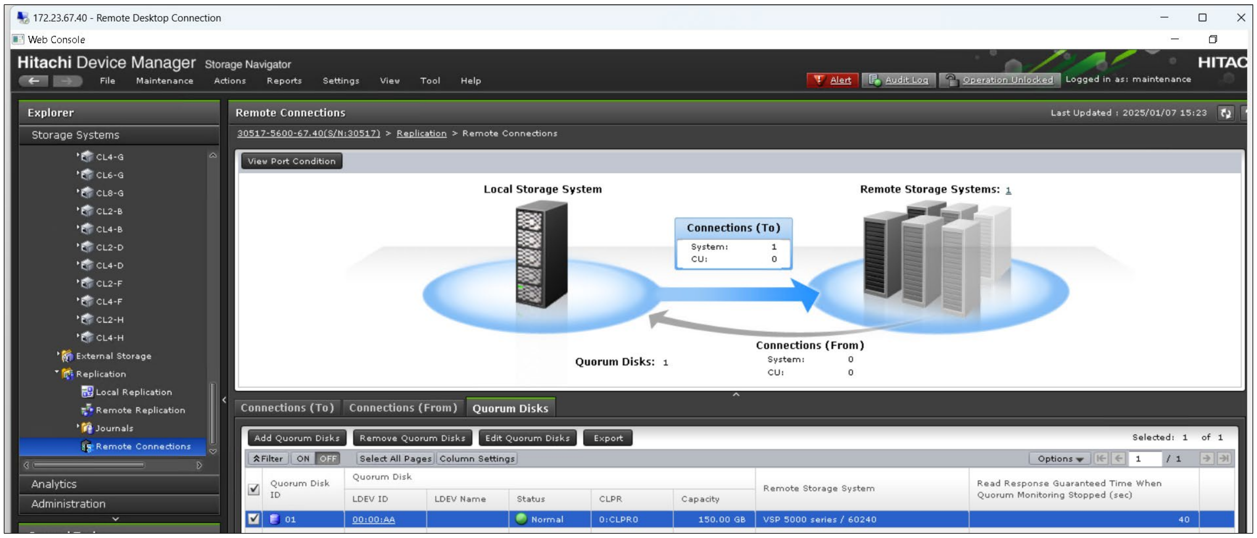


□	Quorum Disk ID	Quorum Disk					Remote Storage System	Read Response Guaranteed Time When Quorum Monitoring Stopped (sec)
		LDEV ID	LDEV Name	Status	CLPR	Capacity		
☑	01	00:00:F5		Normal	0:CLPR0	150.00 GB	VSP 5000 series / 30517	40

Primary storage system Quorum LDEV information:

```
[root@cci~]# raidcom get ldev -ldev_id 00:F5 -fx -IH
Serial#  : 5****5
LDEV : f5
SL : 0
CL : 0
VOL_TYPE : OPEN-V
VOL_Capacity(BLK) : 314572800
NUM_PORT : 0
PORTs :
F_POOLID : NONE
VOL_ATTR : ELUN : QRD
CMP : -
EXP_SPACE : -
E_VendorID : HITACHI
E_ProductID : OPEN-V
E_VOLID :
484954414348492035303430323734383030394100000000000000000000000000000000
E_VOLID_C : HITACHI 50402748009A................
NUM_E_PORT : 1
E_PORTs : CL4-C-0 0 50060e8012274855
LDEV_NAMING :
STS : NML
OPE_TYPE : NONE
OPE_RATE : 100
MP# : 0
ASSIGNED_MP# : 0
SSID : 0004
QRDID : 1
QRP_Serial# : 5****6
QRP_ID : R9
ALUA : Disable
RSGID : 0
PWSV_S : -
CL_MIG : N
[root@cci~]#
```

4. Create and specify the quorum disk in the secondary storage system.



☑	Quorum Disk ID	Quorum Disk					Remote Storage System	Read Response Guaranteed Time When Quorum Monitoring Stopped (sec)
		LDEV ID	LDEV Name	Status	CLPR	Capacity		
☑	01	00:00:AA		● Normal	0:CLPR0	150.00 GB	VSP 5000 series / 60240	40

Secondary storage system Quorum LDEV information:

```
[root@cci~]# raidcom get ldev -ldev_id 00:AA -fx -IH
Serial#  : 5****6
LDEV : aa
SL : 0
CL : 0
VOL_TYPE : OPEN-V
VOL_Capacity(BLK) : 314572800
NUM_PORT : 0
PORTs :
F_POOLID : NONE
VOL_ATTR : ELUN : QRD
CMP : -
EXP_SPACE : -
E_VendorID : HITACHI
E_ProductID : OPEN-V
E_VOLID :
484954414348492035303430323734383030394100000000000000000000000000000000
E_VOLID_C : HITACHI 50402748009A................
NUM_E_PORT : 1
E_PORTs : CL4-C-0 0 50060e8012274875
LDEV_NAMING :
STS : NML
OPE_TYPE : NONE
OPE_RATE : 100
MP# : 0
ASSIGNED_MP# : 0
SSID : 0004
QRDID : 1
QRP_Serial# : 5****5
QRP_ID : R9
ALUA : Disable
RSGID : 0
PWSV_S : -
CL_MIG : N
[root@cci~]#
```

Creating Resource Groups and Adding Resources

1. Create resource groups in both the primary and secondary storage systems:

```
[root@cci~]# raidcom add resource -resource_name SRM_GAD_VMW -virtual_type 55***4 R900G -IH
[root@cci~]# raidcom get resource -key opt -IH
RS_GROUP            RGID   V_Serial#  V_ID   V_IF    Serial#
meta_resource          0      5****5  RH10HG Y        5****5
SRM_GAD_VMW            3      55***4  R9G    Y        5****5
-
[root@cci~]#
[root@cci~]#
[root@cci~]# raidcom add resource -resource_name SRM_GAD_VMW -virtual_type 55***4 R900G -IH
[root@cci~]# raidcom get resource -key opt -IH
RS_GROUP            RGID   V_Serial#  V_ID   V_IF    Serial#
meta_resource          0      5****6  RH10HG Y        5****6
SRM_GAD_VMW            5      55***4  R9G    Y        5****6
```

2. Create a 10 GB basic LDEV on both the primary and secondary storage systems to create the placeholder datastore for the SRM operation.

3. Assign the LDEVs to the resource group by running the following commands:

```
[root@cci~]# raidcom unmap resource -ldev_id 00:E8 -virtual_ldev_id 00:E8 -IH
[root@cci~]# raidcom add resource -resource_name SRM_GAD_VMW -ldev_id 00:E8
-IH
[root@cci~]# raidcom map resource -ldev_id 00:E8 -virtual_ldev_id 00:E8 -IH
[root@cci~]#
[root@cci~]#
[root@cci~]# raidcom unmap resource -ldev_id 00:05 -virtual_ldev_id 00:05 -IH
[root@cci~]# raidcom add resource -resource_name SRM_GAD_VMW -ldev_id 00:05 -IH
[root@cci~]# raidcom map resource -ldev_id 00:05 -virtual_ldev_id 00:05 -IH
[root@cci~]#
```

Creating LDEVs for the Block Host and GAD Replication

1. Create a 50 GB Thin LDEV on the primary site for the block host:

```
[root@cci~]# raidcom get ldev -ldev_id 00:F6 -fx -IH
Serial#  : 5****5
LDEV : f6
SL : 0
CL : 0
VOL_TYPE : OPEN-V-CVS
VOL_Capacity(BLK) : 104857600
NUM_LDEV : 1
LDEVs : 0
NUM_PORT : 0
PORTs :
F_POOLID : NONE
VOL_ATTR : CVS
CMP : NA
EXP_SPACE : R
RAID_LEVEL  : RAID6
RAID_TYPE   : 6D+2P
NUM_GROUP : 1
RAID_GROUPs : 01-01
DRIVE_TYPE  : SNR5A-R3R8NC
DRIVE_Capa : 7500000062
```

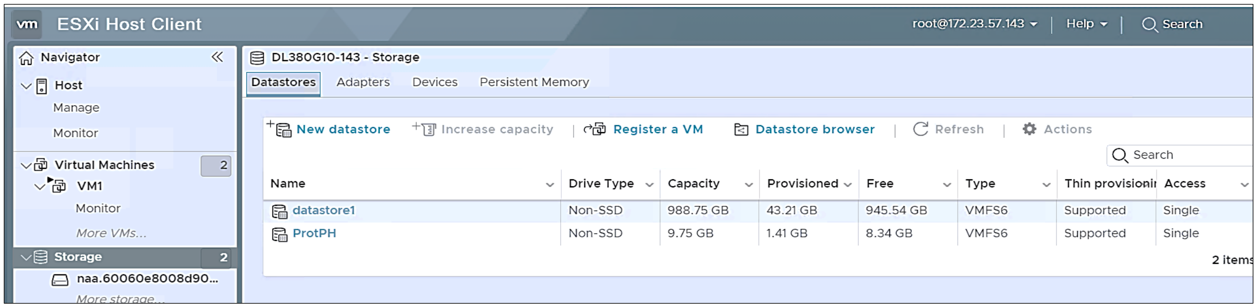
```
LDEV_NAMING : SRA_LUNS_50
STS : NML
OPE_TYPE : NONE
OPE_RATE : 100
MP# : 2
ASSIGNED_MP# : 2
SSID : 0004
ALUA : Disable
RSGID : 0
PWSV_S : -
CL_MIG : N
[root@cci~]#
```

2. Create a DP-VOL as a replication LUN and add it to the resource group of the primary storage system. Make sure that both the physical and virtual ID of the LDEV is the same.

```
[root@cci~]# raidcom unmap resource -ldev_id 00:FE -virtual_ldev_id 00:FE -IH
[root@cci~]# raidcom add resource -resource_name SRM_GAD_VMW -ldev_id 00:FE -IH
[root@cci~]# raidcom map resource -ldev_id 00:FE -virtual_ldev_id 00:FE -IH
[root@cci~]#
[root@cci~]# raidcom get ldev -ldev_id 00:FE -fx -IH
Serial#  : 5****5
LDEV : fe VIR_LDEV : fe
SL : 0
CL : 0
VOL_TYPE : OPEN-V-CVS
VOL_Capacity(BLK) : 104857600
NUM_PORT : 0
PORTs :
F_POOLID : NONE
VOL_ATTR : CVS : HDP
CMP : -
EXP_SPACE : -
B_POOLID : 13
LDEV_NAMING : SRM_LUNS_50
STS : NML
OPE_TYPE : NONE
OPE_RATE : 100
MP# : 1
ASSIGNED_MP# : 1
SSID : 0004
Used_Block(BLK) : 0
FLA(MB) : Disable
RSV(MB) : 0
CSV_Status : DISABLED
CSV_PROGRESS(%) : -
CSV_Mode : DISABLED
COMPRESSION_ACCELERATION : -
COMPRESSION_ACCELERATION_STATUS : -
CSV_PROCESS_MODE : -
DEDUPLICATION_DATA : DISABLED
ALUA : Disable
RSGID : 3
PWSV_S : -
CL_MIG : N
[root@cci~]#
```

Creating a Datastore

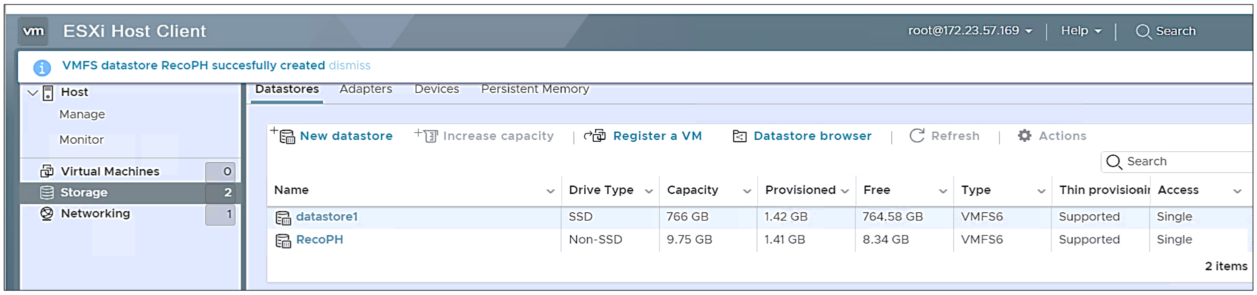
1. Create a datastore on top of the LUNs on each host. For more details, see the Broadcom documentation on creation of a Datastore. On the primary host, create a datastore (ProtPH) using the previously created LUN.



Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provisionir	Access
datastore1	Non-SSD	988.75 GB	43.21 GB	945.54 GB	VMFS6	Supported	Single
ProtPH	Non-SSD	9.75 GB	1.41 GB	8.34 GB	VMFS6	Supported	Single

2 items

2. On the secondary host, create a datastore using the previously created LUN.



VMFS datastore RecoPH succesfully created dismiss

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provisionir	Access
datastore1	SSD	766 GB	1.42 GB	764.58 GB	VMFS6	Supported	Single
RecoPH	Non-SSD	9.75 GB	1.41 GB	8.34 GB	VMFS6	Supported	Single

2 items

Installing Ops Center Protector and Configuring GAD

This section shows how to install Ops Center Protector, configure GAD, and set up Ops Center Protector Adapter for VMware SRM.

Installing Ops Center Protector

1. Download the installation package from https://support.hitachivantara.com/ and prepare a new VM with a Windows guest OS.
2. Transfer and unzip the package, then launch the installer (install.exe or setup.bat) with administrator privileges.
3. Accept the license agreement.
4. Select the installation directory and type (for example, Master).
5. Configure the node name, user account type (for example, Administrator), and HTTPS port (default: 443).
6. Complete the installation and access Hitachi Ops Center Protector through a web browser using the configured IP address.

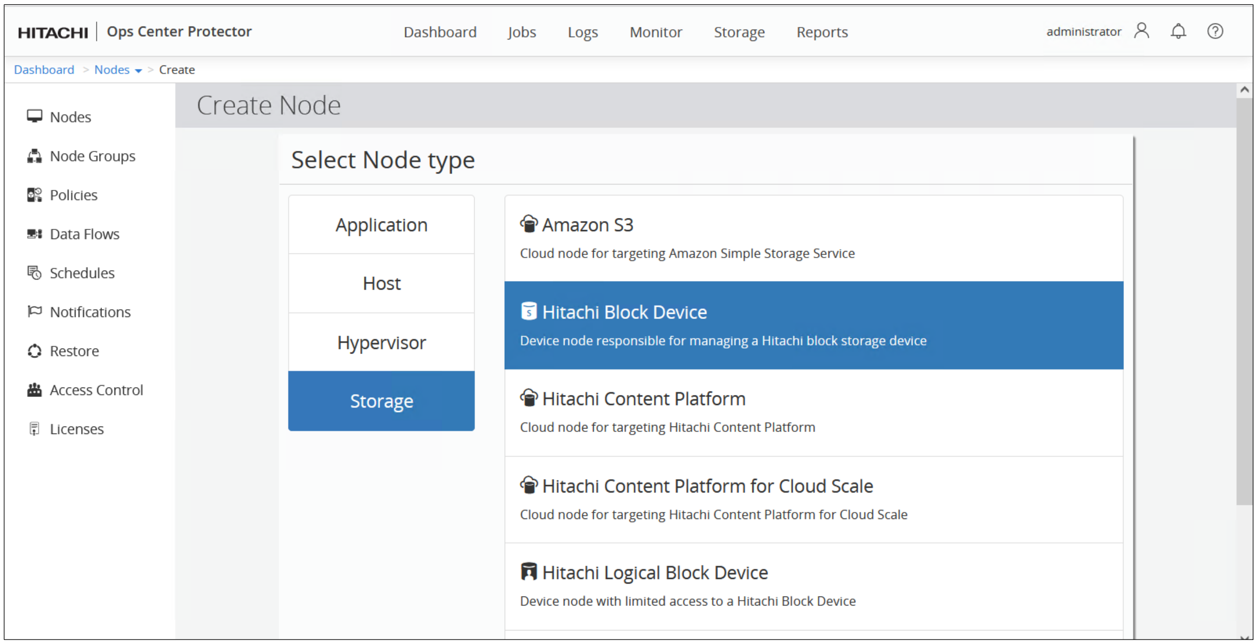
For detailed instructions on installing Hitachi Ops Center Protector, see the Hitachi documentation on Ops Center Protector.

Configuring GAD with Ops Center Protector

In Ops Center Protector, nodes represent resources such as storage systems, applications, or servers that can be managed, protected, or monitored. Storage nodes represent storage systems used for replication, snapshots, and backups.

Creating Nodes with Hitachi Block Devices

1. From Ops Center Protector, navigate to Nodes and select **Create a new item**. Click **NEXT**.
2. Select the Node Type as **Storage** and then select **Hitachi Block Device**. Click **NEXT**.



Create Node

Select Node type

Application

Host

Hypervisor

Storage

Amazon S3
Cloud node for targeting Amazon Simple Storage Service

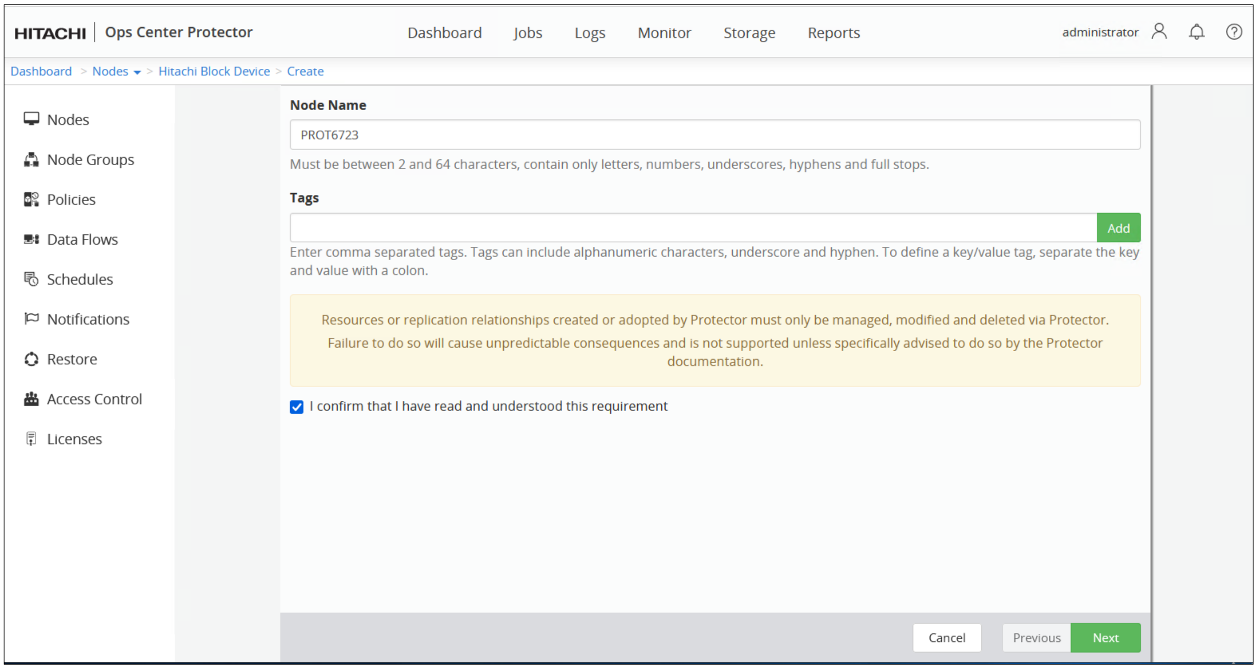
Hitachi Block Device
Device node responsible for managing a Hitachi block storage device

Hitachi Content Platform
Cloud node for targeting Hitachi Content Platform

Hitachi Content Platform for Cloud Scale
Cloud node for targeting Hitachi Content Platform for Cloud Scale

Hitachi Logical Block Device
Device node with limited access to a Hitachi Block Device

3. Enter a node name and select the checkbox to confirm the requirement. Click **NEXT**.



Node Name

PROT6723

Must be between 2 and 64 characters, contain only letters, numbers, underscores, hyphens and full stops.

Tags

Add

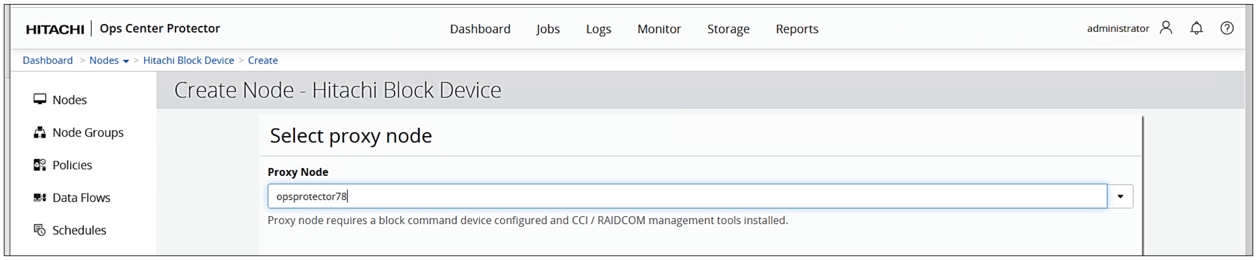
Enter comma separated tags. Tags can include alphanumeric characters, underscore and hyphen. To define a key/value tag, separate the key and value with a colon.

Resources or replication relationships created or adopted by Protector must only be managed, modified and deleted via Protector. Failure to do so will cause unpredictable consequences and is not supported unless specifically advised to do so by the Protector documentation.

☑ I confirm that I have read and understood this requirement

Cancel Previous Next

4. In Proxy Node field, enter the name of the Ops Center VM and click **NEXT**.



Create Node - Hitachi Block Device

Select proxy node

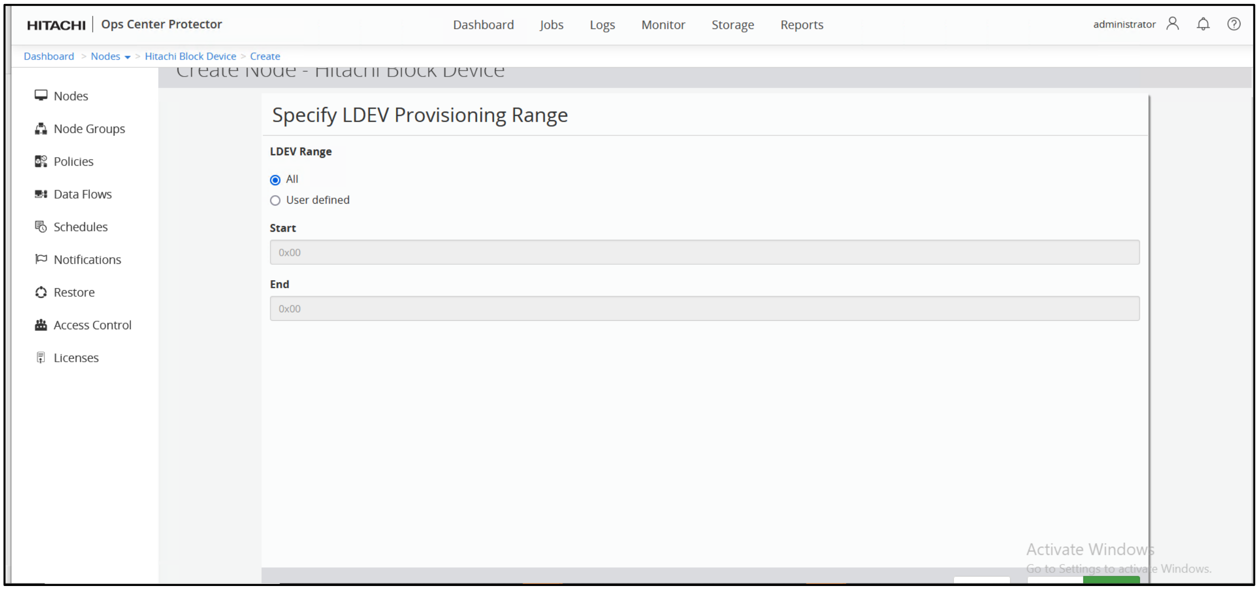
Proxy Node

opsprotector78

Proxy node requires a block command device configured and CCI / RAIDCOM management tools installed.

5. Enter the primary storage serial number and credentials, and click **NEXT**.

6. Select the LDEV Provisioning Range and click **NEXT**.



Specify LDEV Provisioning Range

LDEV Range

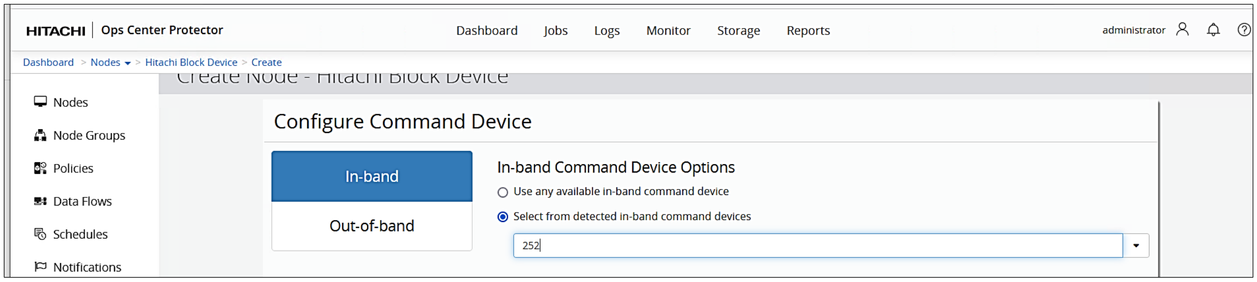
● All

○ User defined

Start: 0x00

End: 0x00

7. Enter the decimal digit LDEV ID of the command device and click **NEXT**.



Configure Command Device

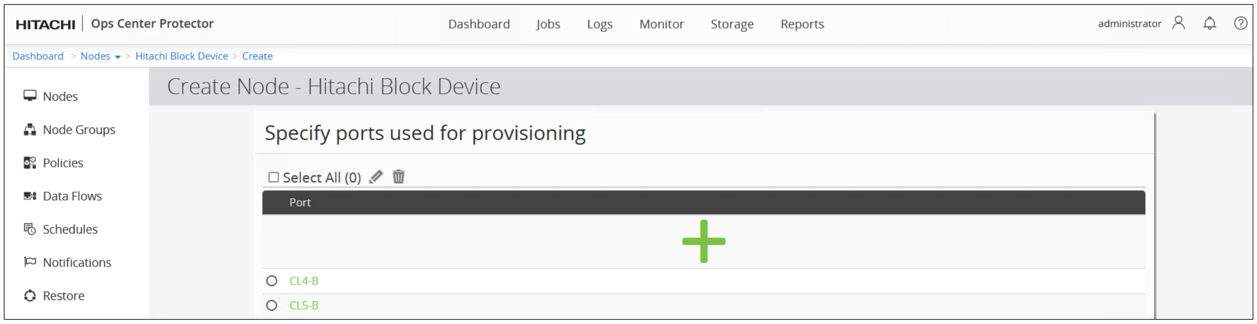
In-band Command Device Options

○ Use any available in-band command device

● Select from detected in-band command devices

252

8. Specify the storage ports used for provisioning and click **NEXT**.



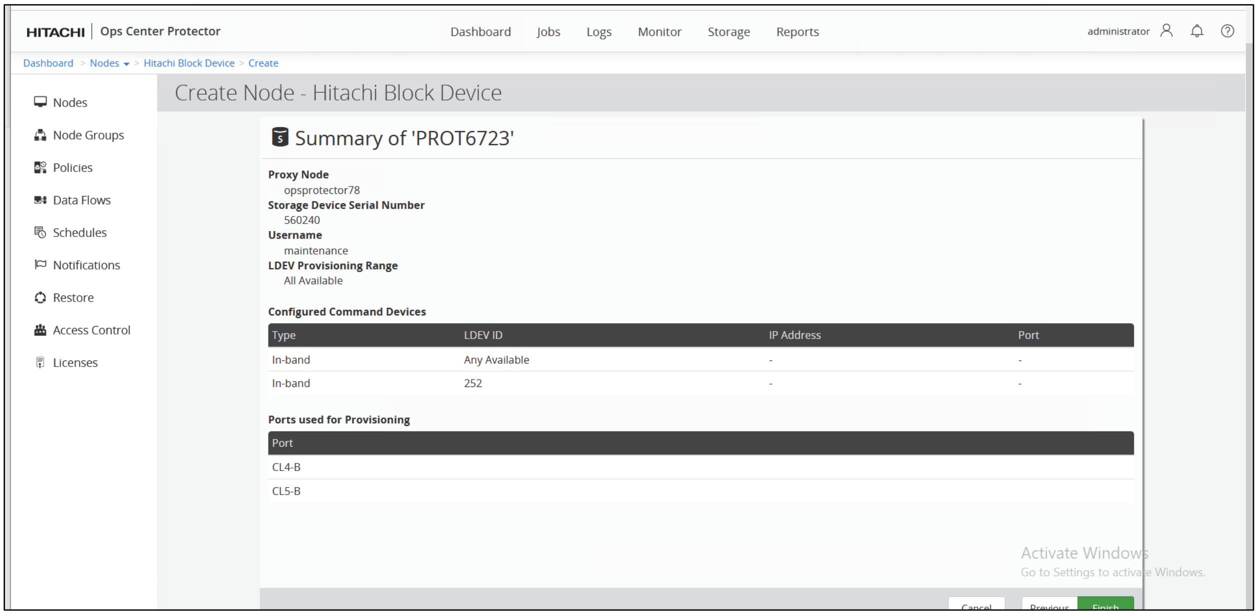
Create Node - Hitachi Block Device

Specify ports used for provisioning

□ Select All (0)

Port
○ CL4-B
○ CL5-B

9. Create a Hitachi Block Device node and click **FINISH**.



Create Node - Hitachi Block Device

Summary of 'PROT6723'

Proxy Node
opsprotector78
Storage Device Serial Number
560240
Username
maintenance
LDEV Provisioning Range
All Available

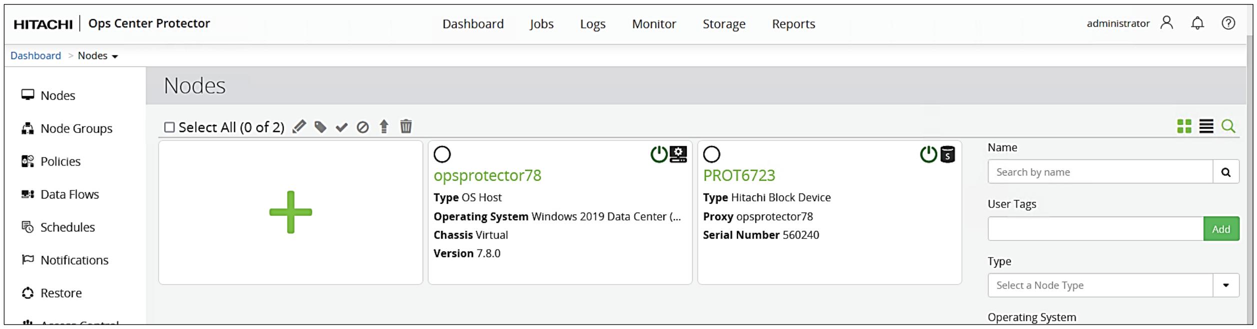
Configured Command Devices

Type	LDEV ID	IP Address	Port
In-band	Any Available	-	-
In-band	252	-	-

Ports used for Provisioning

Port
CL4-B
CL5-B

The Hitachi Block Device is created under Nodes:

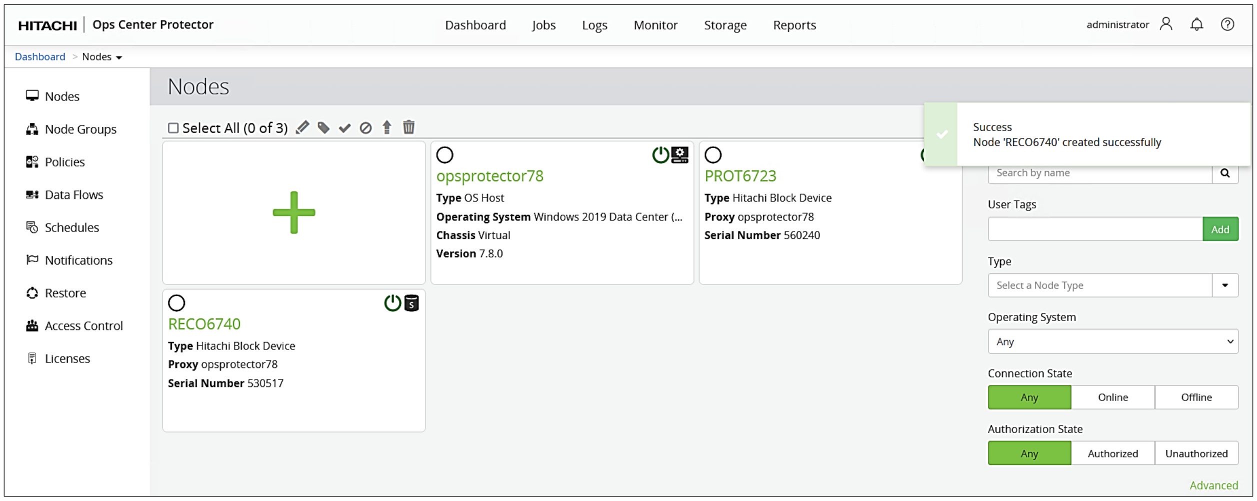


Nodes

opsprotector78
Type OS Host
Operating System Windows 2019 Data Center (...
Chassis Virtual
Version 7.8.0

PROT6723
Type Hitachi Block Device
Proxy opsprotector78
Serial Number 560240

10. Repeat the procedure to create a new block host for the secondary storage system:



Nodes

Success
Node 'RECO6740' created successfully

opsprotector78
Type OS Host
Operating System Windows 2019 Data Center (...
Chassis Virtual
Version 7.8.0

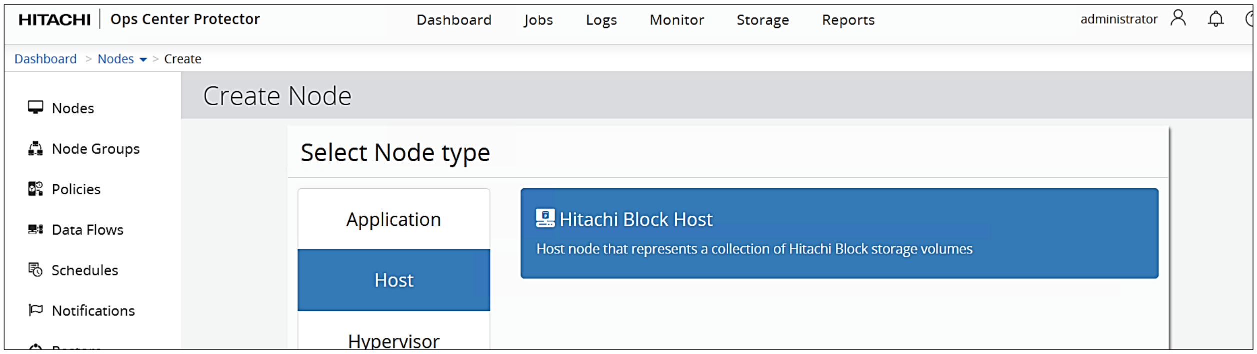
PROT6723
Type Hitachi Block Device
Proxy opsprotector78
Serial Number 560240

RECO6740
Type Hitachi Block Device
Proxy opsprotector78
Serial Number 530517

Creating a Hitachi Block Host

A Hitachi Block Host in Ops Center Protector represents a server connected to block storage devices, enabling data transfer through iSCSI or Fibre Channel protocols.

1. Navigate to Nodes and select **Create a new item**. Click **Next**.
2. Select the Node Type as **Host** and then select **Hitachi Block Host**.



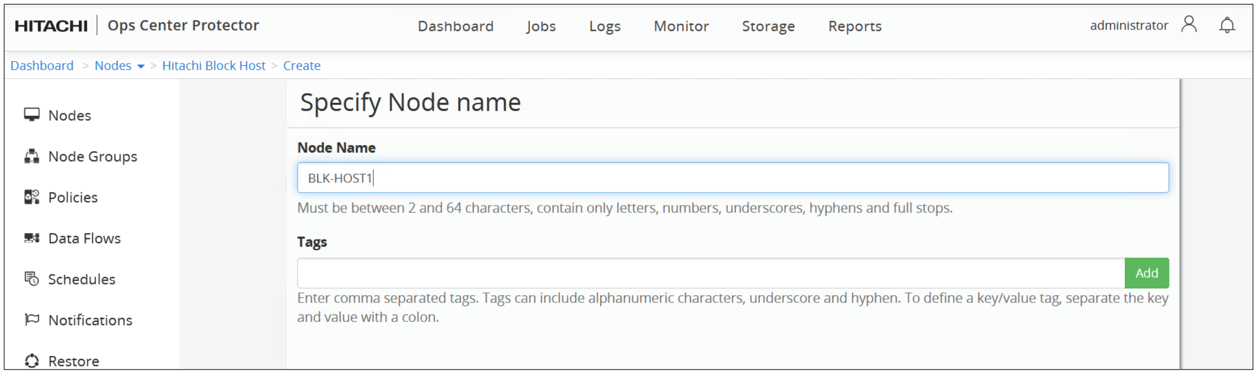
Create Node

Select Node type

Hitachi Block Host

Host node that represents a collection of Hitachi Block storage volumes

3. Enter a node name and click **NEXT**.



Specify Node name

Node Name

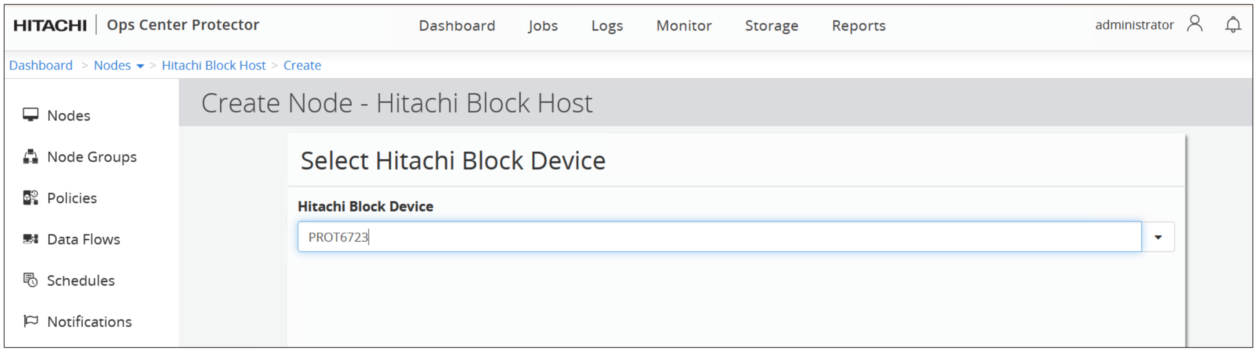
BLK-HOST1

Must be between 2 and 64 characters, contain only letters, numbers, underscores, hyphens and full stops.

Tags

Enter comma separated tags. Tags can include alphanumeric characters, underscore and hyphen. To define a key/value tag, separate the key and value with a colon.

4. Enter the name of the Hitachi Block Device. Click **NEXT**.



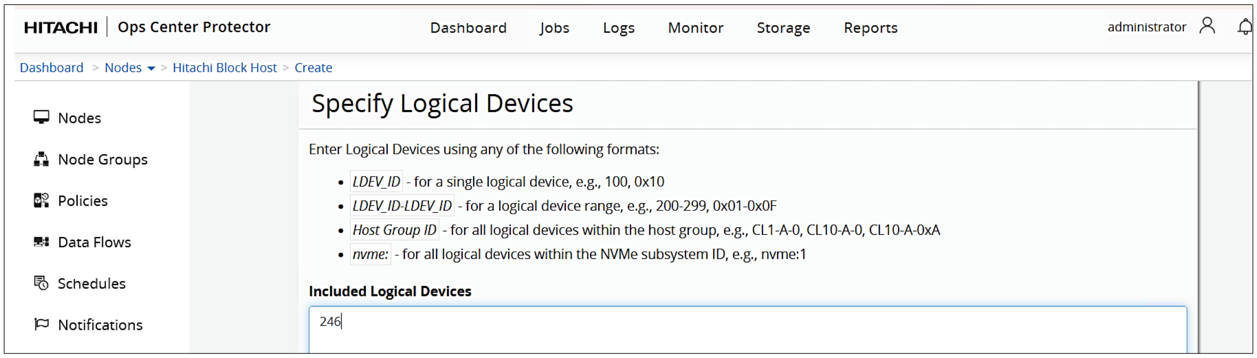
Create Node - Hitachi Block Host

Select Hitachi Block Device

Hitachi Block Device

PROT6723

5. Mention the Logical Devices number in the decimal format. Click **NEXT**.



Specify Logical Devices

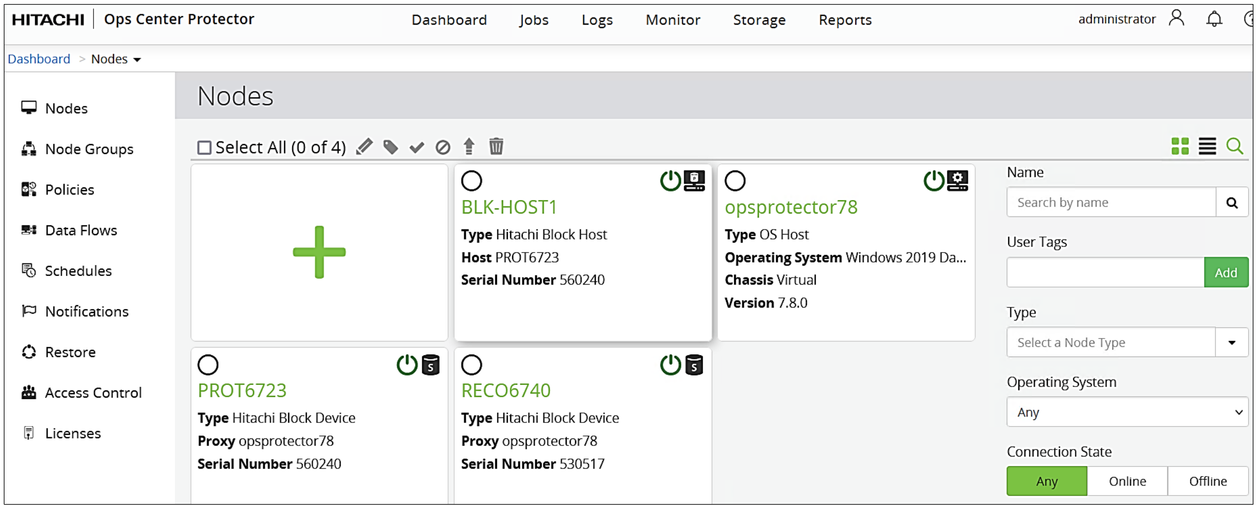
Enter Logical Devices using any of the following formats:

- *LDEV_ID* - for a single logical device, e.g., 100, 0x10
- *LDEV_ID-LDEV_ID* - for a logical device range, e.g., 200-299, 0x01-0x0F
- *Host Group ID* - for all logical devices within the host group, e.g., CL1-A-0, CL10-A-0, CL10-A-0xA
- *nvme:* - for all logical devices within the NVMe subsystem ID, e.g., nvme:1

Included Logical Devices

246

The Hitachi Block Device is created under Nodes:



Nodes

BLK-HOST1
Type Hitachi Block Host
Host PROT6723
Serial Number 560240

opsprotector78
Type OS Host
Operating System Windows 2019 Da...
Chassis Virtual
Version 7.8.0

PROT6723
Type Hitachi Block Device
Proxy opsprotector78
Serial Number 560240

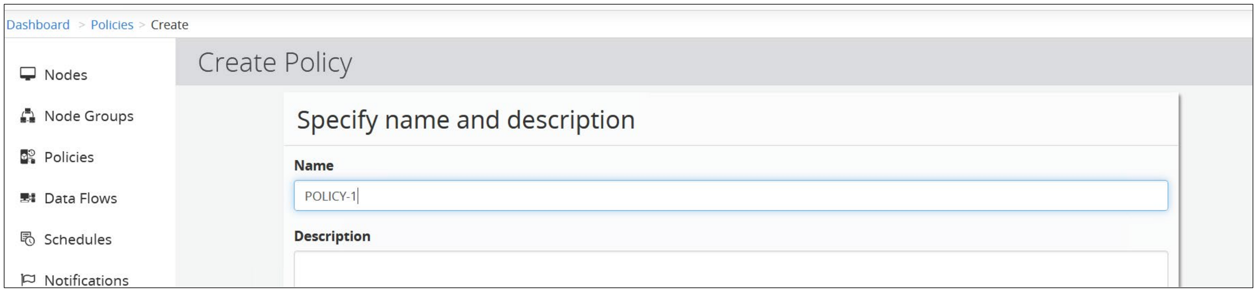
RECO6740
Type Hitachi Block Device
Proxy opsprotector78
Serial Number 530517

Creating a Policy

In Ops Center Protector, a policy defines rules for data protection, including backups, retention, and storage, ensuring efficient recovery and compliance.

1. Click **Create a new policy**.

2. Enter the policy name and click **NEXT**.



Create Policy

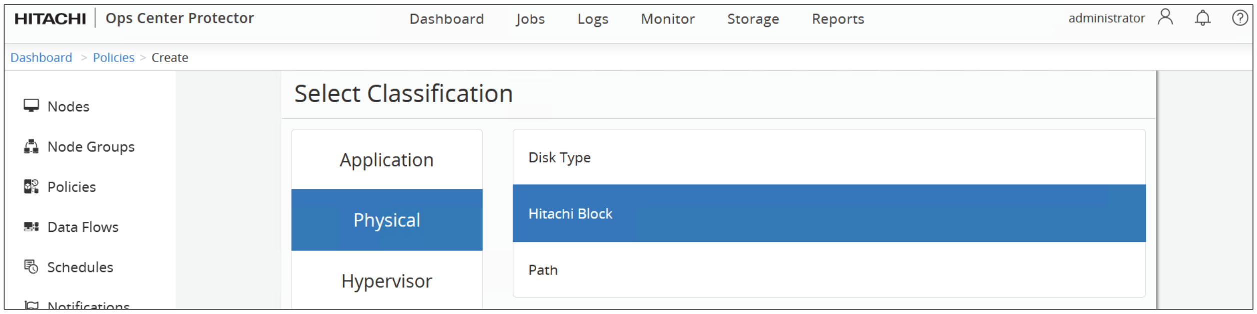
Specify name and description

Name

POLICY-1

Description

3. Select **Classification as a Physical** and then select **Hitachi Block**. Click **NEXT**.

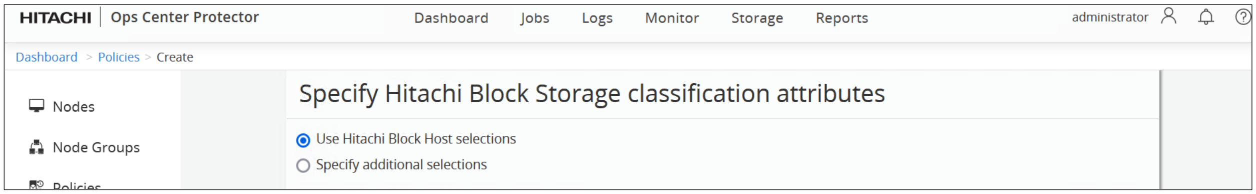

HITACHI | Ops Center Protector
Dashboard Jobs Logs Monitor Storage Reports
administrator
Dashboard > Policies > Create
Nodes
Node Groups
Policies
Data Flows
Schedules
Notifications

Select Classification

Application
Physical
Hypervisor

Disk Type
Hitachi Block
Path

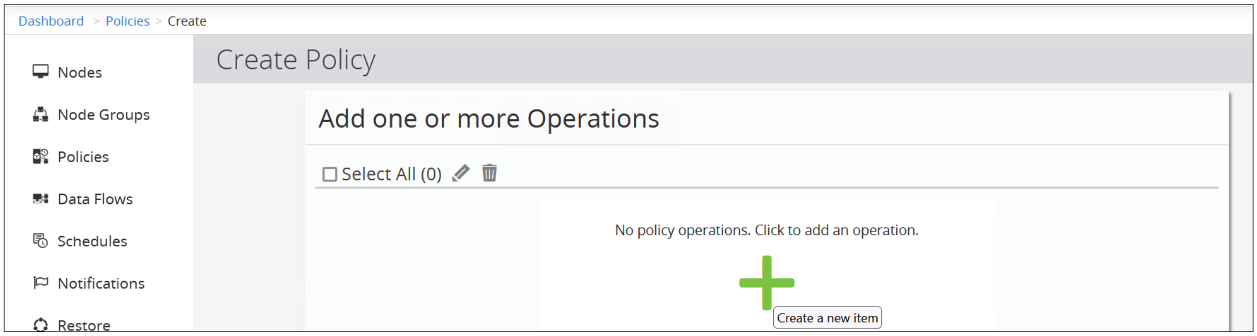
4. Select Use Hitachi Block Host Selection as Hitachi Block Storage Classification Attributes. Click **NEXT**.


HITACHI | Ops Center Protector
Dashboard Jobs Logs Monitor Storage Reports
administrator
Dashboard > Policies > Create
Nodes
Node Groups
Policies

Specify Hitachi Block Storage classification attributes

● Use Hitachi Block Host selections
○ Specify additional selections

5. To add an operation, click the add (**+**) icon. Click **NEXT**.



Create Policy

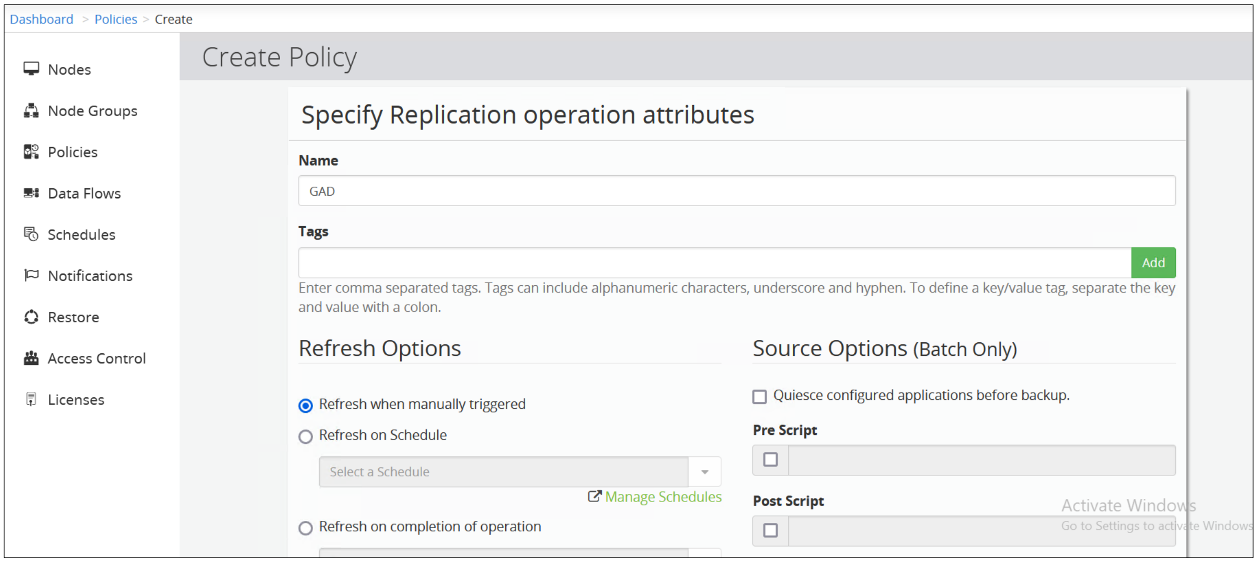
Add one or more Operations

□ Select All (0)

No policy operations. Click to add an operation.

6. For operation, select **Replicate**.

7. Specify the replication operation attributes and name. Click **NEXT**.



Create Policy

Specify Replication operation attributes

Name

GAD

Tags

Enter comma separated tags. Tags can include alphanumeric characters, underscore and hyphen. To define a key/value tag, separate the key and value with a colon.

Refresh Options

● Refresh when manually triggered

○ Refresh on Schedule

Select a Schedule

○ Refresh on completion of operation

Source Options (Batch Only)

□ Quiesce configured applications before backup.

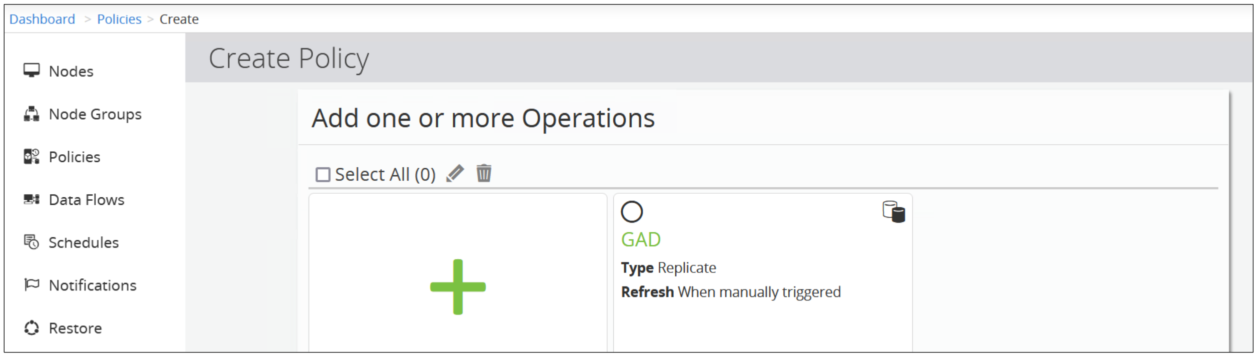
Pre Script

□

Post Script

□

The GAD operation is created:



Create Policy

Add one or more Operations

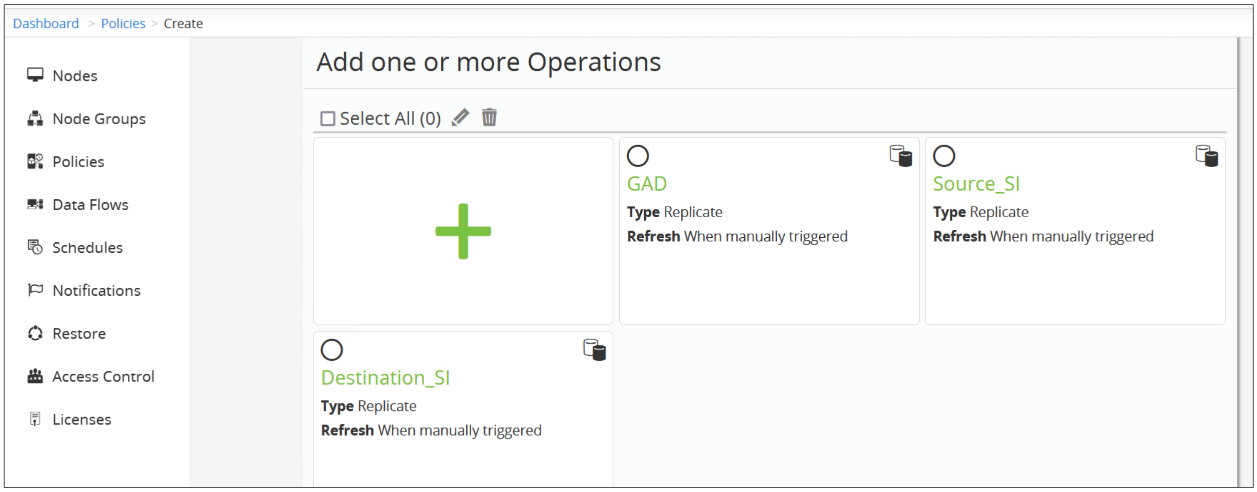
□ Select All (0)

○ GAD

Type Replicate

Refresh When manually triggered

8. Repeat the procedure to define two other operations for primary and secondary storage SI.



Add one or more Operations

□ Select All (0)

○ GAD

Type Replicate

Refresh When manually triggered

○ Source_SI

Type Replicate

Refresh When manually triggered

○ Destination_SI

Type Replicate

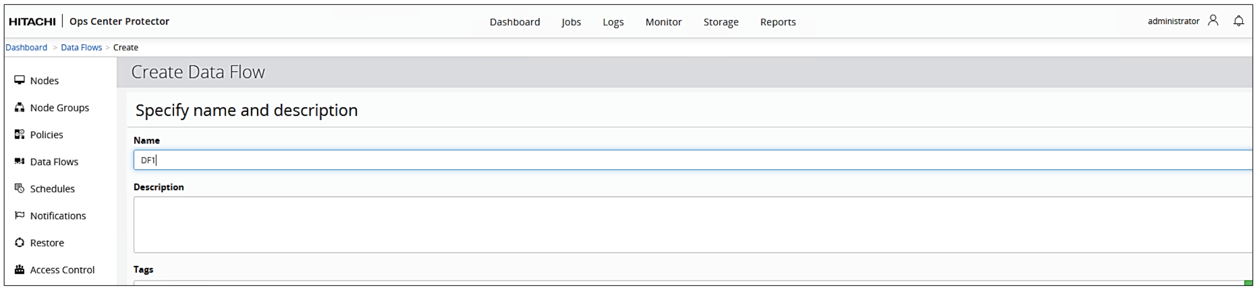
Refresh When manually triggered

Creating a Data Flow

Creating a data flow in Ops Center Protector involves setting up a sequence of operations for efficient data protection and replication.

1. Select **Create Data Flow** and click **NEXT**.

2. Enter the name of the data flow and click **NEXT**.



Create Data Flow

Specify name and description

Name

DF1

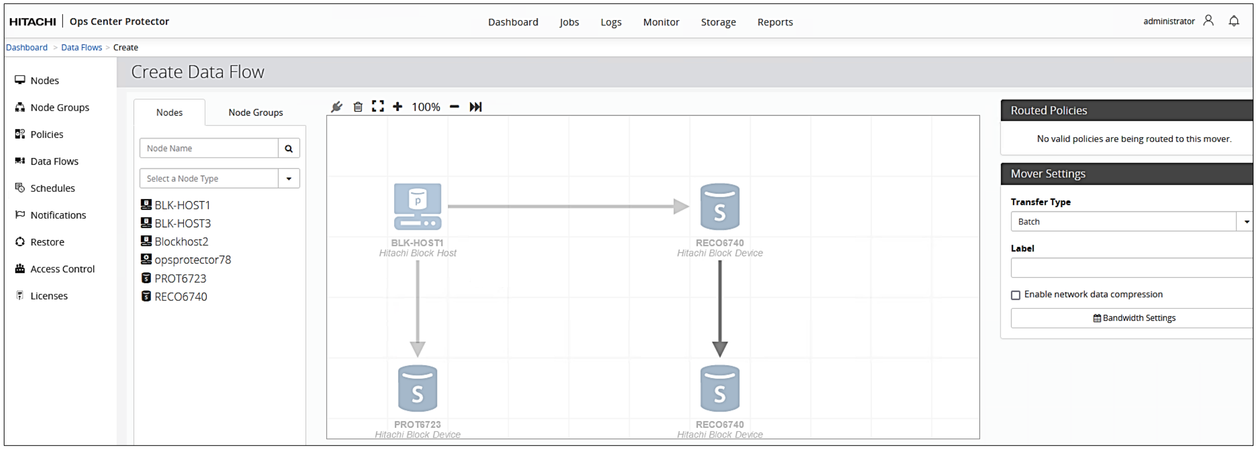
Description

Tags

3. Select the Source (Hitachi Block Host – BLK-HOST1) where the data resides by assigning the resources as the Source, ensuring they are already registered in the system. Drag it to the flow.

4. Specify the destination by dragging it to the Flow (Hitachi Block Device – RECO6740) where the data will be transferred or replicated.

5. Add all the assigned resources to the flow using the drag-and-drop method.



Create Data Flow

- BLK-HOST1
- BLK-HOST3
- Blockhost2
- opsprotector78
- PROT6723
- RECO6740

Routed Policies

No valid policies are being routed to this mover.

Mover Settings

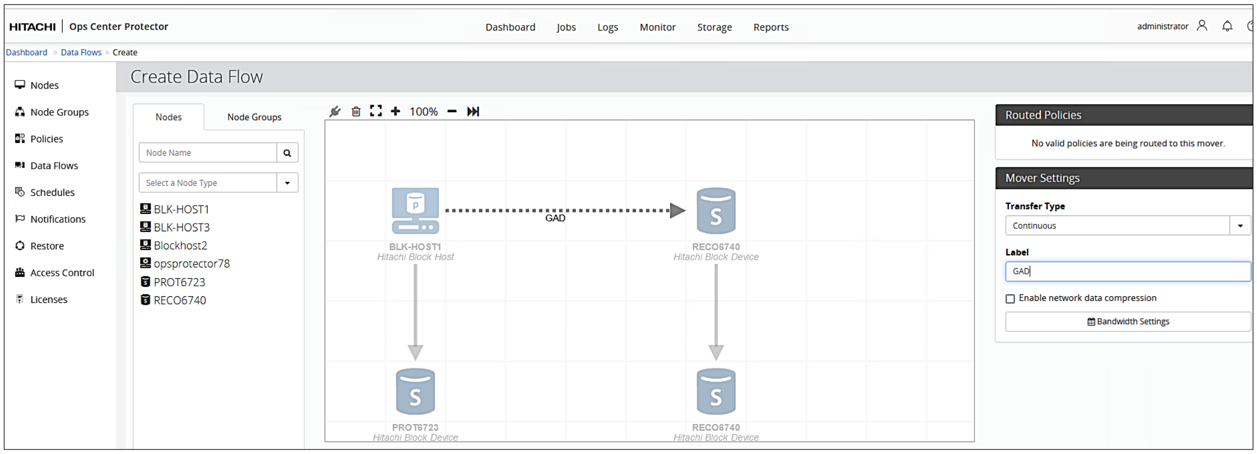
Transfer Type

Batch

Label

☐ Enable network data compression

6. Select **Block Host** and set the Transfer Type to **Continuous**. In this scenario, the label is named GAD.

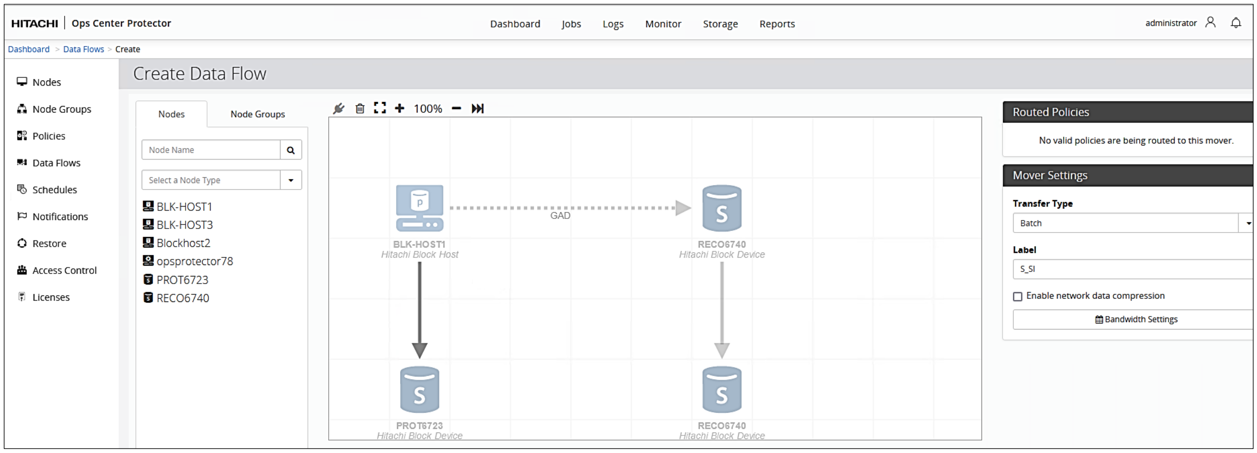


Transfer Type: Continuous

Label: GAD

☐ Enable network data compression

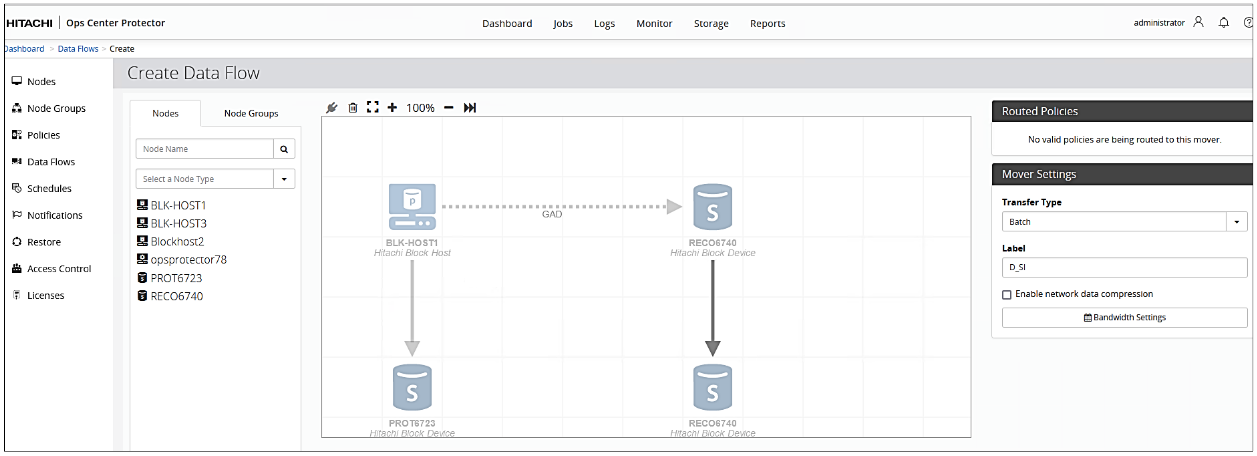
7. Rename the labels of the remaining transfers.



Transfer Type: Batch

Label: S_SI

☐ Enable network data compression

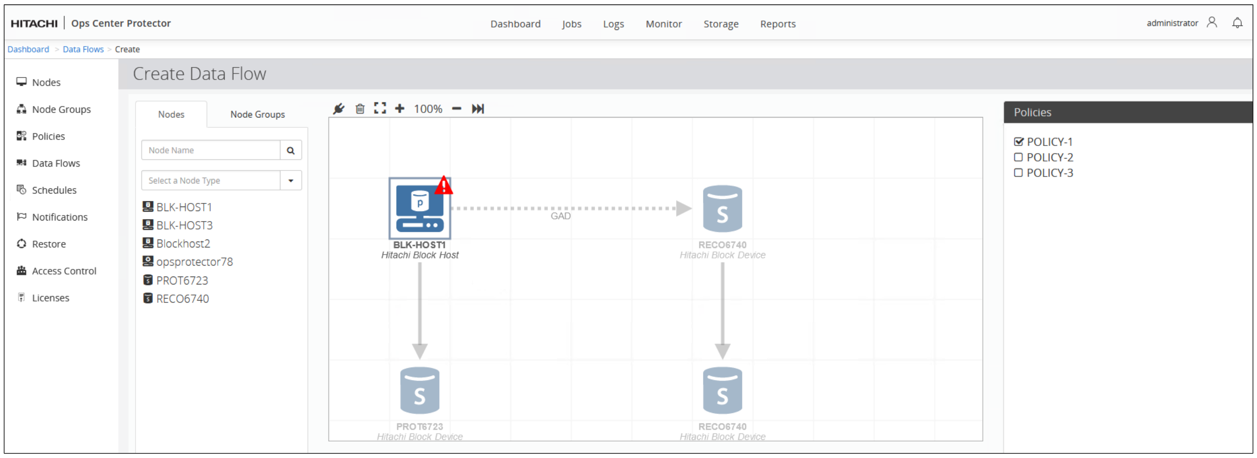


Transfer Type: Batch

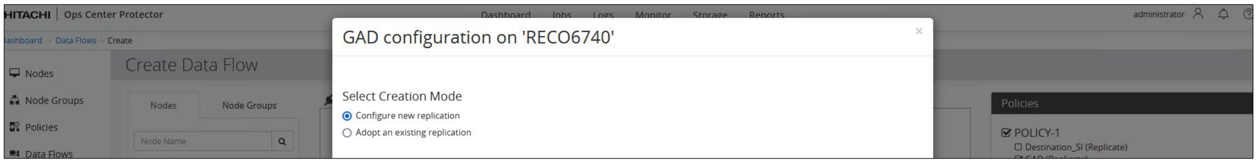
Label: D_SI

☐ Enable network data compression

8. Select the block host and select the policy.



9. Specify the GAD policy to attach to the block host and configure the policy settings. Select the Creation Mode of the GAD policy and click **NEXT**.



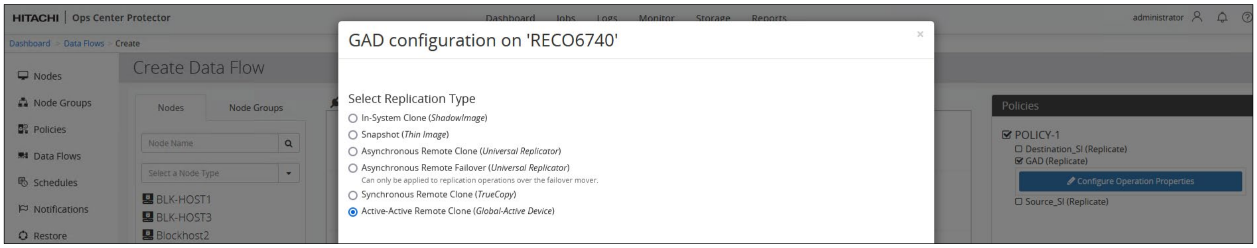
GAD configuration on 'RECO6740'

Select Creation Mode

● Configure new replication

○ Adopt an existing replication

10. Select the replication type as Active-Active Remote Clone (Global-Active Device). Click **NEXT**.



GAD configuration on 'RECO6740'

Select Replication Type

○ In-System Clone (*ShadowImage*)

○ Snapshot (*Thin Image*)

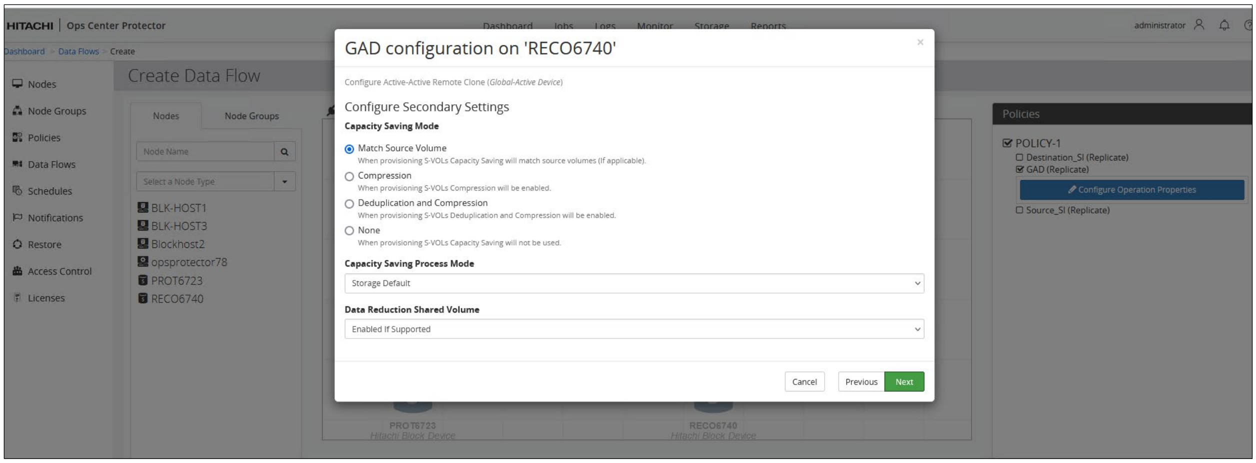
○ Asynchronous Remote Clone (*Universal Replicator*)

○ Asynchronous Remote Failover (*Universal Replicator*)
Can only be applied to replication operations over the failover mover.

○ Synchronous Remote Clone (*TrueCopy*)

● Active-Active Remote Clone (*Global-Active Device*)

11. Set up the configuration by entering the following details. Click **NEXT**.



GAD configuration on 'RECO6740'

Configure Active-Active Remote Clone (*Global-Active Device*)

Configure Secondary Settings

Capacity Saving Mode

● Match Source Volume
When provisioning S-VOLs Capacity Saving will match source volumes (If applicable).

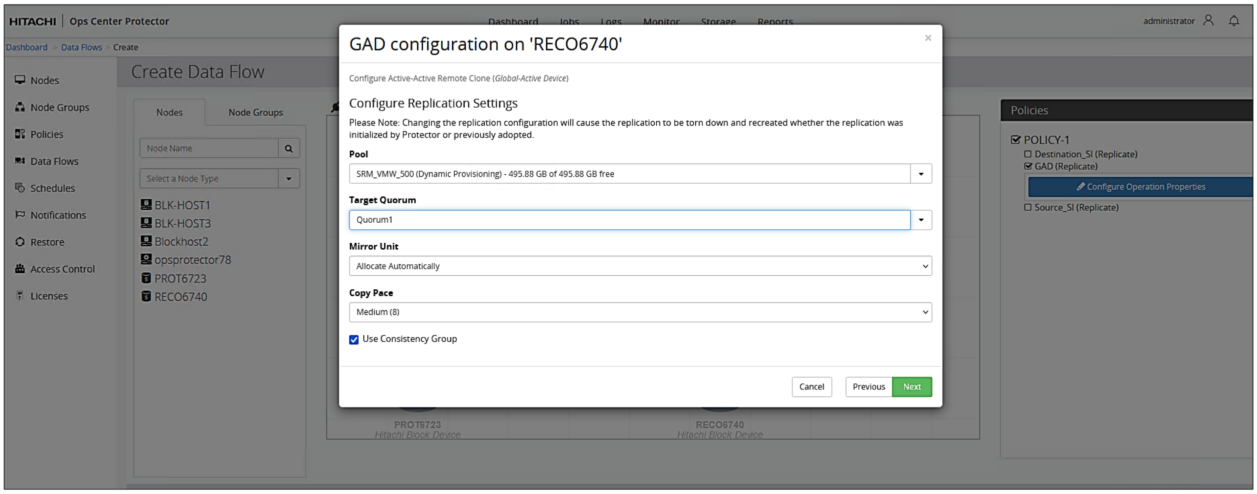
○ Compression
When provisioning S-VOLs Compression will be enabled.

○ Deduplication and Compression
When provisioning S-VOLs Deduplication and Compression will be enabled.

○ None
When provisioning S-VOLs Capacity Saving will not be used.

Capacity Saving Process Mode: Storage Default

Data Reduction Shared Volume: Enabled If Supported



GAD configuration on 'RECO6740'

Configure Active-Active Remote Clone (*Global-Active Device*)

Configure Replication Settings

Please Note: Changing the replication configuration will cause the replication to be torn down and recreated whether the replication was initialized by Protector or previously adopted.

Pool: SRM_VMW_500 (Dynamic Provisioning) - 495.88 GB of 495.88 GB free

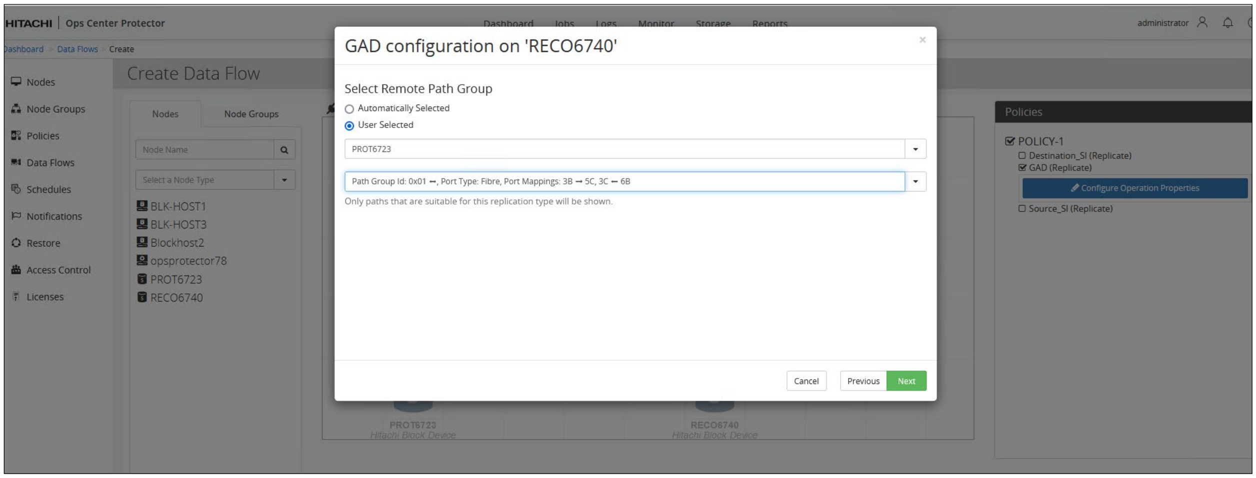
Target Quorum: Quorum1

Mirror Unit: Allocate Automatically

Copy Pace: Medium (8)

☑ Use Consistency Group

12. Specify the Remote Path Group details and click **NEXT**.



GAD configuration on 'RECO6740'

Select Remote Path Group

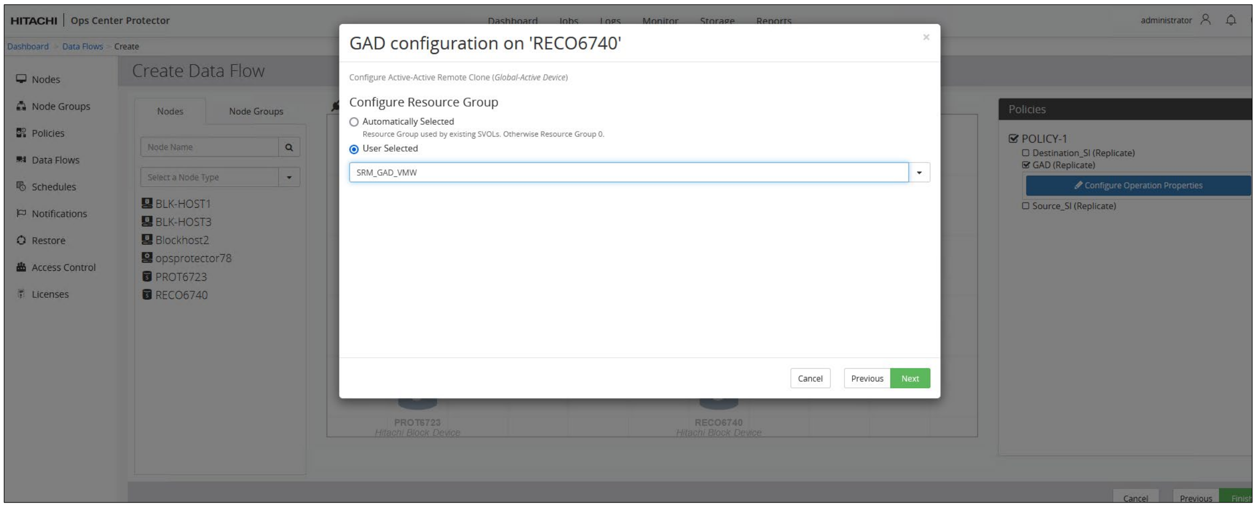
○ Automatically Selected
● User Selected

PROT6723

Path Group Id: 0x01 ↔, Port Type: Fibre, Port Mappings: 3B → 5C, 3C ← 6B

Only paths that are suitable for this replication type will be shown.

13. Add the details in the Configure Resource Group window and click **NEXT**.



GAD configuration on 'RECO6740'

Configure Active-Active Remote Clone (*Global-Active Device*)

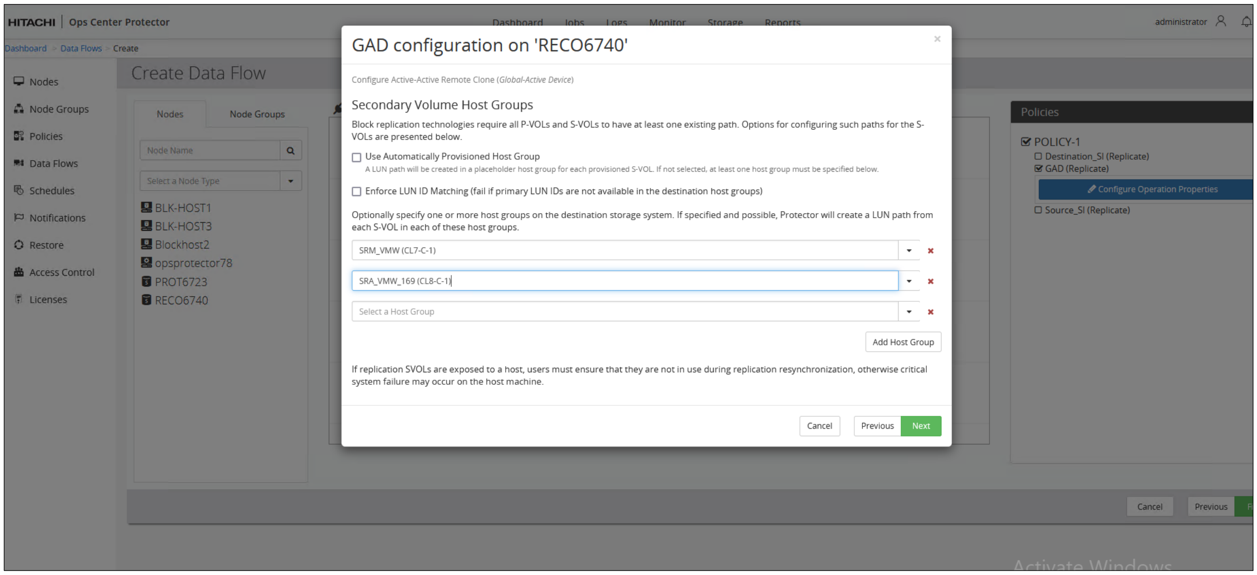
Configure Resource Group

○ Automatically Selected
Resource Group used by existing SVOLs. Otherwise Resource Group 0.

● User Selected

SRM_GAD_VMW

14. Select the secondary volume host group and click **NEXT**.



GAD configuration on 'RECO6740'

Configure Active-Active Remote Clone (*Global-Active Device*)

Secondary Volume Host Groups

Block replication technologies require all P-VOLs and S-VOLs to have at least one existing path. Options for configuring such paths for the S-VOLs are presented below.

□ Use Automatically Provisioned Host Group
A LUN path will be created in a placeholder host group for each provisioned S-VOL. If not selected, at least one host group must be specified below.

□ Enforce LUN ID Matching (fail if primary LUN IDs are not available in the destination host groups)

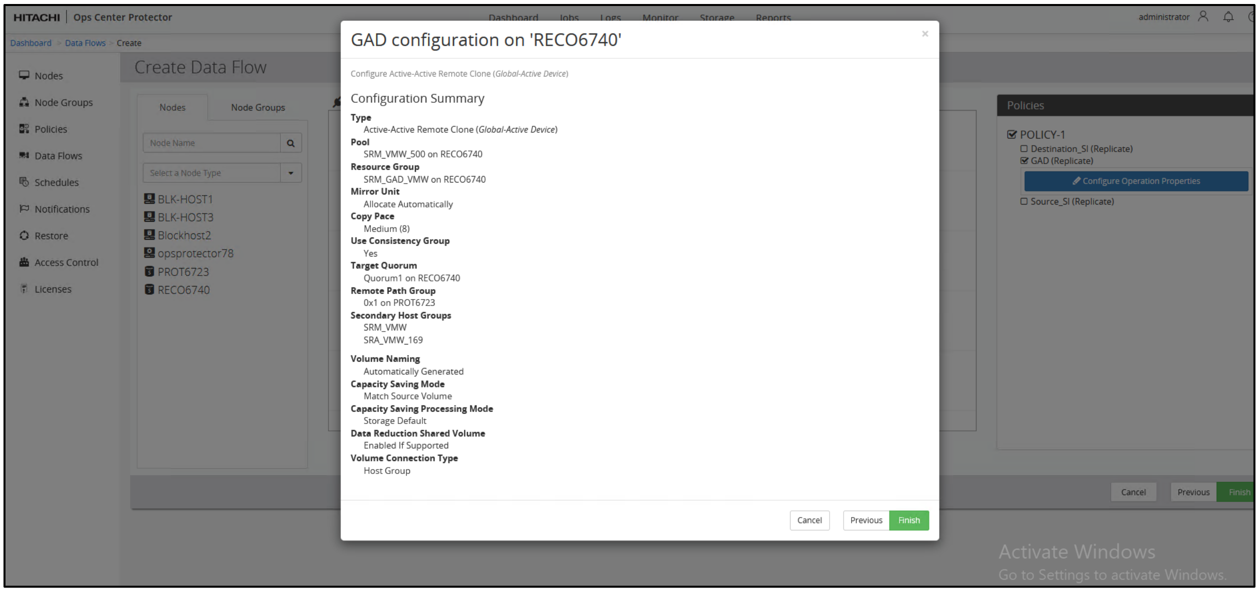
Optionally specify one or more host groups on the destination storage system. If specified and possible, Protector will create a LUN path from each S-VOL in each of these host groups.

SRM_VMW (CL7-C-1)

SRA_VMW_169 (CL8-C-1)

If replication SVOLs are exposed to a host, users must ensure that they are not in use during replication resynchronization, otherwise critical system failure may occur on the host machine.

15. Click **Finish**.



GAD configuration on 'RECO6740'

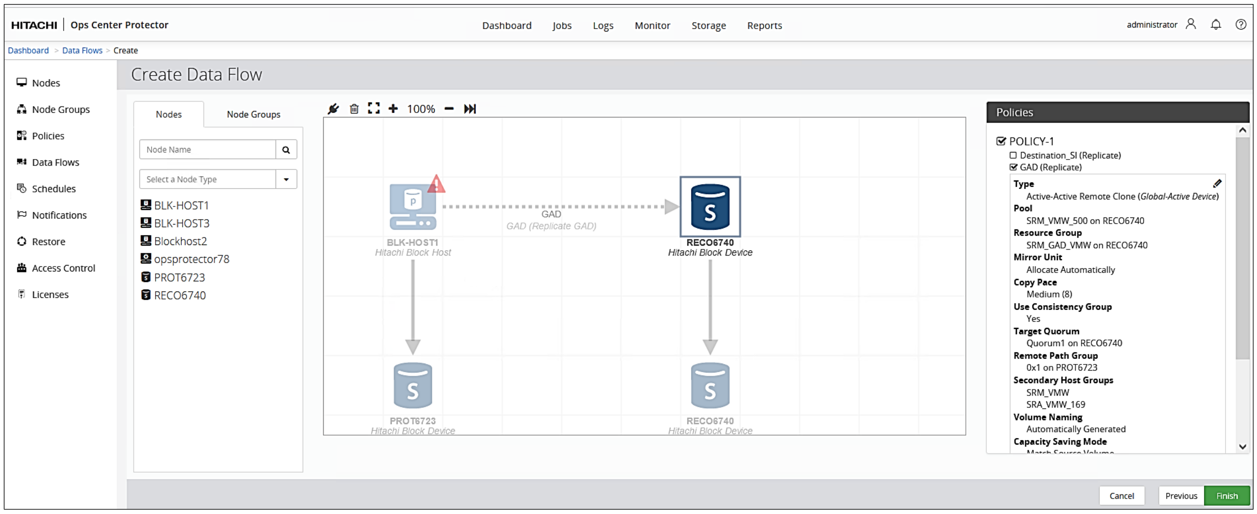
Configure Active-Active Remote Clone (*Global-Active Device*)

Configuration Summary

Type
Active-Active Remote Clone (*Global-Active Device*)
Pool
SRM_VMW_500 on RECO6740
Resource Group
SRM_GAD_VMW on RECO6740
Mirror Unit
Allocate Automatically
Copy Pace
Medium (8)
Use Consistency Group
Yes
Target Quorum
Quorum1 on RECO6740
Remote Path Group
0x1 on PROT6723
Secondary Host Groups
SRM_VMW
SRA_VMW_169
Volume Naming
Automatically Generated
Capacity Saving Mode
Match Source Volume
Capacity Saving Processing Mode
Storage Default
Data Reduction Shared Volume
Enabled If Supported
Volume Connection Type
Host Group

Cancel | Previous | Finish

The GAD Configuration Policy is complete.



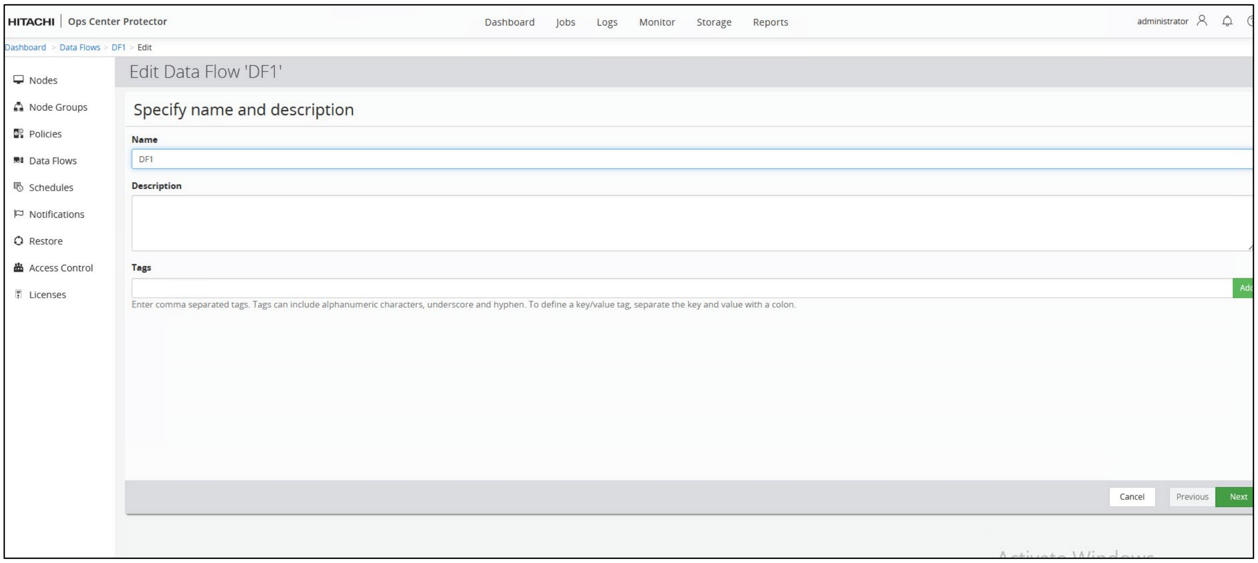
Policies

☑ POLICY-1
☐ Destination_SI (Replicate)
☑ GAD (Replicate)

Type
Active-Active Remote Clone (*Global-Active Device*)
Pool
SRM_VMW_500 on RECO6740
Resource Group
SRM_GAD_VMW on RECO6740
Mirror Unit
Allocate Automatically
Copy Pace
Medium (8)
Use Consistency Group
Yes
Target Quorum
Quorum1 on RECO6740
Remote Path Group
0x1 on PROT6723
Secondary Host Groups
SRM_VMW
SRA_VMW_169
Volume Naming
Automatically Generated
Capacity Saving Mode
Match Source Volume

Modify the other two policies, Source_SI and Destination_SI, as follows:

1. Edit the Data Flow ‘DF1’ as shown in the following screenshot and then click **NEXT**.



Edit Data Flow 'DF1'

Specify name and description

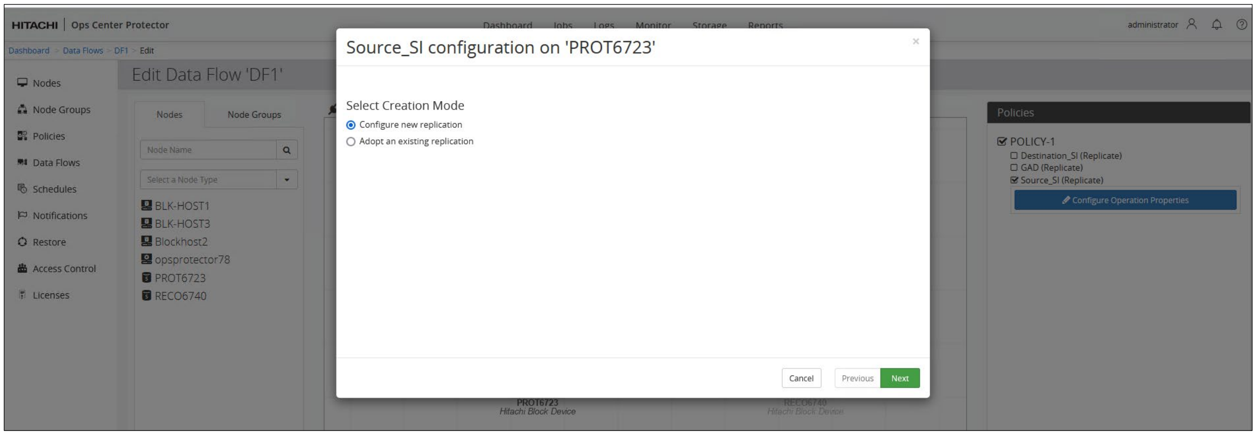
Name: DF1

Description

Tags

Enter comma separated tags. Tags can include alphanumeric characters, underscore and hyphen. To define a key/value tag, separate the key and value with a colon.

2. For creation mode, select **Configure new replication**. Click **NEXT**.



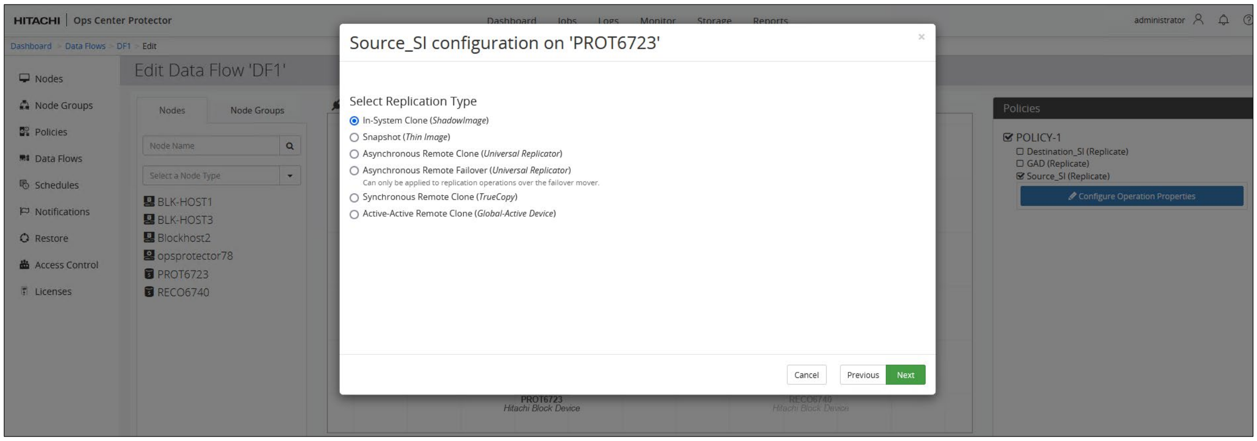
Source_SI configuration on 'PROT6723'

Select Creation Mode

● Configure new replication
○ Adopt an existing replication

☑ POLICY-1
□ Destination_SI (Replicate)
□ GAD (Replicate)
☑ Source_SI (Replicate)

3. For replication type, select **In-System Clone (ShadowImage)**. Click **NEXT**.



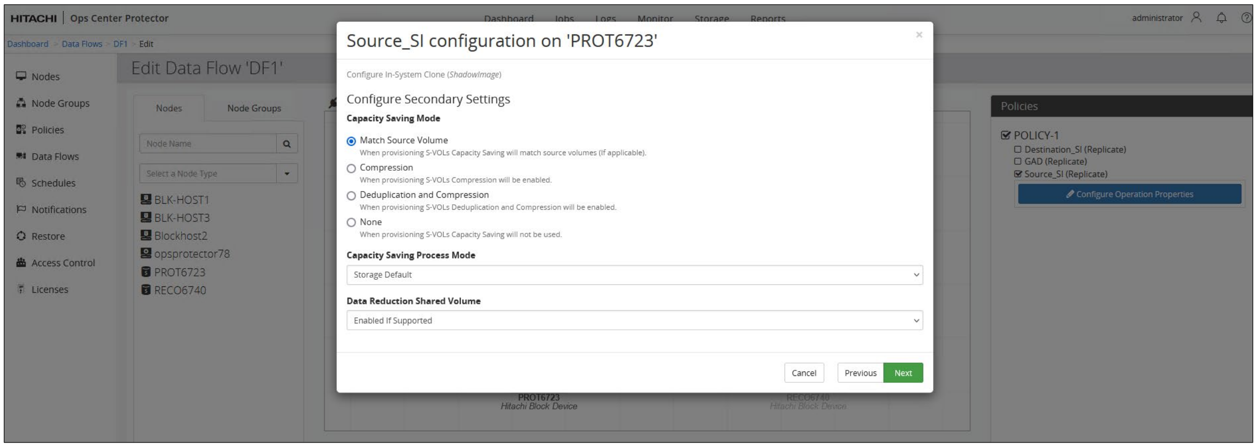
Source_SI configuration on 'PROT6723'

Select Replication Type

● In-System Clone (*ShadowImage*)
○ Snapshot (*Thin Image*)
○ Asynchronous Remote Clone (*Universal Replicator*)
○ Asynchronous Remote Failover (*Universal Replicator*)
Can only be applied to replication operations over the failover mover.
○ Synchronous Remote Clone (*TrueCopy*)
○ Active-Active Remote Clone (*Global-Active Device*)

☑ POLICY-1
□ Destination_SI (Replicate)
□ GAD (Replicate)
☑ Source_SI (Replicate)

4. Configure the In-System Clone (ShadowImage) and click **NEXT**.



Source_SI configuration on 'PROT6723'

Configure In-System Clone (*ShadowImage*)

Configure Secondary Settings

Capacity Saving Mode

● Match Source Volume
When provisioning S-VOLs Capacity Saving will match source volumes (If applicable).

○ Compression
When provisioning S-VOLs Compression will be enabled.

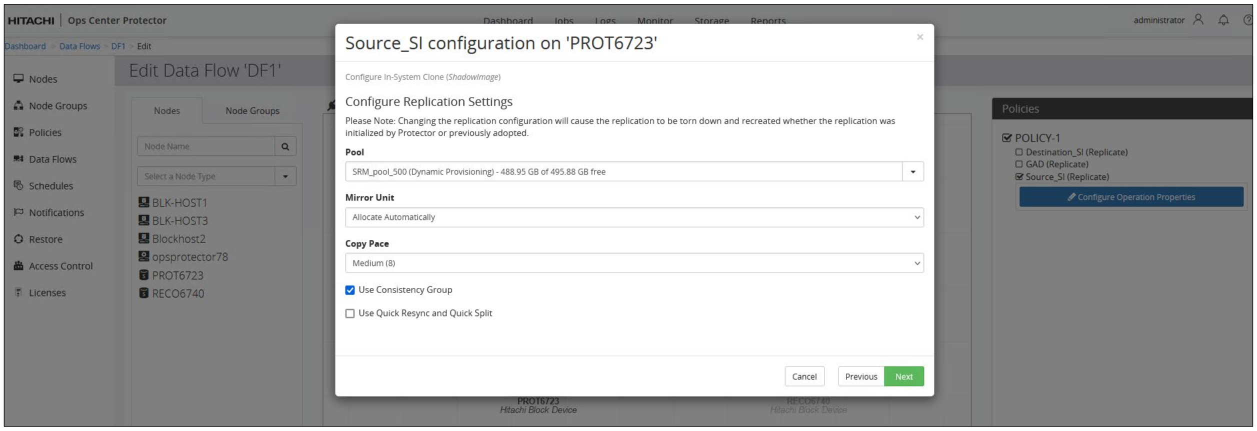
○ Deduplication and Compression
When provisioning S-VOLs Deduplication and Compression will be enabled.

○ None
When provisioning S-VOLs Capacity Saving will not be used.

Capacity Saving Process Mode
Storage Default

Data Reduction Shared Volume
Enabled If Supported

5. Specify the Pool, Mirror unit, and Copy pace. Click **NEXT**.



Source_SI configuration on 'PROT6723'

Configure In-System Clone (*ShadowImage*)

Configure Replication Settings

Please Note: Changing the replication configuration will cause the replication to be torn down and recreated whether the replication was initialized by Protector or previously adopted.

Pool
SRM_pool_500 (Dynamic Provisioning) - 488.95 GB of 495.88 GB free

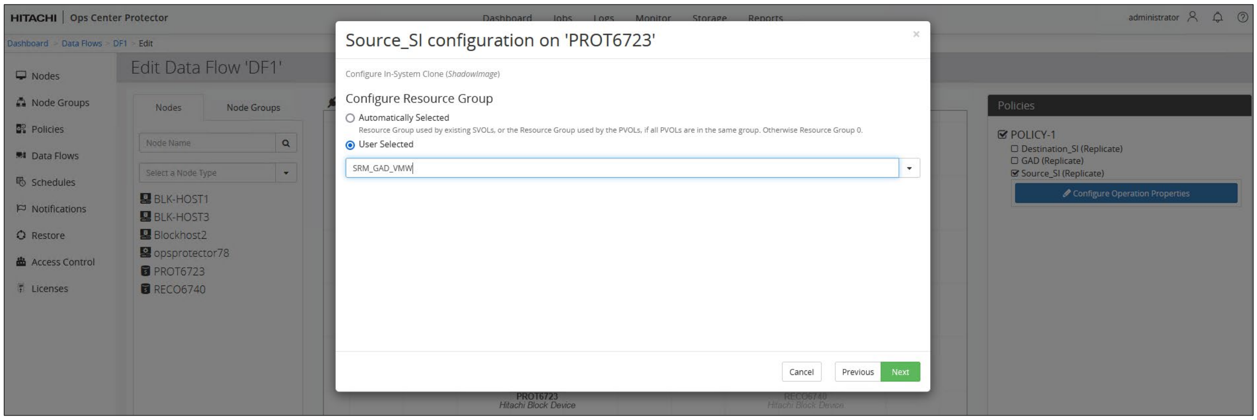
Mirror Unit
Allocate Automatically

Copy Pace
Medium (8)

☑ Use Consistency Group

□ Use Quick Resync and Quick Split

6. Specify the resource group. Click **NEXT**.



Source_SI configuration on 'PROT6723'

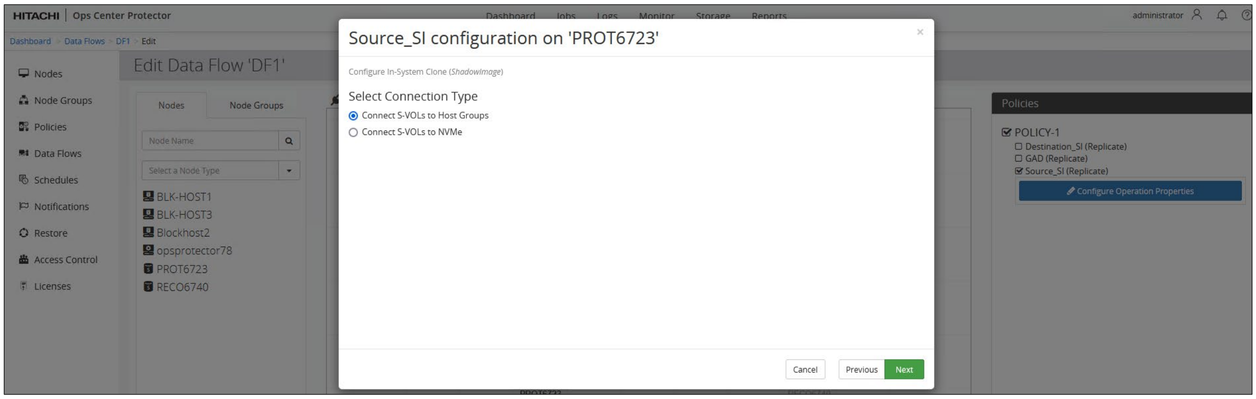
Configure In-System Clone (*ShadowImage*)

Configure Resource Group

○ Automatically Selected
Resource Group used by existing SVOLs, or the Resource Group used by the PVOLs, if all PVOLs are in the same group. Otherwise Resource Group 0.

● User Selected
SRM_GAD_VMW

7. For connection type, select **Connect S-VOLs to Host Groups**. Click **NEXT**.



Source_SI configuration on 'PROT6723'

Configure In-System Clone (*ShadowImage*)

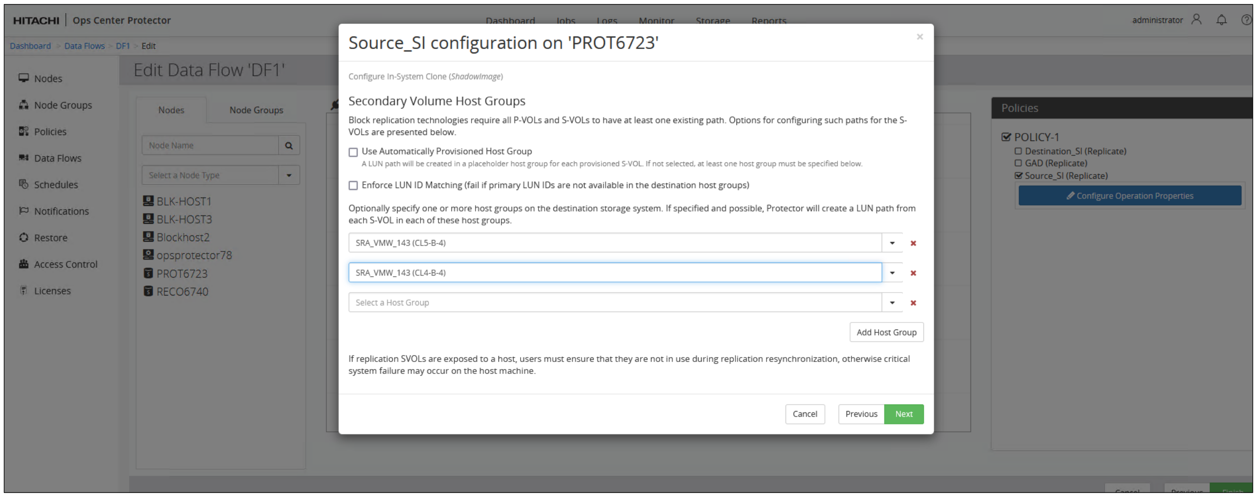
Select Connection Type

● Connect S-VOLs to Host Groups

○ Connect S-VOLs to NVMe

Cancel | Previous | Next

8. Specify the secondary volume host groups. Click **NEXT**.



Source_SI configuration on 'PROT6723'

Configure In-System Clone (*ShadowImage*)

Secondary Volume Host Groups

Block replication technologies require all P-VOLs and S-VOLs to have at least one existing path. Options for configuring such paths for the S-VOLs are presented below.

□ Use Automatically Provisioned Host Group

A LUN path will be created in a placeholder host group for each provisioned S-VOL. If not selected, at least one host group must be specified below.

□ Enforce LUN ID Matching (fail if primary LUN IDs are not available in the destination host groups)

Optionally specify one or more host groups on the destination storage system. If specified and possible, Protector will create a LUN path from each S-VOL in each of these host groups.

SRA_VMW_143 (CL5-B-4)

SRA_VMW_143 (CL4-B-4)

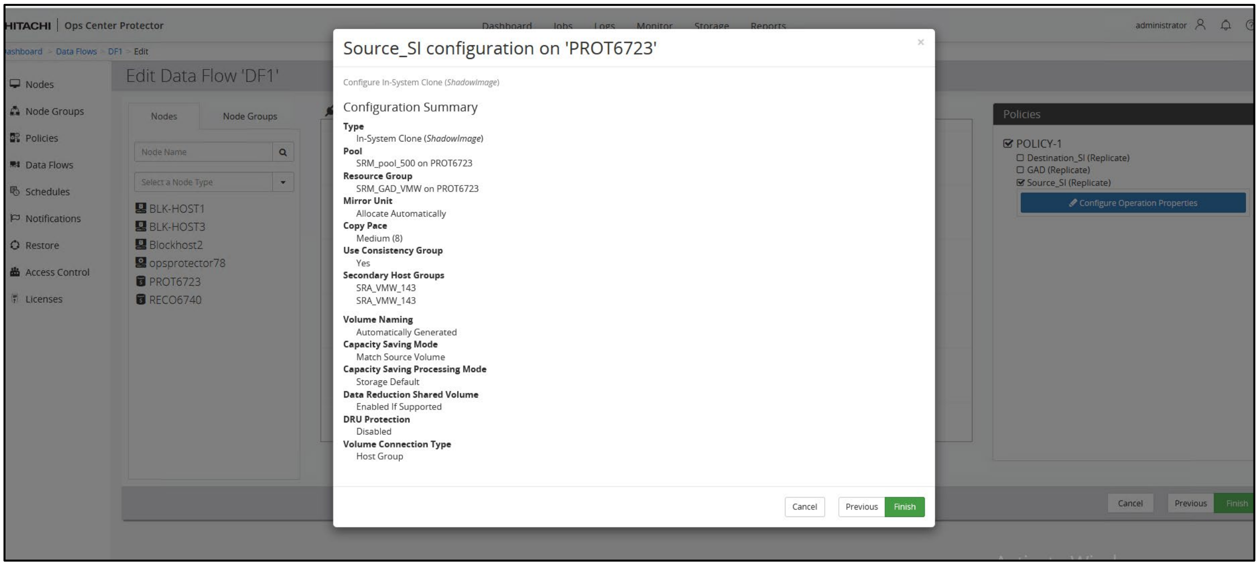
Select a Host Group

Add Host Group

If replication SVOLs are exposed to a host, users must ensure that they are not in use during replication resynchronization, otherwise critical system failure may occur on the host machine.

Cancel | Previous | Next

9. Click **Finish**.



Source_SI configuration on 'PROT6723'

Configure In-System Clone (*ShadowImage*)

Configuration Summary

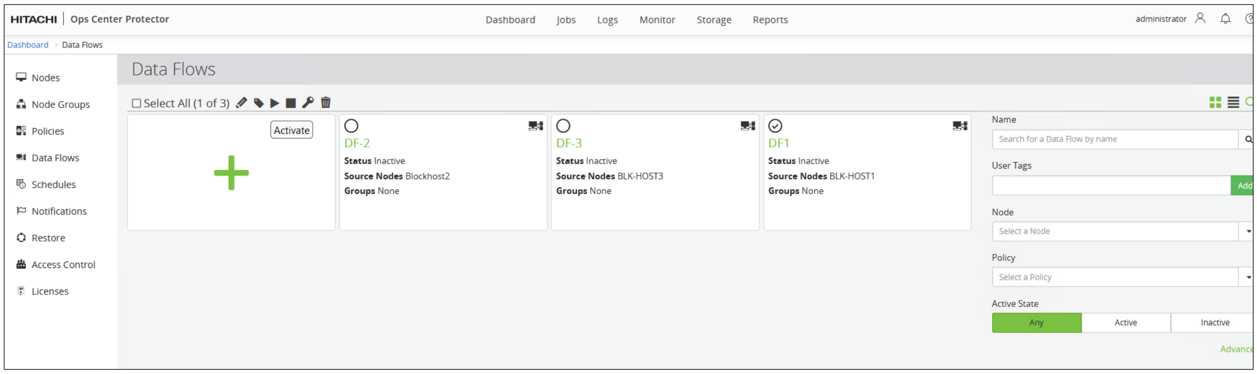
Type
In-System Clone (*ShadowImage*)
Pool
SRM_pool_500 on PROT6723
Resource Group
SRM_GAD_VMW on PROT6723
Mirror Unit
Allocate Automatically
Copy Pace
Medium (8)
Use Consistency Group
Yes
Secondary Host Groups
SRA_VMW_143
SRA_VMW_143
Volume Naming
Automatically Generated
Capacity Saving Mode
Match Source Volume
Capacity Saving Processing Mode
Storage Default
Data Reduction Shared Volume
Enabled If Supported
DRU Protection
Disabled
Volume Connection Type
Host Group

Cancel | Previous | Finish

The Soure_SI is created successfully.

10. Repeat the procedure to edit and configure the operations for the Destination_SI policy.

11. Select the Data Flow and click **Activate**.



○ DF-2
Status Inactive
Source Nodes Blockhost2
Groups None

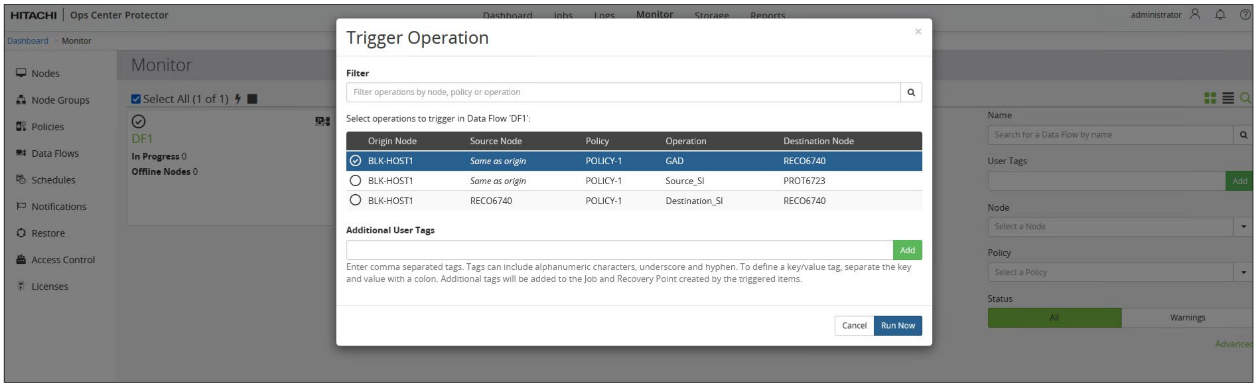
○ DF-3
Status Inactive
Source Nodes BLK-HOST3
Groups None

✓ DF1
Status Inactive
Source Nodes BLK-HOST1
Groups None

Triggering Data Flow Operations

1. Select the previously configured data flow and run each operation individually.

2. Select the GAD operation and click **Run Now**.



Trigger Operation

Select operations to trigger in Data Flow 'DF1':

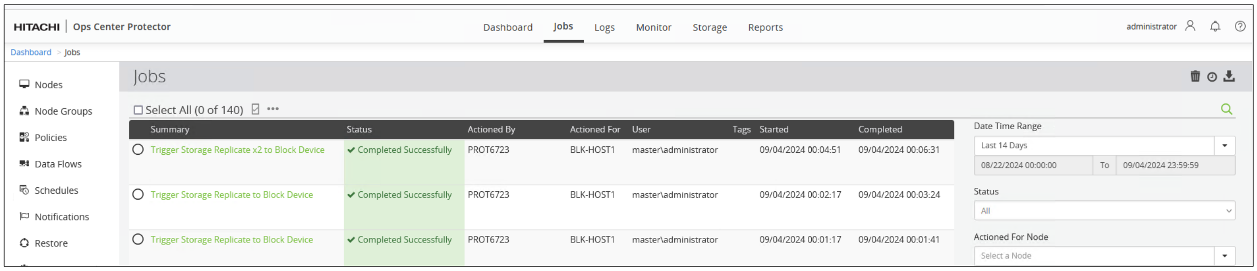
	Origin Node	Source Node	Policy	Operation	Destination Node
✓	BLK-HOST1	*Same as origin*	POLICY-1	GAD	RECO6740
○	BLK-HOST1	*Same as origin*	POLICY-1	Source_SI	PROT6723
○	BLK-HOST1	RECO6740	POLICY-1	Destination_SI	RECO6740

Additional User Tags

Enter comma separated tags. Tags can include alphanumeric characters, underscore and hyphen. To define a key/value tag, separate the key and value with a colon. Additional tags will be added to the Job and Recovery Point created by the triggered items.

3. Select the subsequent operations and click **Run Now**.

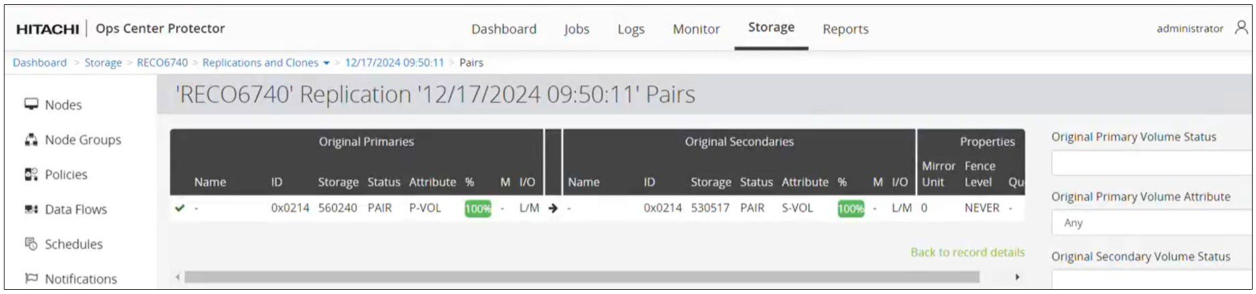
4. Verify whether the trigger operation has run successfully.



	Summary	Status	Actioned By	Actioned For	User	Tags	Started	Completed
○	Trigger Storage Replicate x2 to Block Device	✓ Completed Successfully	PROT6723	BLK-HOST1	master\administrator		09/04/2024 00:04:51	09/04/2024 00:06:31
○	Trigger Storage Replicate to Block Device	✓ Completed Successfully	PROT6723	BLK-HOST1	master\administrator		09/04/2024 00:02:17	09/04/2024 00:03:24
○	Trigger Storage Replicate to Block Device	✓ Completed Successfully	PROT6723	BLK-HOST1	master\administrator		09/04/2024 00:01:17	09/04/2024 00:01:41

The GAD Pair is created successfully.

5. Verify the GAD pair.


HITACHI | Ops Center Protector
Dashboard
Jobs
Logs
Monitor
Storage
Reports
administrator
Dashboard > Storage > RECO6740 > Replications and Clones > 12/17/2024 09:50:11 > Pairs
Nodes
Node Groups
Policies
Data Flows
Schedules
Notifications

'RECO6740' Replication '12/17/2024 09:50:11' Pairs

	Original Primaries									Original Secondaries								Properties		
	Name	ID	Storage	Status	Attribute	%	M	I/O		Name	ID	Storage	Status	Attribute	%	M	I/O	Mirror Unit	Fence Level	Qu
✓	-	0x0214	560240	PAIR	P-VOL	100%	-	L/M	→	-	0x0214	530517	PAIR	S-VOL	100%	-	L/M	0	NEVER	-

Original Primary Volume Status

Original Primary Volume Attribute
Any

Original Secondary Volume Status

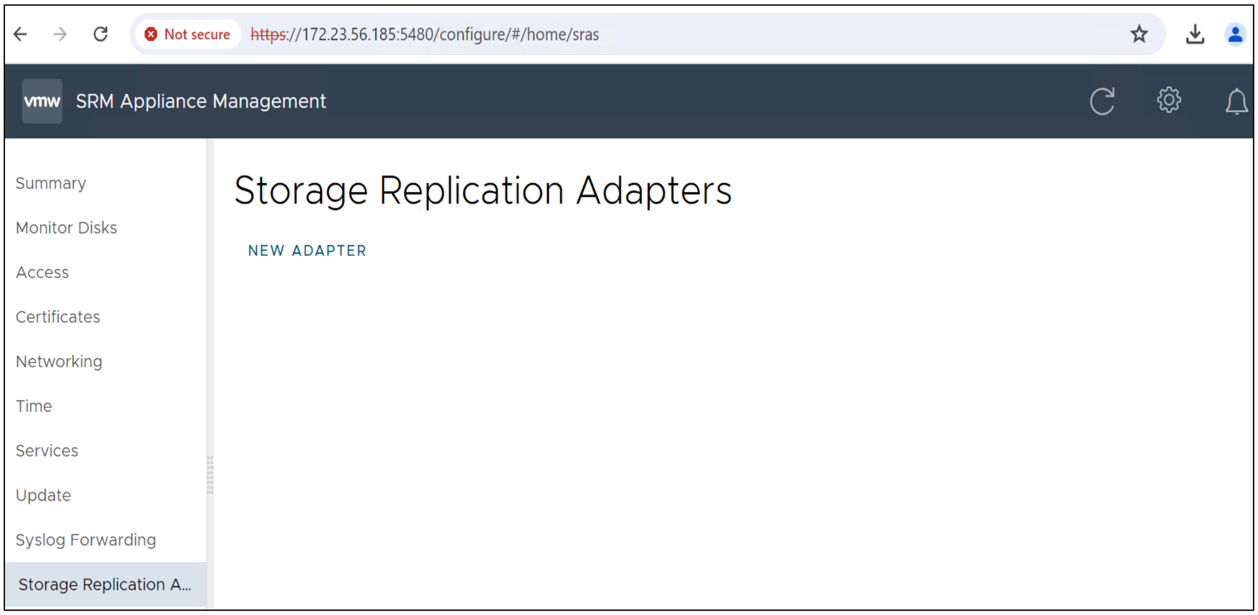
Installing SRA and Configuring SRM

Installing Ops Center Protector SRA

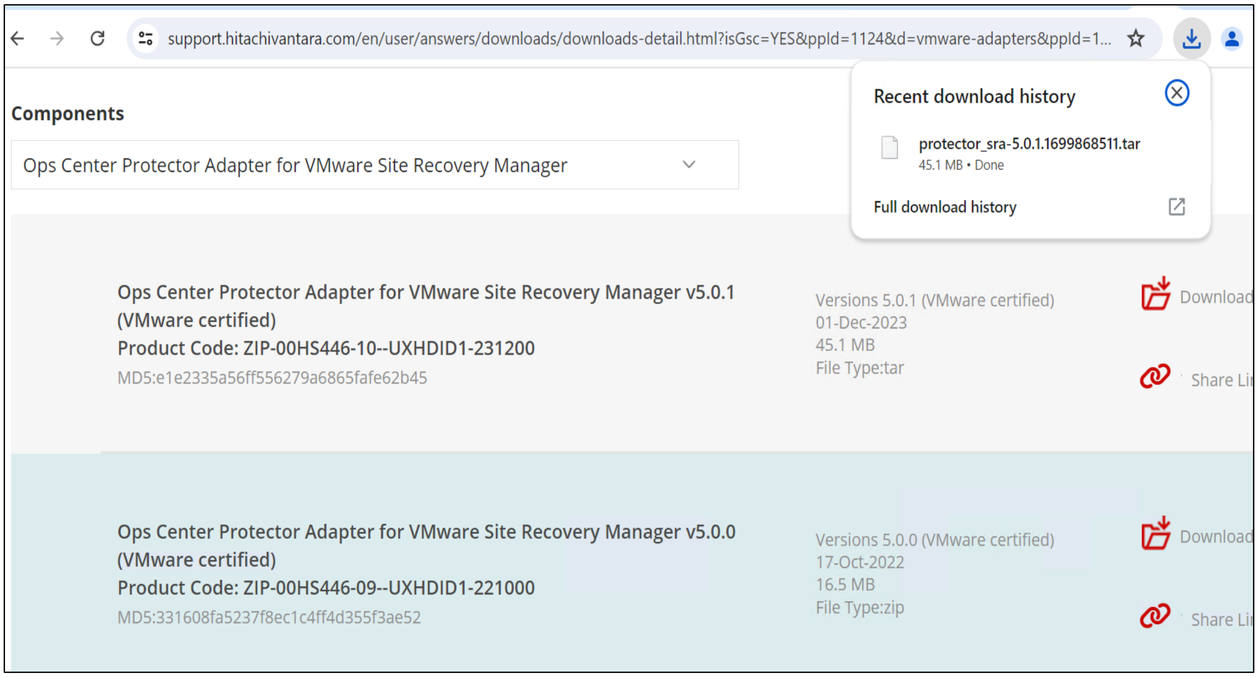
Ops Center Protector Adapter for VMware SRM is an integration module that connects Hitachi Ops Center Protector with VMware SRM to enhance disaster recovery and data protection capabilities in virtualized environments. To install the adapter, complete the following steps:

1. Download the adapter package and extract the contents on the VMware SRM server from https://support.hitachivantara.com/.

2. Navigate to the primary SRM site, select **Storage Replication Adapters**, and click **NEW ADAPTER**.



3. Upload the downloaded protector file. You can download the file from support.hitachivantara.com.



support.hitachivantara.com/en/user/answers/downloads/downloads-detail.html?isGsc=YES&ppId=1124&d=vmware-adapters&ppId=1...

Recent download history

protector_sra-5.0.1.1699868511.tar
45.1 MB • Done

Full download history

Components

Ops Center Protector Adapter for VMware Site Recovery Manager

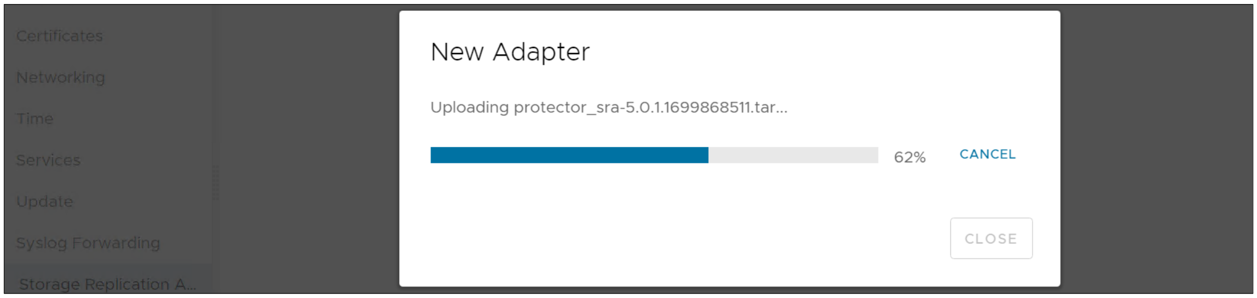
Ops Center Protector Adapter for VMware Site Recovery Manager v5.0.1 (VMware certified)
Product Code: ZIP-00HS446-10--UXHDID1-231200
MD5:e1e2335a56ff556279a6865fafe62b45

Versions 5.0.1 (VMware certified)
01-Dec-2023
45.1 MB
File Type:tar

Ops Center Protector Adapter for VMware Site Recovery Manager v5.0.0 (VMware certified)
Product Code: ZIP-00HS446-09--UXHDID1-221000
MD5:331608fa5237f8ec1c4ff4d355f3ae52

Versions 5.0.0 (VMware certified)
17-Oct-2022
16.5 MB
File Type:zip

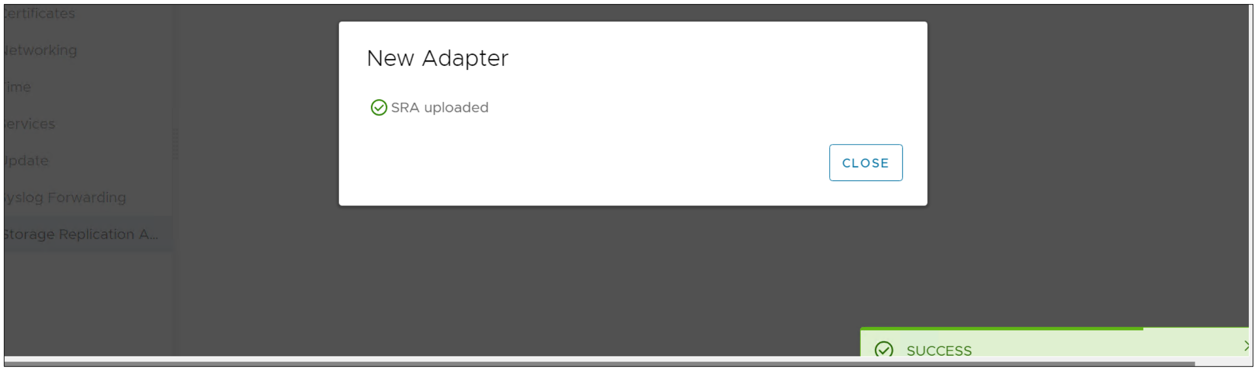
4. Click **New Adapter** and upload the file to the SRM site.



New Adapter

Uploading protector_sra-5.0.1.1699868511.tar...

62%

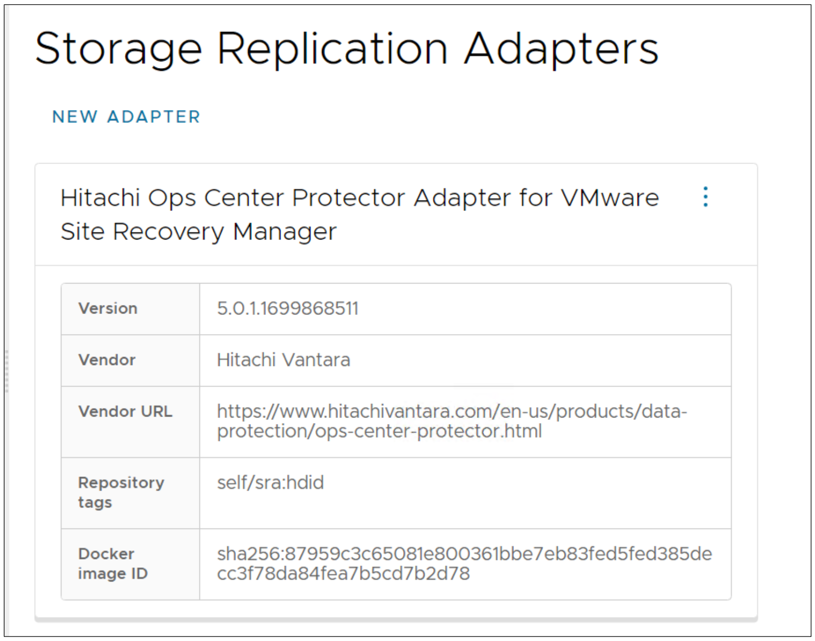


New Adapter

SRA uploaded

SUCCESS

5. Verify the details of the adapter on the primary site.

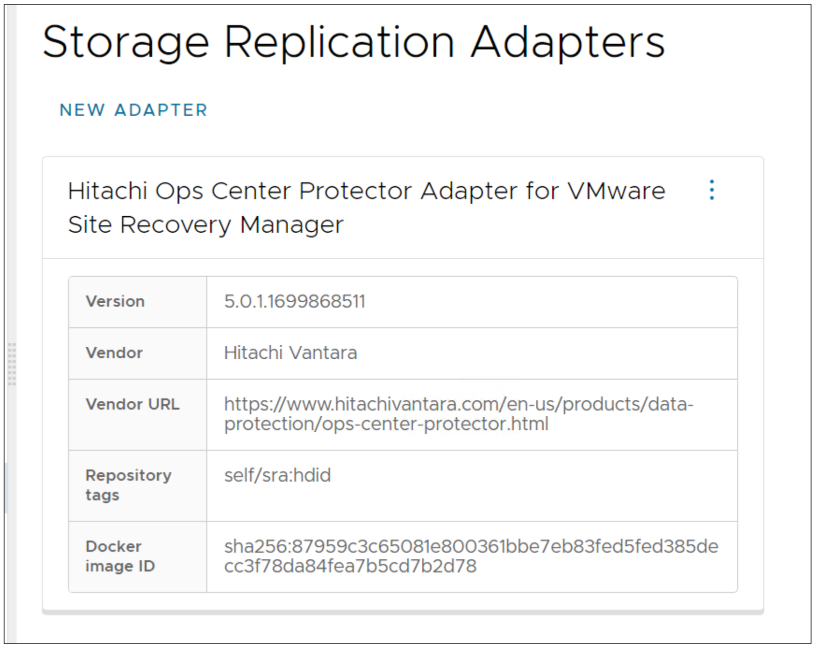


Storage Replication Adapters

Hitachi Ops Center Protector Adapter for VMware Site Recovery Manager

Version	5.0.1.1699868511
Vendor	Hitachi Vantara
Vendor URL	https://www.hitachivantara.com/en-us/products/data-protection/ops-center-protector.html
Repository tags	self/sra:hdid
Docker image ID	sha256:87959c3c65081e800361bbe7eb83fed5fed385decc3f78da84fea7b5cd7b2d78

6. Verify the same for the secondary SRM site.



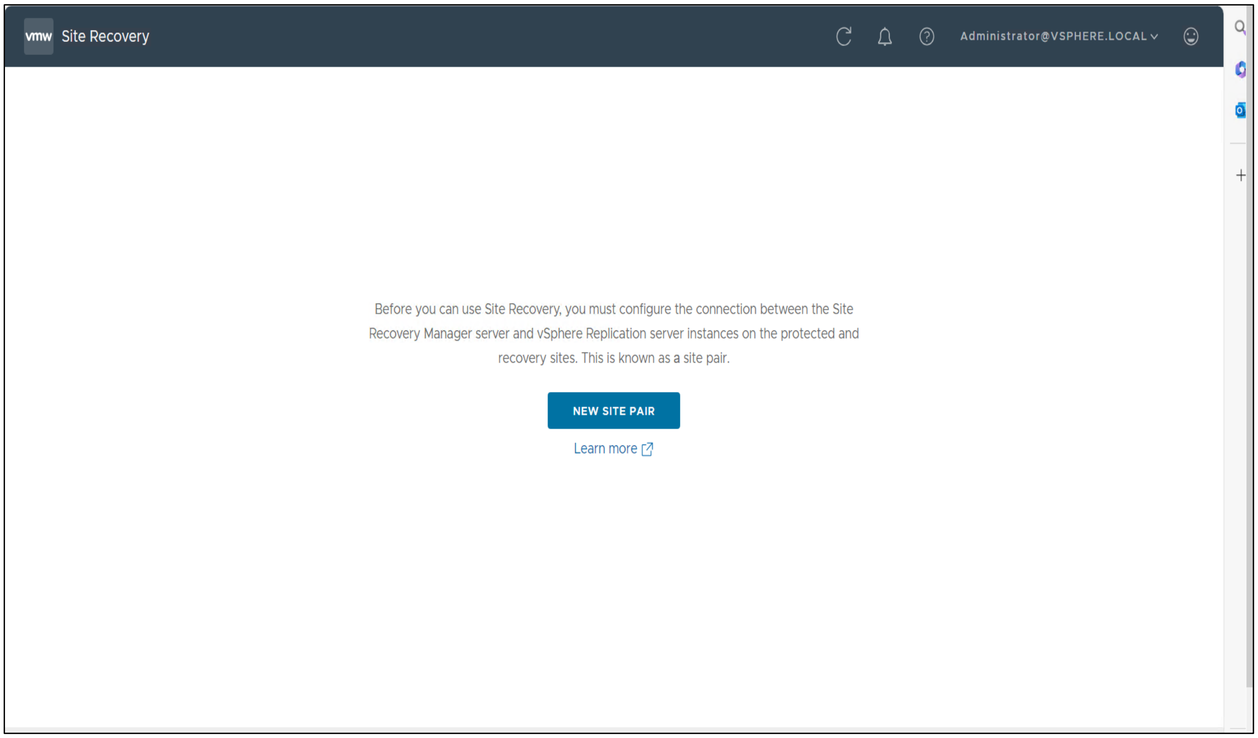
Storage Replication Adapters

Hitachi Ops Center Protector Adapter for VMware Site Recovery Manager

Version	5.0.1.1699868511
Vendor	Hitachi Vantara
Vendor URL	https://www.hitachivantara.com/en-us/products/data-protection/ops-center-protector.html
Repository tags	self/sra:hdid
Docker image ID	sha256:87959c3c65081e800361bbe7eb83fed5fed385decc3f78da84fea7b5cd7b2d78

Creating an SRM Site Pair

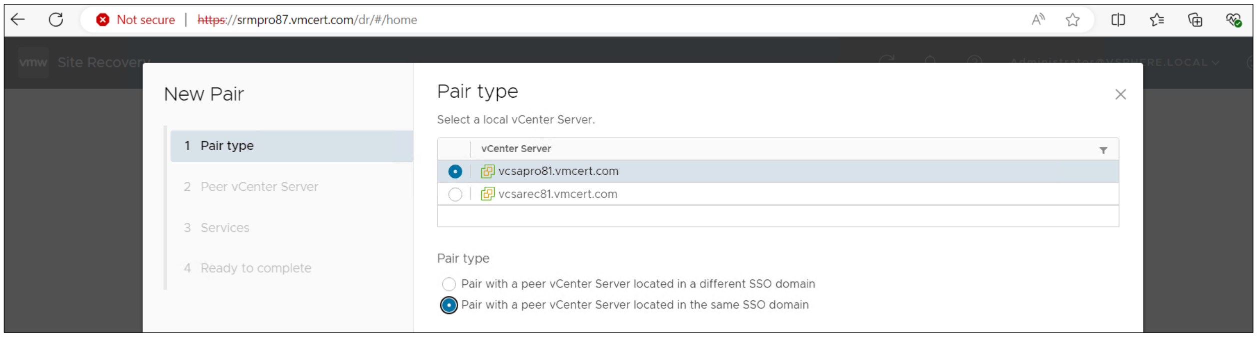
1. Navigate to the primary SRM interface and click **New Site Pair**.



Site Recovery

Before you can use Site Recovery, you must configure the connection between the Site Recovery Manager server and vSphere Replication server instances on the protected and recovery sites. This is known as a site pair.

2. Select the pair type and the local vCenter server as follows and click **NEXT**.



Not secure | https://srmpro87.vmcert.com/dr/#/home

New Pair

1 Pair type
2 Peer vCenter Server
3 Services
4 Ready to complete

Pair type

Select a local vCenter Server.

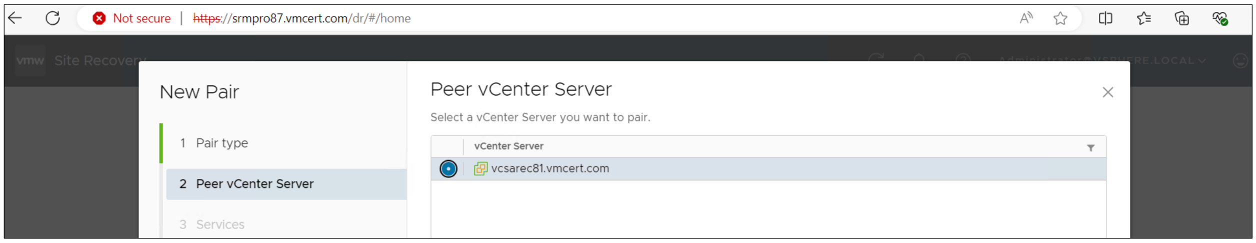
	vCenter Server
●	vcsapro81.vmcert.com
○	vcsarec81.vmcert.com

Pair type

○ Pair with a peer vCenter Server located in a different SSO domain

● Pair with a peer vCenter Server located in the same SSO domain

3. Select the vCenter server you want to pair with and click **NEXT**.



Not secure | https://srmpro87.vmcert.com/dr/#/home

New Pair

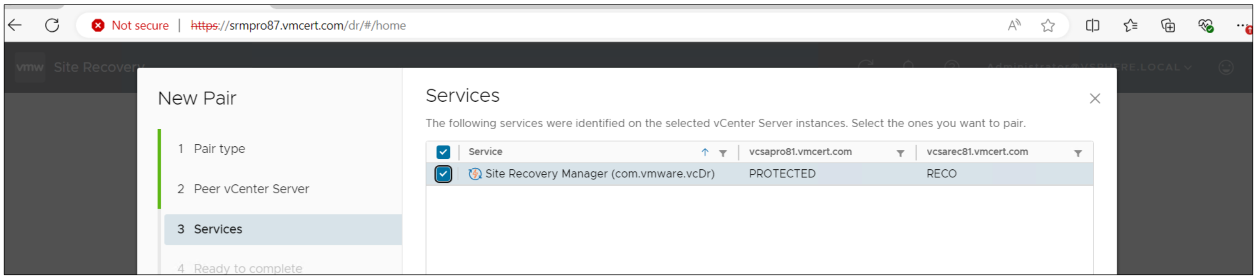
1 Pair type
2 Peer vCenter Server
3 Services

Peer vCenter Server

Select a vCenter Server you want to pair.

	vCenter Server
●	vcsarec81.vmcert.com

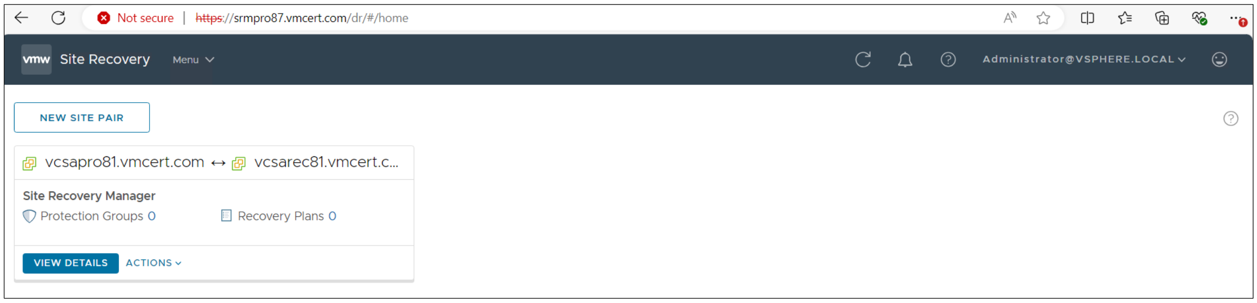
4. Specify the services and click **NEXT**.



Services

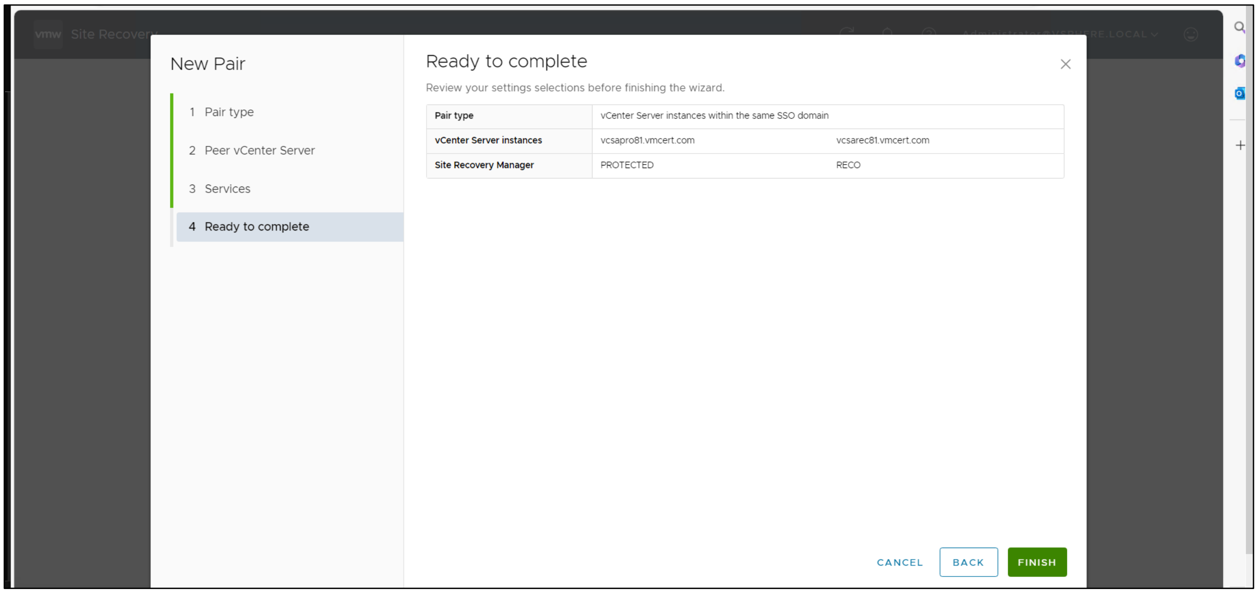
The following services were identified on the selected vCenter Server instances. Select the ones you want to pair.

☑	Service	vcsapro81.vmcert.com	vcsarec81.vmcert.com
☑	Site Recovery Manager (com.vmware.vcDr)	PROTECTED	RECO



Not secure | https://srmpro87.vmcert.com/dr/#/home
vmw Site Recovery
Menu
Administrator@VSPHERE.LOCAL
NEW SITE PAIR
vcsapro81.vmcert.com ↔ vcsarec81.vmcert.c...
Site Recovery Manager
Protection Groups 0
Recovery Plans 0
VIEW DETAILS
ACTIONS

5. Click **Finish**.

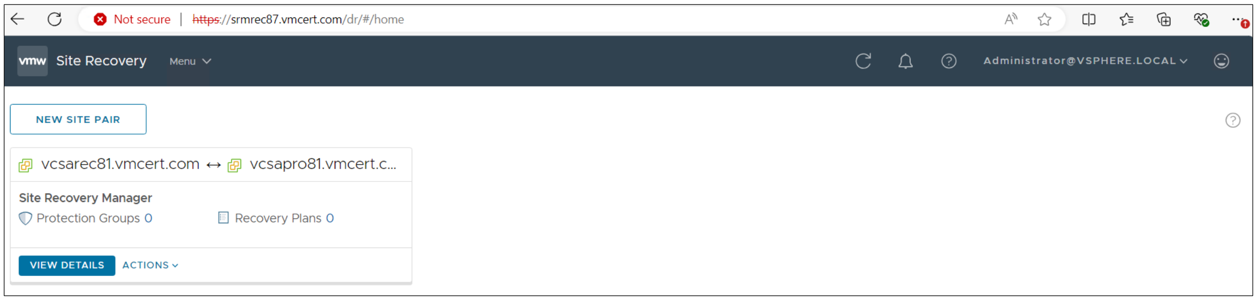


Ready to complete

Review your settings selections before finishing the wizard.

Pair type	vCenter Server instances within the same SSO domain	
vCenter Server instances	vcsapro81.vmcert.com	vcsarec81.vmcert.com
Site Recovery Manager	PROTECTED	RECO

6. Verify that the pair is created and reflected on both the sites (primary and secondary):

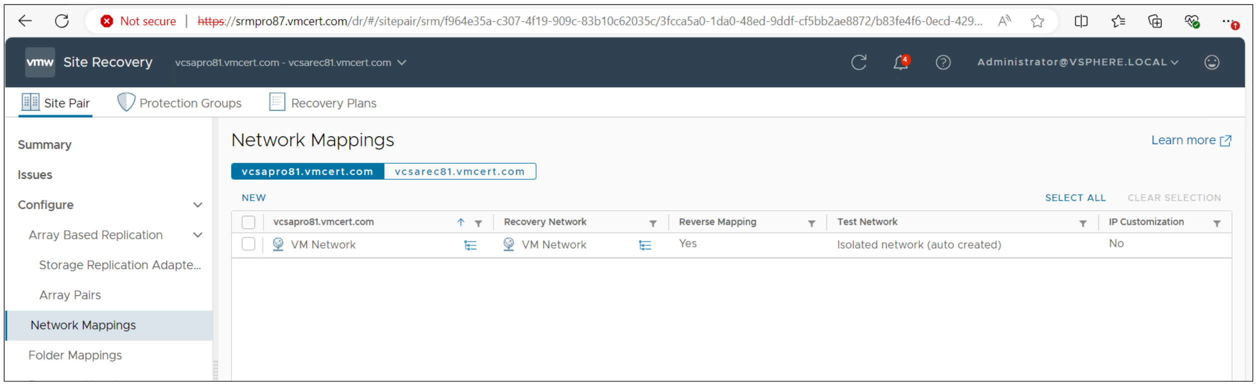


Not secure | https://srmrec87.vmcert.com/dr/#/home
vmw Site Recovery
Menu
Administrator@VSPHERE.LOCAL
NEW SITE PAIR
vcsarec81.vmcert.com ↔ vcsapro81.vmcert.c...
Site Recovery Manager
Protection Groups 0
Recovery Plans 0
VIEW DETAILS
ACTIONS

Configuring Resource Mapping

For more details on how to map the resources, create TAG, and other storage policies, see the Broadcom documentation.

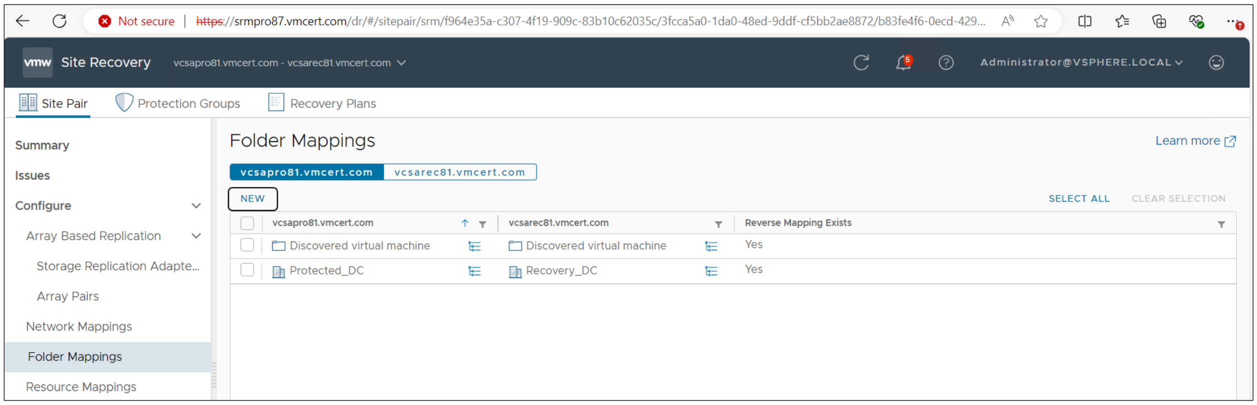
1. To create network mapping, navigate to **Configure > Network Mappings**, select the network from both sites, and map them to each other to ensure proper connectivity during recovery.


Not secure | https://srmpro87.vmcert.com/dr/#/sitepair/srm/f964e35a-c307-4f19-909c-83b10c62035c/3fcca5a0-1da0-48ed-9ddf-cf5bb2ae8872/b83fe4f6-0ecd-429...
vmw Site Recovery
vcsapro81.vmcert.com - vcsarec81.vmcert.com
Administrator@VSPHERE.LOCAL
Site Pair
Protection Groups
Recovery Plans
Summary
Issues
Configure
Array Based Replication
Storage Replication Adapte...
Array Pairs
Network Mappings
Folder Mappings
Learn more
vcsapro81.vmcert.com
vcsarec81.vmcert.com
NEW
SELECT ALL
CLEAR SELECTION

Network Mappings

vcsapro81.vmcert.com	Recovery Network	Reverse Mapping	Test Network	IP Customization
VM Network	VM Network	Yes	Isolated network (auto created)	No

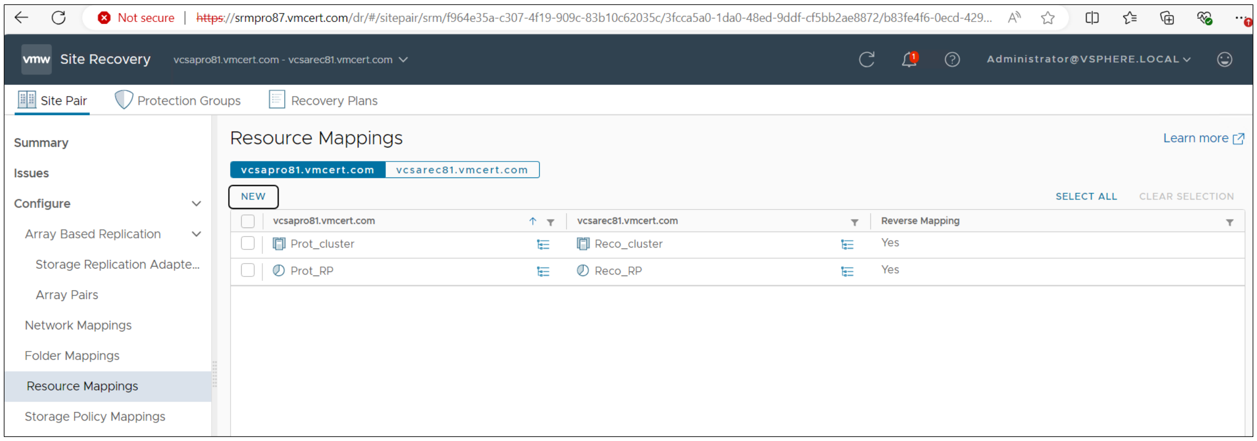
2. To create folder mapping, navigate to **Configure > Folder Mapping**, select the VM folders from both sites, and map them to align resources correctly during recovery.


Not secure | https://srmpro87.vmcert.com/dr/#/sitepair/srm/f964e35a-c307-4f19-909c-83b10c62035c/3fcca5a0-1da0-48ed-9ddf-cf5bb2ae8872/b83fe4f6-0ecd-429...
vmw Site Recovery
vcsapro81.vmcert.com - vcsarec81.vmcert.com
Administrator@VSPHERE.LOCAL
Site Pair
Protection Groups
Recovery Plans
Summary
Issues
Configure
Array Based Replication
Storage Replication Adapte...
Array Pairs
Network Mappings
Folder Mappings
Resource Mappings
Learn more
vcsapro81.vmcert.com
vcsarec81.vmcert.com
NEW
SELECT ALL
CLEAR SELECTION

Folder Mappings

vcsapro81.vmcert.com	vcsarec81.vmcert.com	Reverse Mapping Exists
Discovered virtual machine	Discovered virtual machine	Yes
Protected_DC	Recovery_DC	Yes

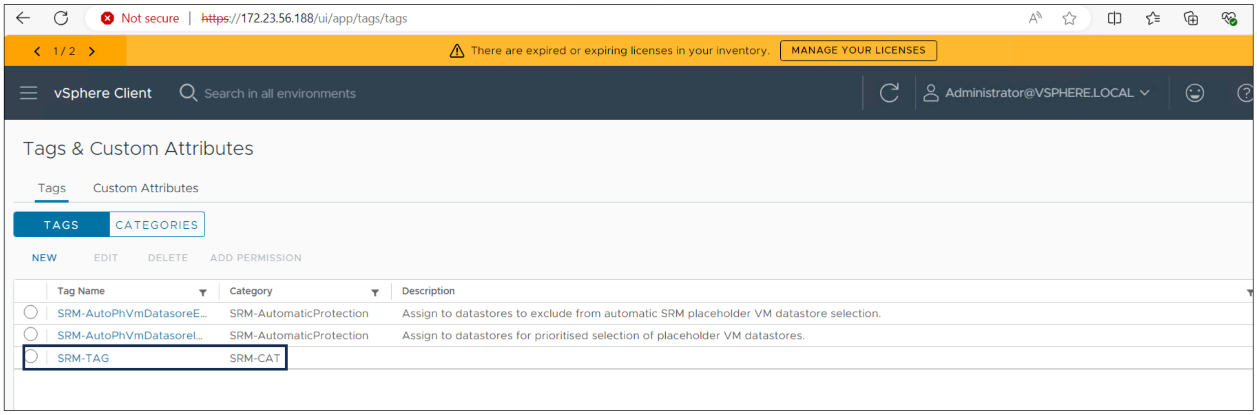
3. To create resource mapping, navigate to **SRM Settings > Resource Mapping**, select the resource from both sites, and map them to ensure proper alignment of compute resources during failover.



□	vcsapro81.vmcert.com	vcsarec81.vmcert.com	Reverse Mapping
□	Prot_cluster	Reco_cluster	Yes
□	Prot_RP	Reco_RP	Yes

4. For storage policy tagging, navigate to **vSphere Client** > **Tags & Custom Attributes**, and create a new tag category.

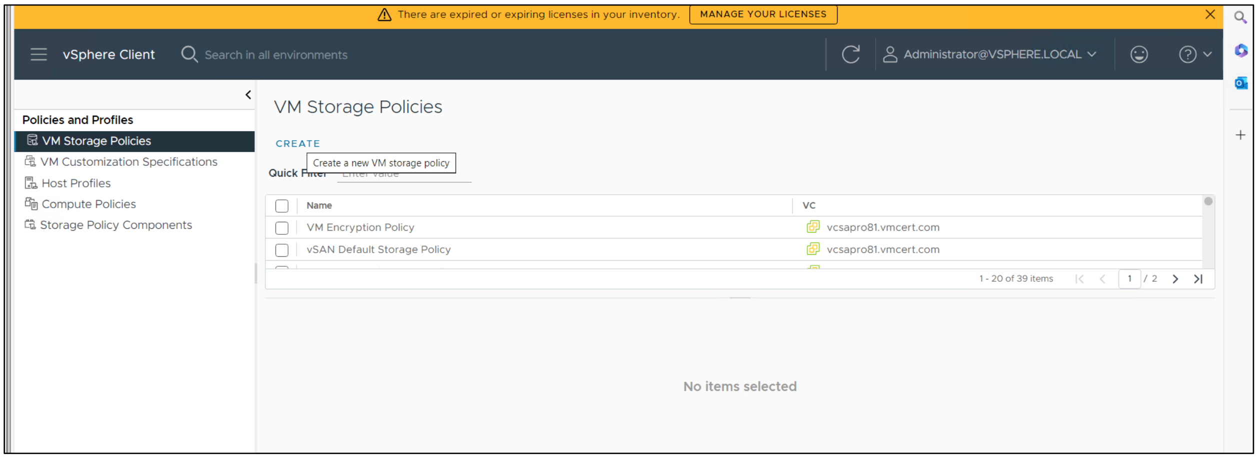
5. Create a TAG. Click **NEW** and assign it to the relevant datastore. In this scenario, SRM-TAG is created in the TAGS section.



There are expired or expiring licenses in your inventory.

	Tag Name	Category	Description
○	SRM-AutoPhVmDatasoreE...	SRM-AutomaticProtection	Assign to datastores to exclude from automatic SRM placeholder VM datastore selection.
○	SRM-AutoPhVmDatasorel...	SRM-AutomaticProtection	Assign to datastores for prioritised selection of placeholder VM datastores.
○	SRM-TAG	SRM-CAT	

6. Navigate to **VM Storage Policies**, and either create a new storage policy, or edit an existing one. To create a new policy, click **CREATE**.



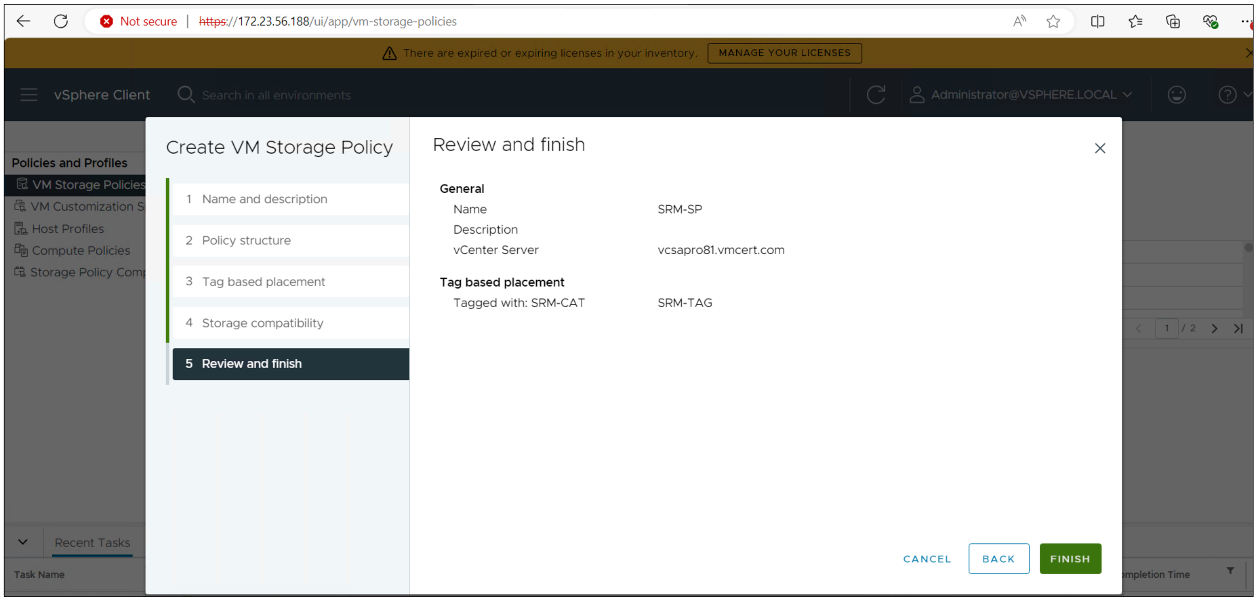
There are expired or expiring licenses in your inventory.

□	Name	VC
□	VM Encryption Policy	vcsapro81.vmcert.com
□	vSAN Default Storage Policy	vcsapro81.vmcert.com

1 - 20 of 39 items 1 / 2

No items selected

7. Complete the storage creation policy by clicking **FINISH**.



Review and finish

General

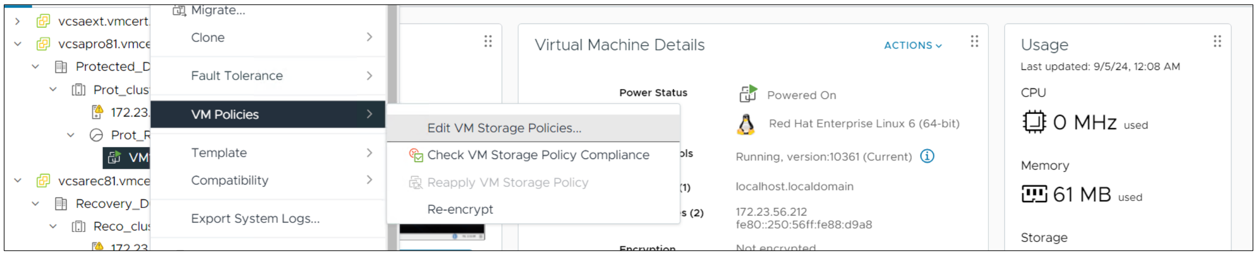
Name	SRM-SP
Description	
vCenter Server	vcsapro81.vmcert.com

Tag based placement

Tagged with: SRM-CAT	SRM-TAG

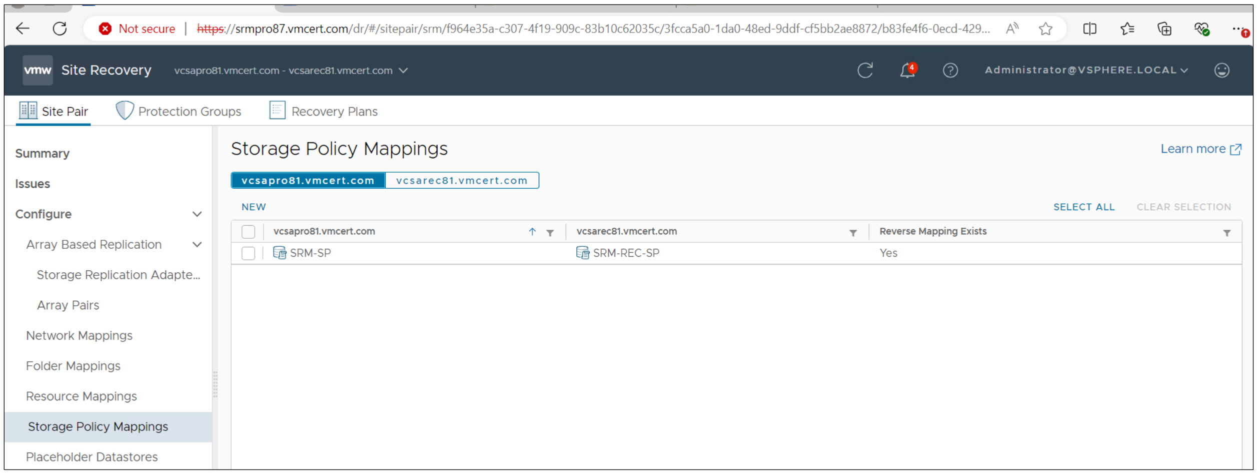
8. Associate the storage policy with the VM by adding the tag and category you created to enforce compliance, as shown in the following screenshot. This ensures that virtual machines are automatically placed on the appropriate storage based on the defined tag and category during provisioning.

9. Click the VM, select **VM Policies**, navigate to Edit VM Storage Policies, and map the policy.

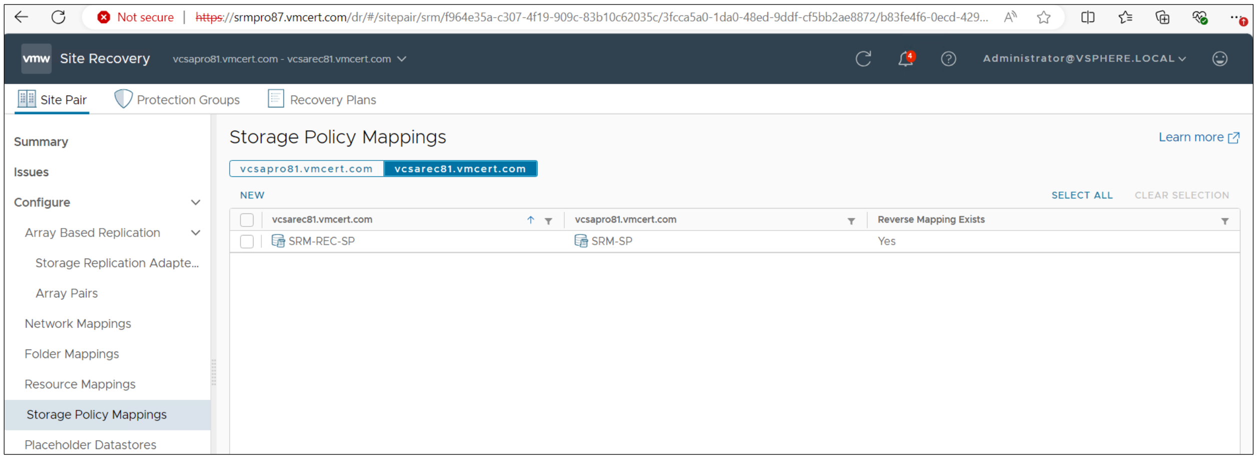


Power Status	Powered On
	Red Hat Enterprise Linux 6 (64-bit)
ols	Running, version:10361 (Current)
(1)	localhost.localdomain
s (2)	172.23.56.212 fe80::250:56ff:fe88:d9a8
Encryption	Not encrypted

Storage policy mapping is created for both primary and secondary sites:



vcsapro81.vmcert.com	vcsarec81.vmcert.com	Reverse Mapping Exists
SRM-SP	SRM-REC-SP	Yes



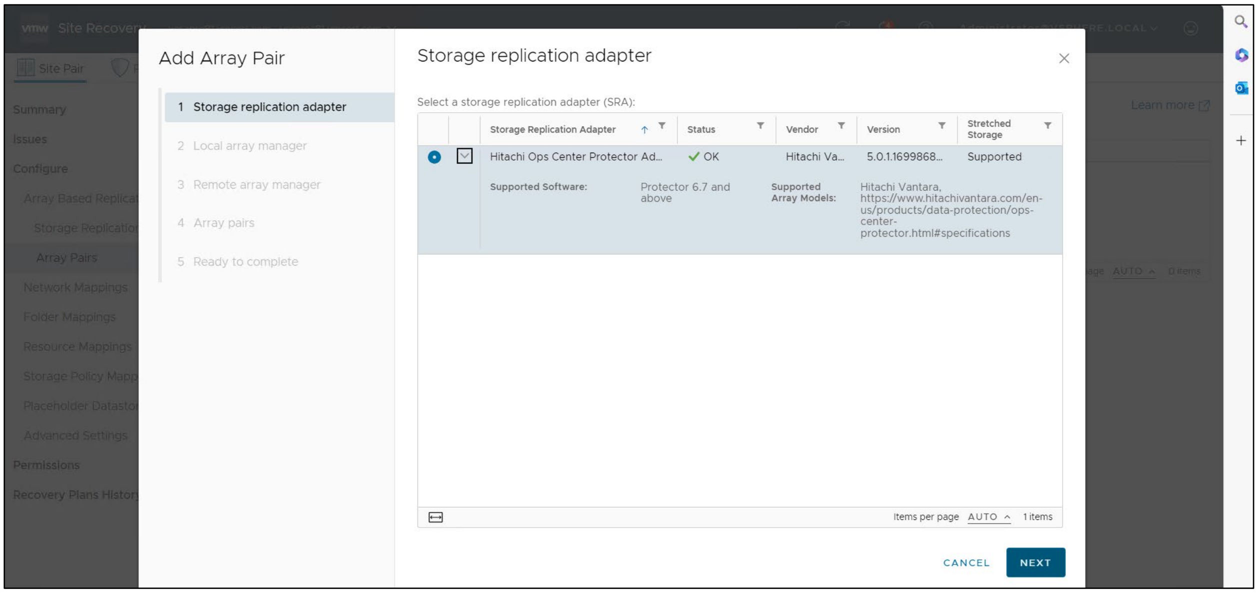
vcsarec81.vmcert.com	vcsapro81.vmcert.com	Reverse Mapping Exists
SRM-REC-SP	SRM-SP	Yes

Creating an Array Pair

An array pair in VMware SRM links storage systems at the protected and recovery sites for disaster recovery, enabling datastore replication to ensure synchronized data. To create an array pair, complete the following steps:

1. In the vSphere Client, navigate to **SRM > Configure > Array Pairs**.

2. Select **Add Array Pair** and select the storage systems from both the protected and recovery sites. Click **NEXT**.



Storage replication adapter

Select a storage replication adapter (SRA):

		Storage Replication Adapter	Status	Vendor	Version	Stretched Storage
●		Hitachi Ops Center Protector Ad...	✓ OK	Hitachi Va...	5.0.1.1699868...	Supported

Supported Software: Protector 6.7 and above

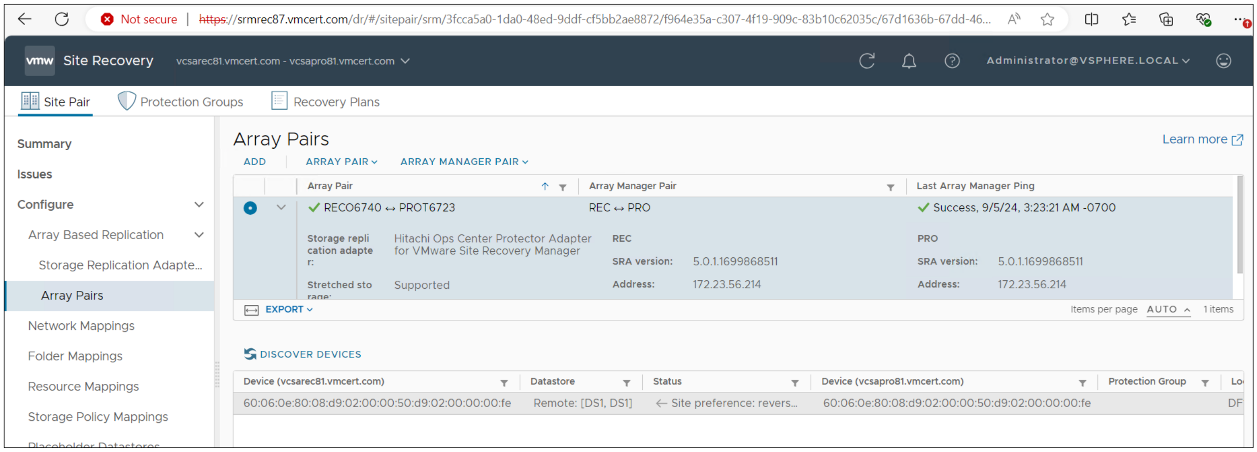
Supported Array Models: Hitachi Vantara, https://www.hitachivantara.com/en-us/products/data-protection/ops-center-protector.html#specifications

Items per page AUTO 1 items

3. Enter the connection details for both storage systems. Click **NEXT**.

4. Select the storage replication type and edit replication settings.

   The pair is created as follows:



Array Pairs

		Array Pair	Array Manager Pair	Last Array Manager Ping
●		✓ RECO6740 ↔ PROT6723	REC ↔ PRO	✓ Success, 9/5/24, 3:23:21 AM -0700

Storage replication adapter: Hitachi Ops Center Protector Adapter for VMware Site Recovery Manager

Stretched storage: Supported

REC
SRA version: 5.0.1.1699868511
Address: 172.23.56.214

PRO
SRA version: 5.0.1.1699868511
Address: 172.23.56.214

Items per page AUTO 1 items

Device (vcsarec81.vmcert.com)	Datastore	Status	Device (vcsapro81.vmcert.com)	Protection Group	Lo
60:06:0e:80:08:d9:02:00:00:50:d9:02:00:00:00:fe	Remote: [DS1, DS1]	← Site preference: revers...	60:06:0e:80:08:d9:02:00:00:50:d9:02:00:00:00:fe		DF

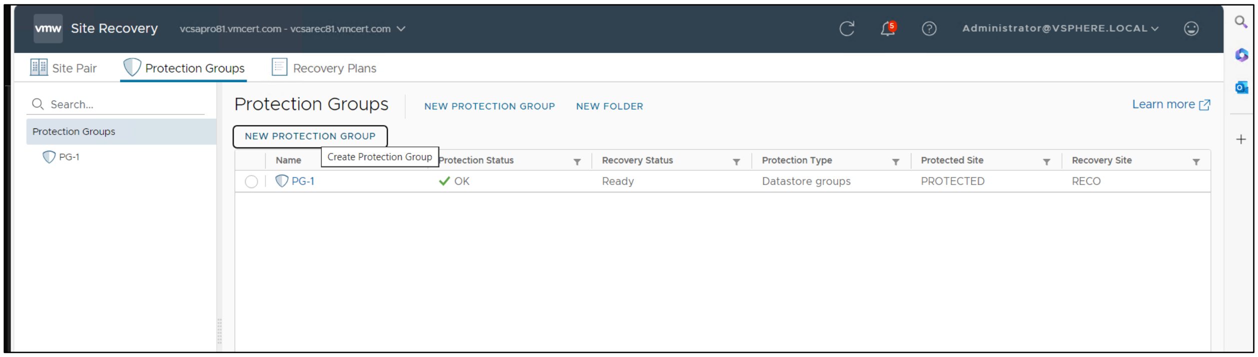
After the array pair is created, you can map datastores and configure replication between the two storage systems for disaster recovery.

Creating a Protection Group and a Recovery Plan

In VMware SRM, a protection group is a set of VMs configured for replication between protected and recovery sites. A recovery plan automates failover, including VM startups, network reconfiguration, and scripts, ensuring business continuity during disasters or migrations.

1. Log in to the vSphere Client and navigate to **Site Recovery** > **Protection Groups**.

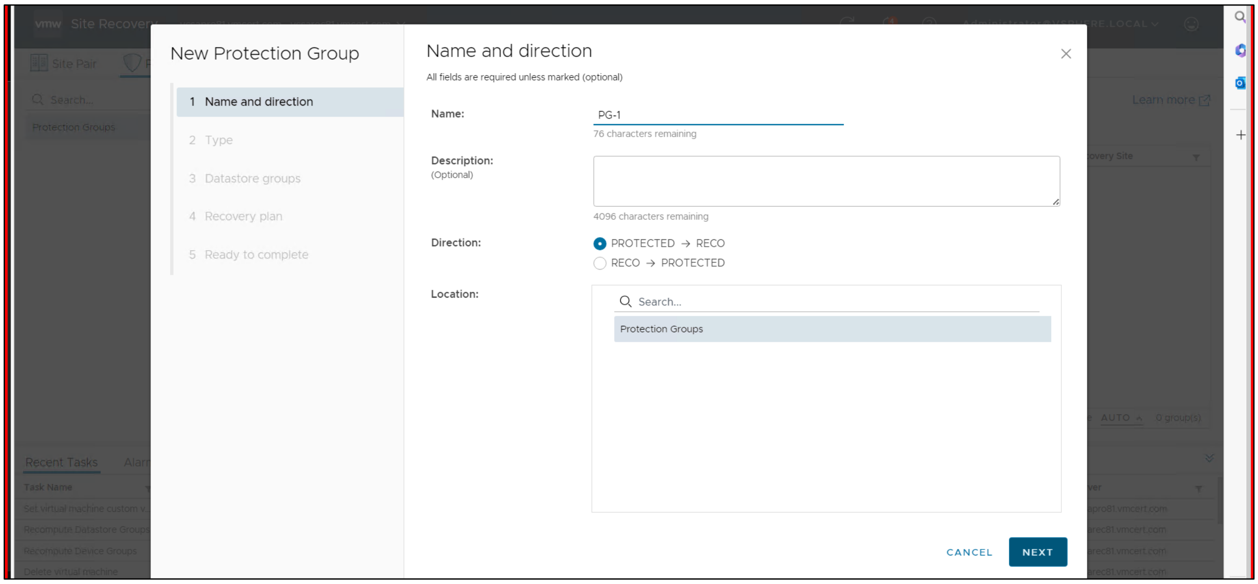
2. Click **New Protection Group**.



Protection Groups

Name	Protection Status	Recovery Status	Protection Type	Protected Site	Recovery Site
PG-1	✓ OK	Ready	Datastore groups	PROTECTED	RECO

3. Select the name and direction. Click **NEXT**.



Name and direction

All fields are required unless marked (optional)

Name: PG-1

76 characters remaining

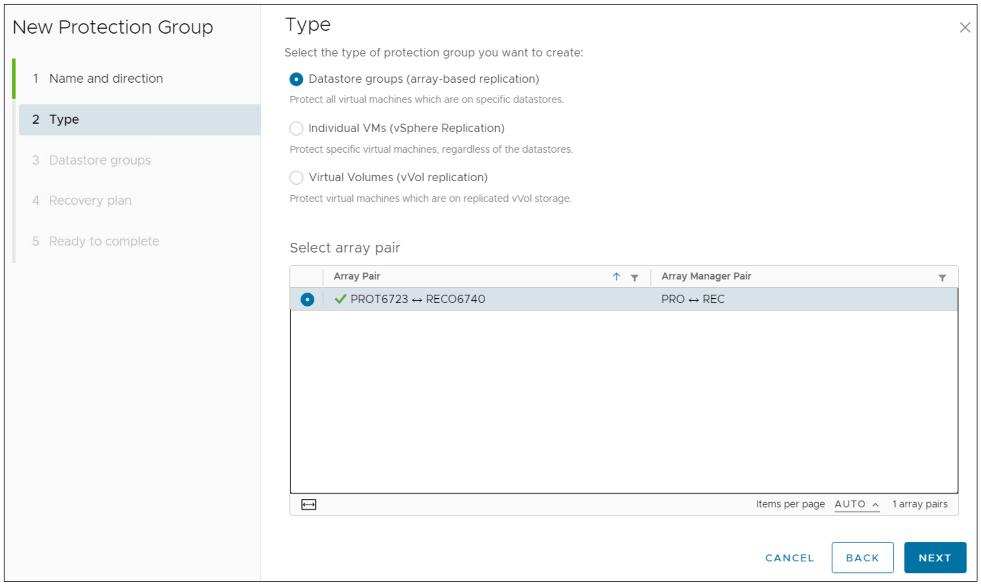
Description: (Optional)

4096 characters remaining

Direction:
● PROTECTED → RECO
○ RECO → PROTECTED

Location: Protection Groups

4. Select the type of replication. In this scenario, we selected Datastore groups (array-based replication). Click **NEXT**.



Type

Select the type of protection group you want to create:

● Datastore groups (array-based replication)
Protect all virtual machines which are on specific datastores.

○ Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.

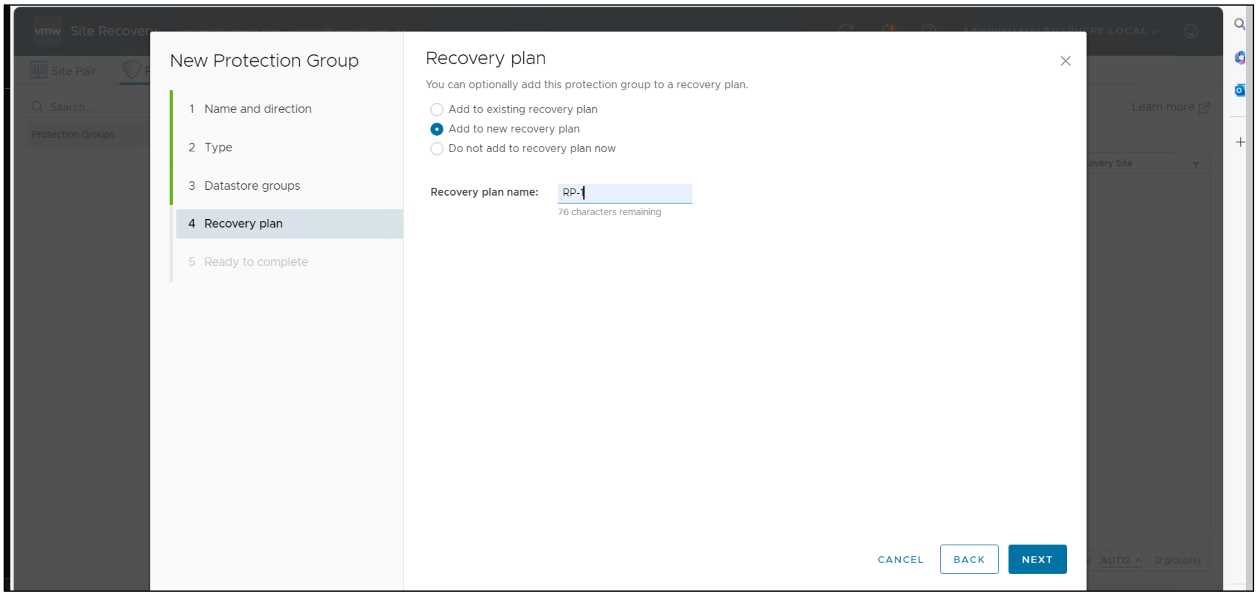
○ Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

Select array pair

	Array Pair	Array Manager Pair
●	✓ PROT6723 ↔ RECO6740	PRO ↔ REC

Items per page AUTO 1 array pairs

5. Select the recovery plan and click **NEXT**.



New Protection Group

1 Name and direction
2 Type
3 Datastore groups
4 Recovery plan
5 Ready to complete

Recovery plan

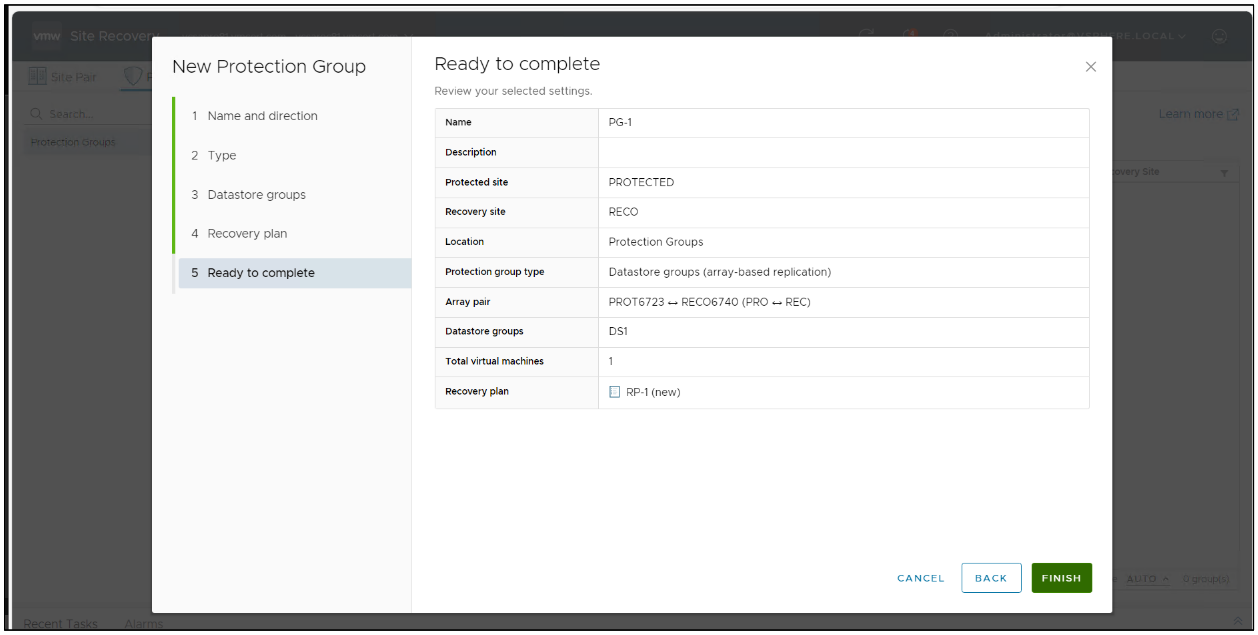
You can optionally add this protection group to a recovery plan.

○ Add to existing recovery plan
● Add to new recovery plan
○ Do not add to recovery plan now

Recovery plan name: RP-1

76 characters remaining

6. Review the summary and click **FINISH**.



New Protection Group

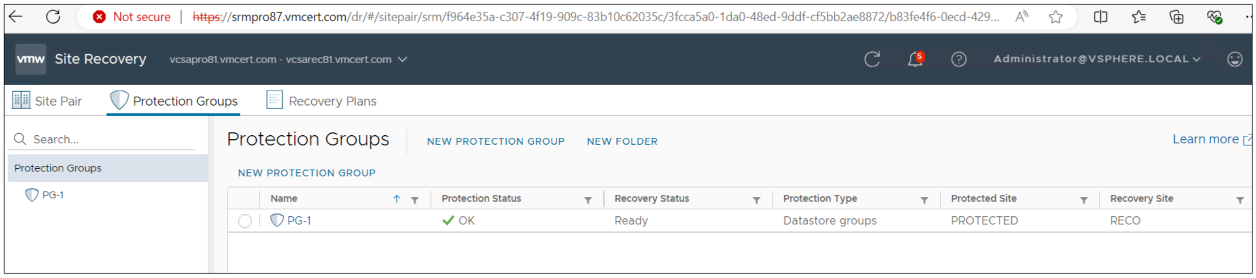
1 Name and direction
2 Type
3 Datastore groups
4 Recovery plan
5 Ready to complete

Ready to complete

Review your selected settings.

Name	PG-1
Description	
Protected site	PROTECTED
Recovery site	RECO
Location	Protection Groups
Protection group type	Datastore groups (array-based replication)
Array pair	PROT6723 ↔ RECO6740 (PRO ↔ REC)
Datastore groups	DS1
Total virtual machines	1
Recovery plan	RP-1 (new)

The Protection Group is created.

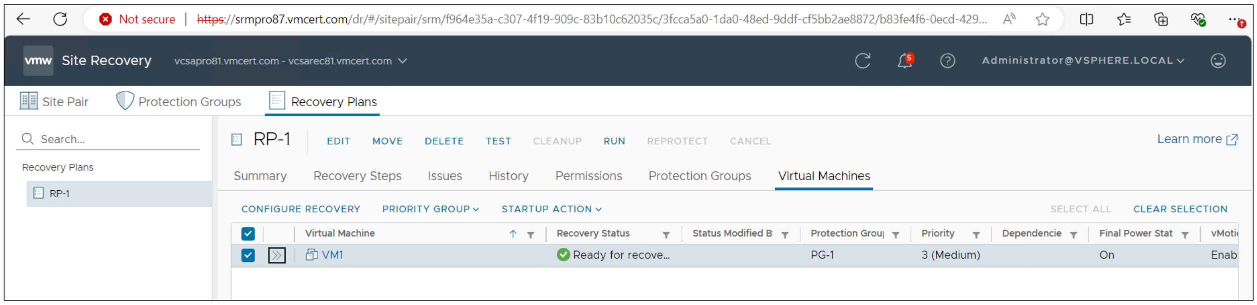


Not secure | ~~https~~://srmpro87.vmcert.com/dr/#/sitepair/srm/f964e35a-c307-4f19-909c-83b10c62035c/3fcca5a0-1da0-48ed-9ddf-cf5bb2ae8872/b83fe4f6-0ecd-429...

Protection Groups

Name	Protection Status	Recovery Status	Protection Type	Protected Site	Recovery Site
PG-1	✓ OK	Ready	Datastore groups	PROTECTED	RECO

7. Verify that the recovery plan is created.

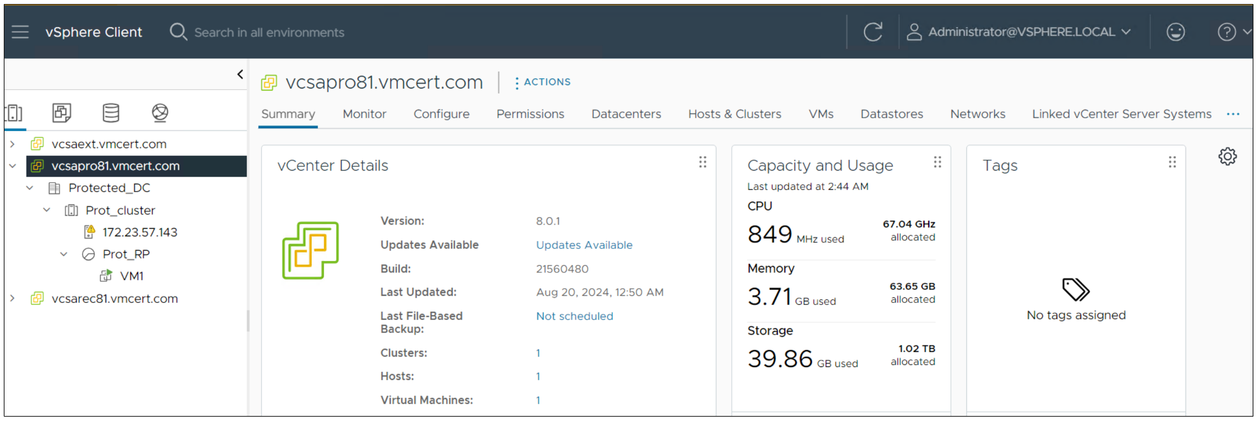


☑	Virtual Machine	Recovery Status	Status Modified B	Protection Grou|	Priority	Dependencie	Final Power Stat	vMoti
☑	VM1	✓ Ready for recove...		PG-1	3 (Medium)		On	Enab

SRM Operation

Planned Migration Test

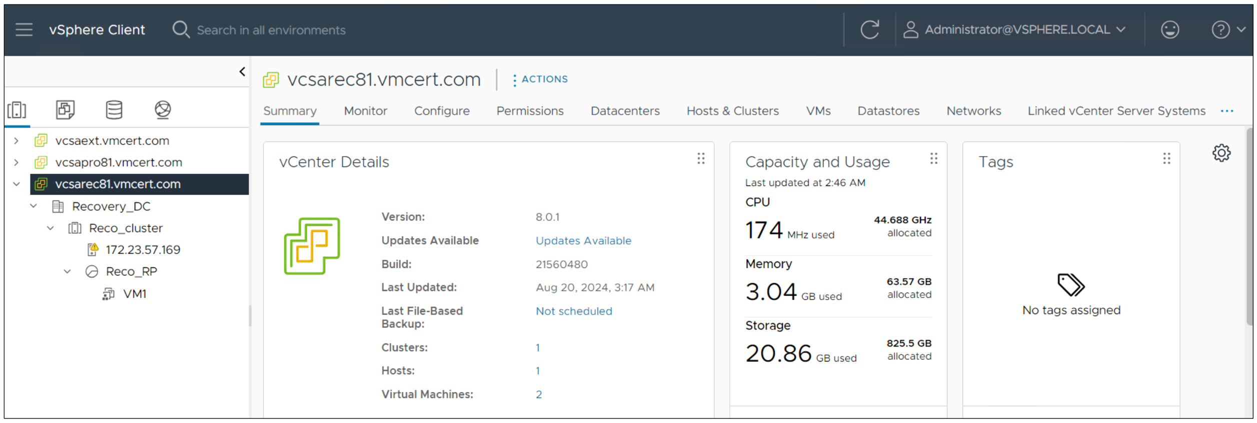
1. Log in to the VCSA where the VM resides and verify the primary host status.



Version: 8.0.1
Updates Available: Updates Available
Build: 21560480
Last Updated: Aug 20, 2024, 12:50 AM
Last File-Based Backup: Not scheduled
Clusters: 1
Hosts: 1
Virtual Machines: 1

Capacity and Usage
Last updated at 2:44 AM
CPU: 849 MHz used, 67.04 GHz allocated
Memory: 3.71 GB used, 63.65 GB allocated
Storage: 39.86 GB used, 1.02 TB allocated

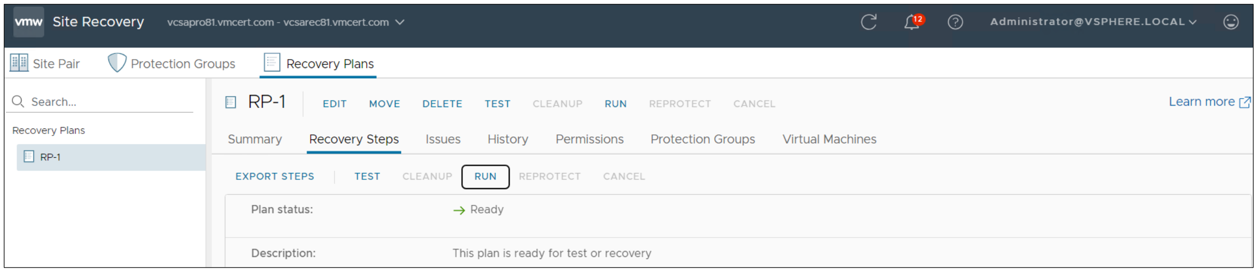
2. Verify the secondary host status.



Version: 8.0.1
Updates Available: Updates Available
Build: 21560480
Last Updated: Aug 20, 2024, 3:17 AM
Last File-Based Backup: Not scheduled
Clusters: 1
Hosts: 1
Virtual Machines: 2

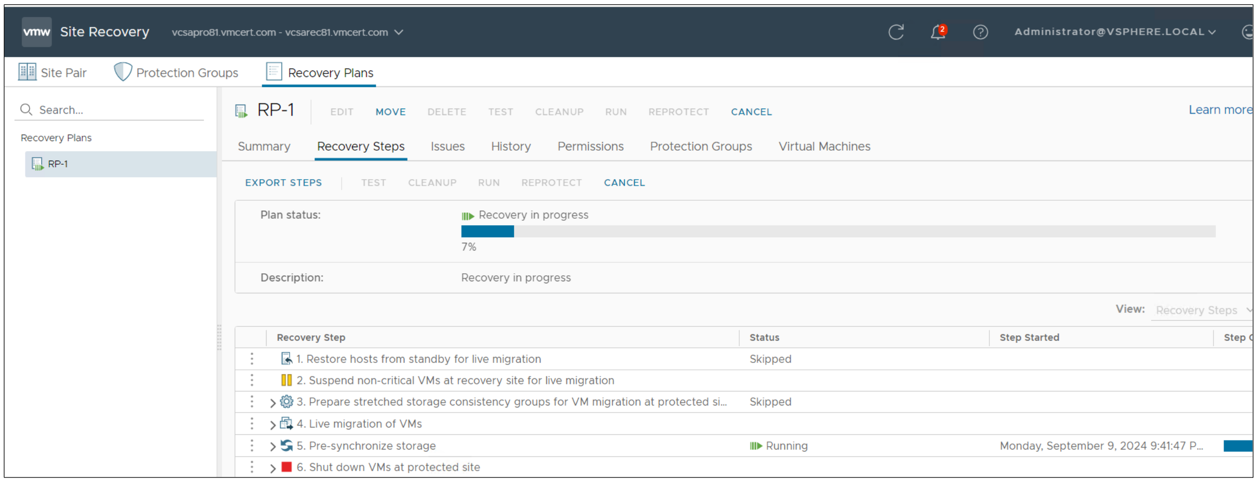
Capacity and Usage
Last updated at 2:46 AM
CPU: 174 MHz used, 44.688 GHz allocated
Memory: 3.04 GB used, 63.57 GB allocated
Storage: 20.86 GB used, 825.5 GB allocated

3. Log in to the SRM site and run the failover test. Click **RUN**.



Plan status: → Ready
Description: This plan is ready for test or recovery

4. Verify the test progress.



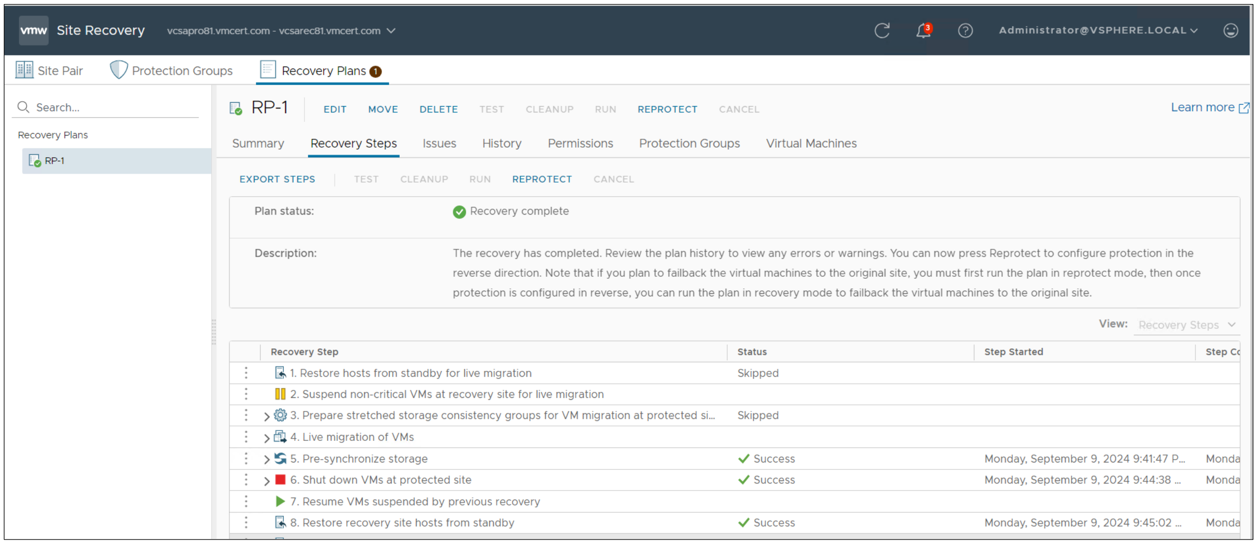
Plan status: Recovery in progress

7%

Description: Recovery in progress

Recovery Step	Status	Step Started	Step C
1. Restore hosts from standby for live migration	Skipped		
2. Suspend non-critical VMs at recovery site for live migration			
3. Prepare stretched storage consistency groups for VM migration at protected si...	Skipped		
4. Live migration of VMs			
5. Pre-synchronize storage	Running	Monday, September 9, 2024 9:41:47 P...	
6. Shut down VMs at protected site			

5. Check whether the test status shows Recovery complete.

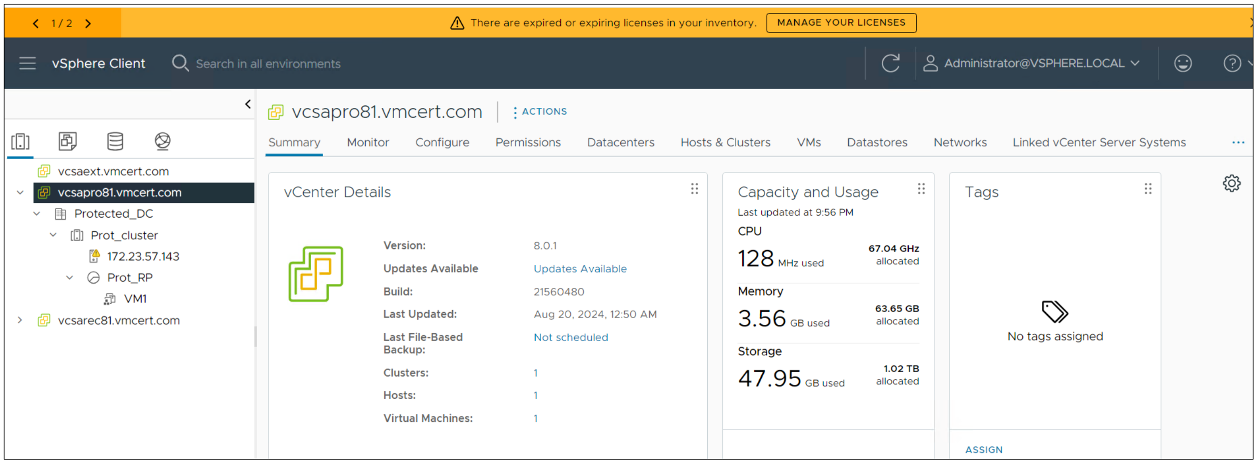


Plan status: ✓ Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Recovery Step	Status	Step Started	Step Co
1. Restore hosts from standby for live migration	Skipped		
2. Suspend non-critical VMs at recovery site for live migration			
3. Prepare stretched storage consistency groups for VM migration at protected si...	Skipped		
4. Live migration of VMs			
5. Pre-synchronize storage	✓ Success	Monday, September 9, 2024 9:41:47 P...	Monda
6. Shut down VMs at protected site	✓ Success	Monday, September 9, 2024 9:44:38 ...	Monda
7. Resume VMs suspended by previous recovery			
8. Restore recovery site hosts from standby	✓ Success	Monday, September 9, 2024 9:45:02 ...	Monda

6. Check the status of the primary host from the vSphere Client after running the failover test operation:



vcsapro81.vmcert.com

vCenter Details

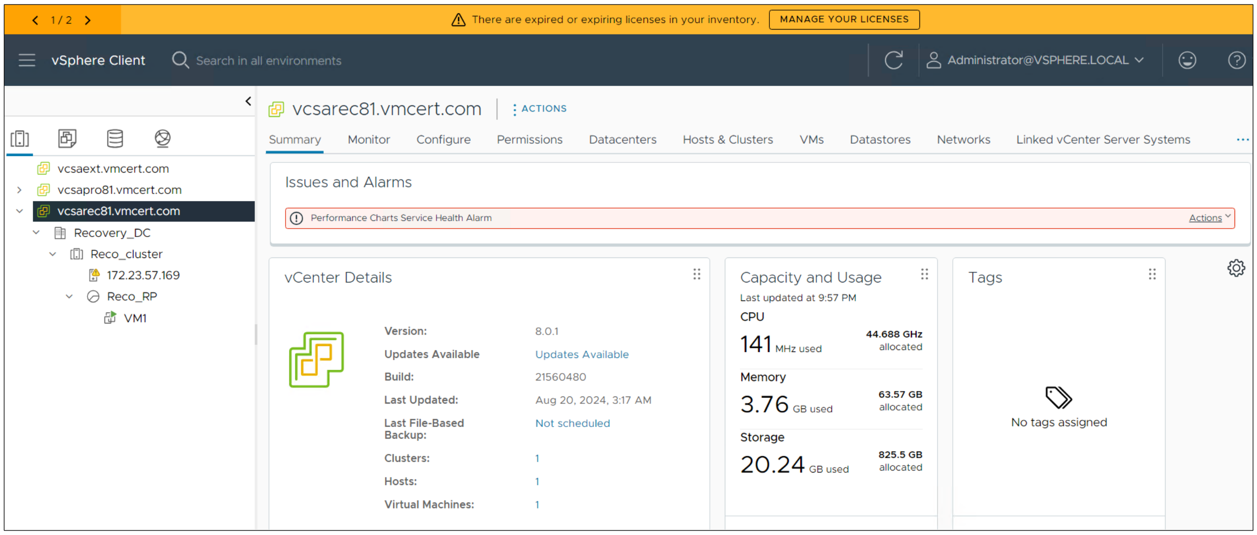
Version:	8.0.1
Updates Available	Updates Available
Build:	21560480
Last Updated:	Aug 20, 2024, 12:50 AM
Last File-Based Backup:	Not scheduled
Clusters:	1
Hosts:	1
Virtual Machines:	1

Capacity and Usage

Last updated at 9:56 PM

	Used	Allocated
CPU	128 MHz used	67.04 GHz allocated
Memory	3.56 GB used	63.65 GB allocated
Storage	47.95 GB used	1.02 TB allocated

7. Check the status of the VM located on the secondary host after the test operation is run. In this scenario, the VM was migrated to the secondary site after the test was completed.



There are expired or expiring licenses in your inventory. MANAGE YOUR LICENSES

vcsarec81.vmcert.com

Issues and Alarms

Performance Charts Service Health Alarm

vCenter Details

Version:	8.0.1
Updates Available	Updates Available
Build:	21560480
Last Updated:	Aug 20, 2024, 3:17 AM
Last File-Based Backup:	Not scheduled
Clusters:	1
Hosts:	1
Virtual Machines:	1

Capacity and Usage

Last updated at 9:57 PM

CPU
141 MHz used — 44.688 GHz allocated

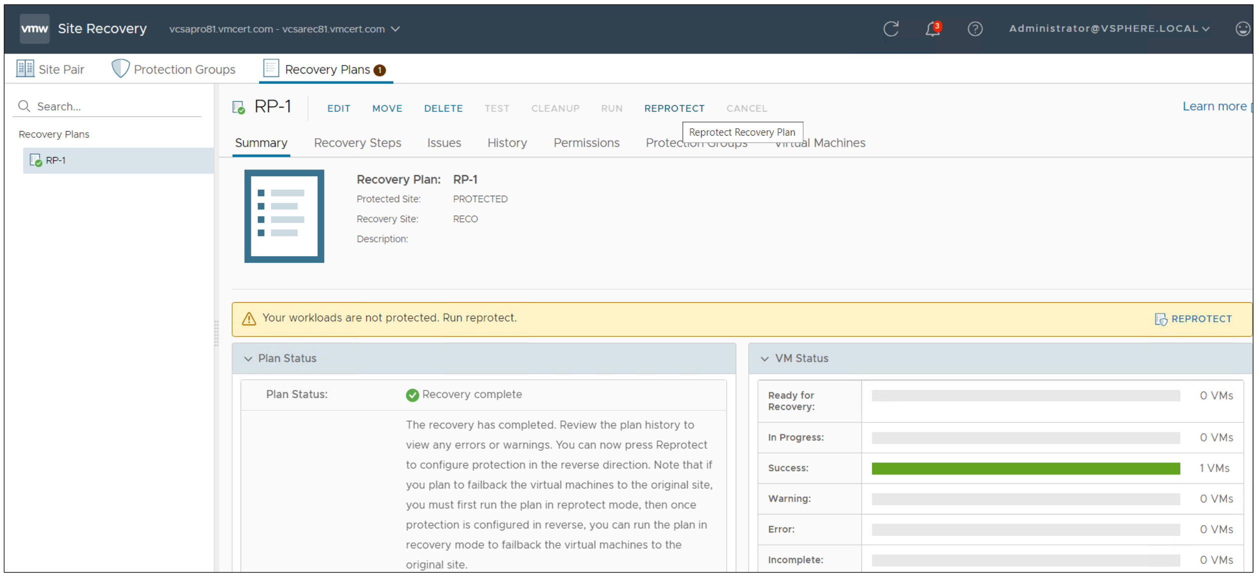
Memory
3.76 GB used — 63.57 GB allocated

Storage
20.24 GB used — 825.5 GB allocated

Tags

No tags assigned

8. After a failover test in VMware SRM, reprotection is required to reverse the replication direction from the recovery site back to the original site. This ensures that the original site is ready to act as the recovery site in case of future failovers. Click **REPROTECT**.



RP-1

Recovery Plan:	RP-1
Protected Site:	PROTECTED
Recovery Site:	RECO
Description:	

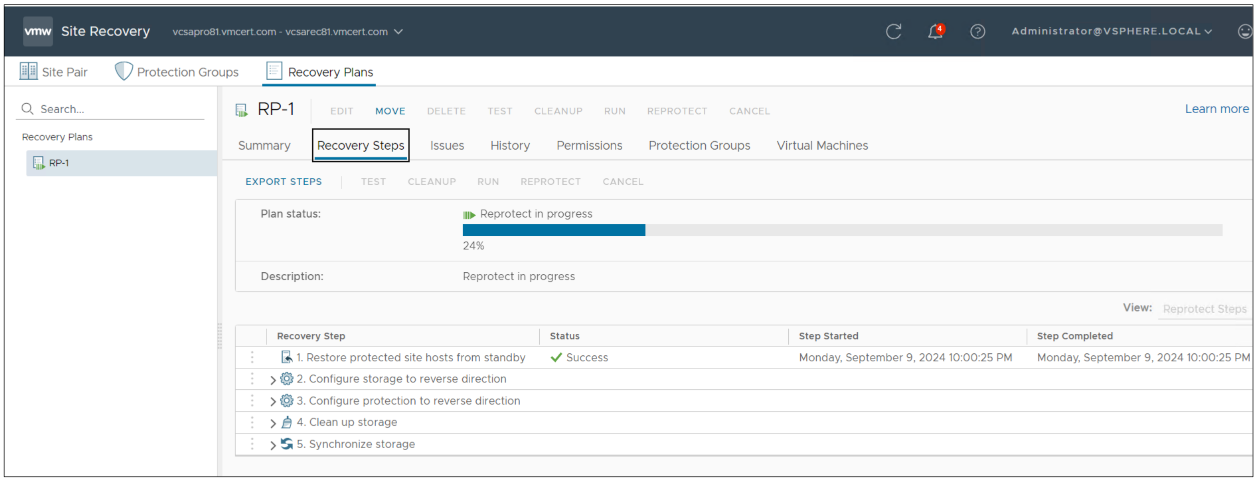
Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	1 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs

9. Verify the Reprotection progress from the Recovery Steps tab.

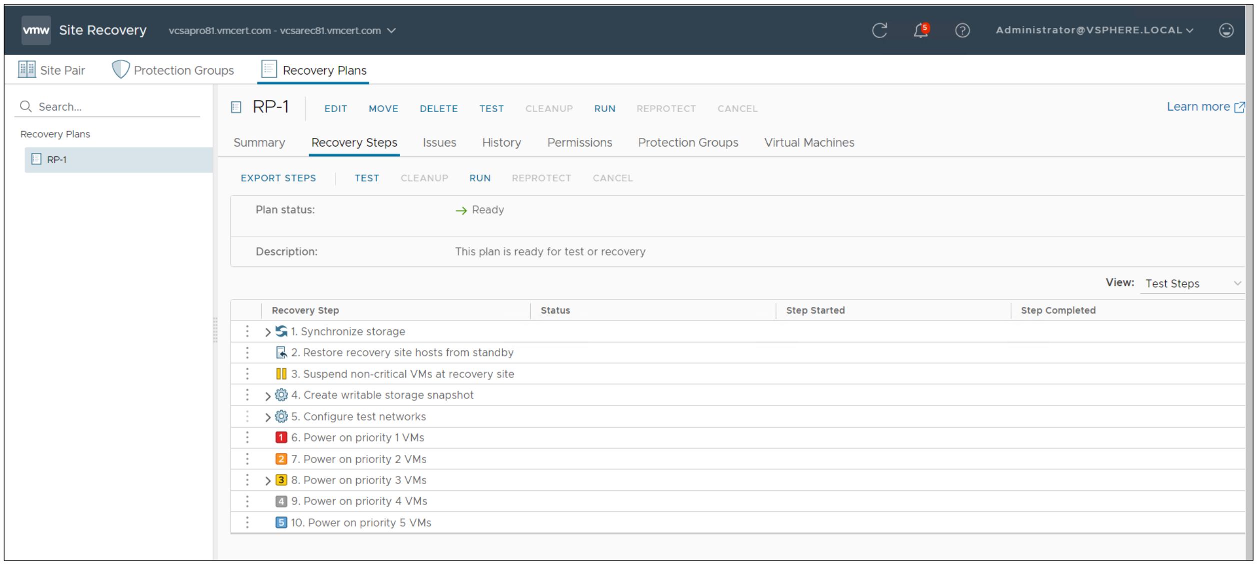


Plan status: Reprotect in progress 24%

Description: Reprotect in progress

Recovery Step	Status	Step Started	Step Completed
1. Restore protected site hosts from standby	✓ Success	Monday, September 9, 2024 10:00:25 PM	Monday, September 9, 2024 10:00:25 PM
2. Configure storage to reverse direction			
3. Configure protection to reverse direction			
4. Clean up storage			
5. Synchronize storage			

10. Verify whether the plan status shows Ready.

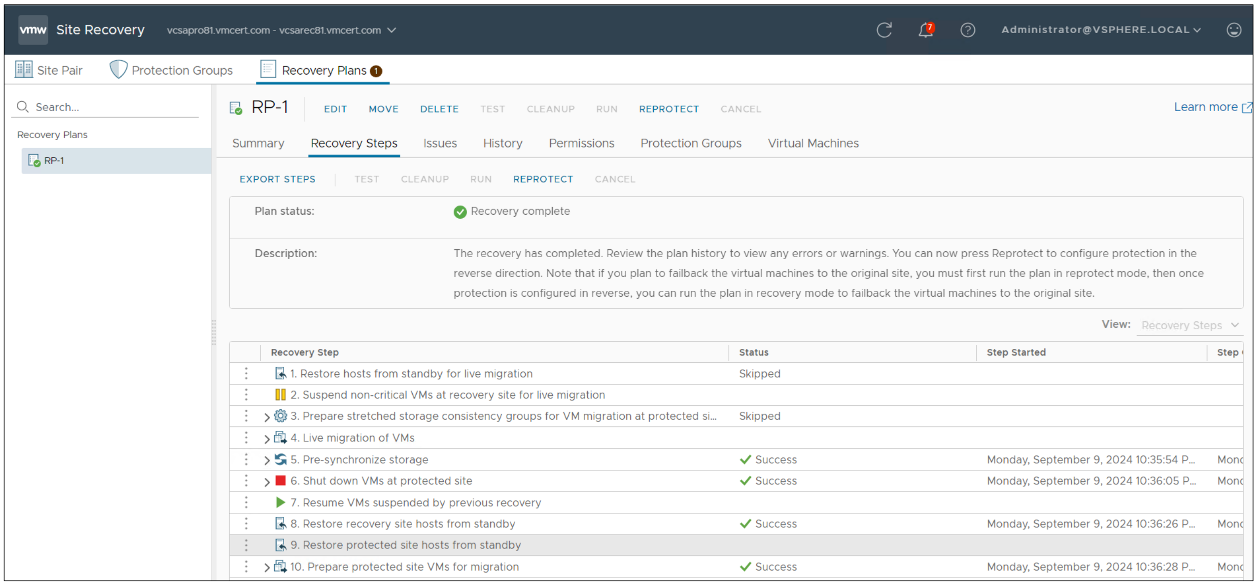


Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage			
2. Restore recovery site hosts from standby			
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot			
5. Configure test networks			
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs			
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

11. Repeat the procedure and click **RUN**.

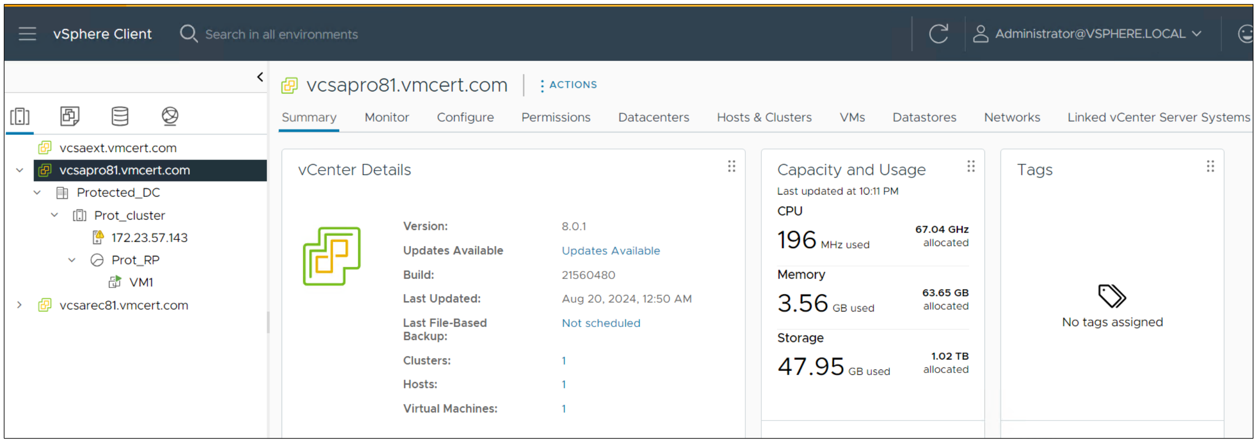


Plan status: Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Recovery Step	Status	Step Started	Step
1. Restore hosts from standby for live migration	Skipped		
2. Suspend non-critical VMs at recovery site for live migration			
3. Prepare stretched storage consistency groups for VM migration at protected si...	Skipped		
4. Live migration of VMs			
5. Pre-synchronize storage	✓ Success	Monday, September 9, 2024 10:35:54 P...	Monc
6. Shut down VMs at protected site	✓ Success	Monday, September 9, 2024 10:36:05 P...	Monc
7. Resume VMs suspended by previous recovery			
8. Restore recovery site hosts from standby	✓ Success	Monday, September 9, 2024 10:36:26 P...	Monc
9. Restore protected site hosts from standby			
10. Prepare protected site VMs for migration	✓ Success	Monday, September 9, 2024 10:36:28 P...	Monc

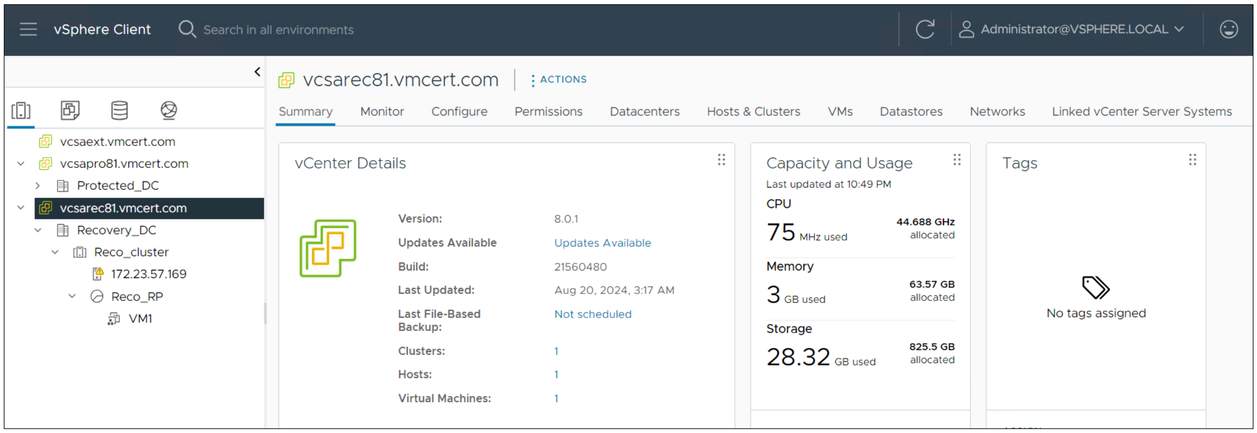
Status of the primary host after reversed planned migration:



Version: 8.0.1
Updates Available: Updates Available
Build: 21560480
Last Updated: Aug 20, 2024, 12:50 AM
Last File-Based Backup: Not scheduled
Clusters: 1
Hosts: 1
Virtual Machines: 1

Last updated at 10:11 PM
CPU
196 MHz used — 67.04 GHz allocated
Memory
3.56 GB used — 63.65 GB allocated
Storage
47.95 GB used — 1.02 TB allocated

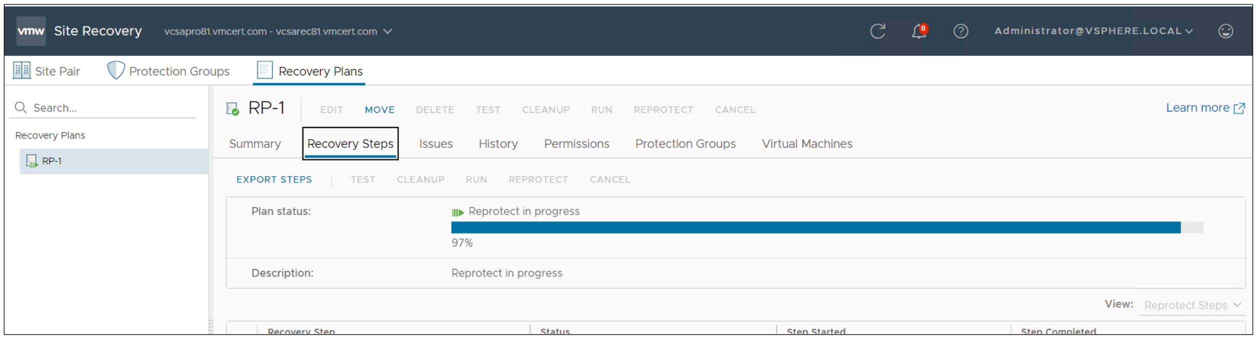
Status of the secondary host after the planned migration:



Version: 8.0.1
Updates Available: Updates Available
Build: 21560480
Last Updated: Aug 20, 2024, 3:17 AM
Last File-Based Backup: Not scheduled
Clusters: 1
Hosts: 1
Virtual Machines: 1

Last updated at 10:49 PM
CPU
75 MHz used — 44.688 GHz allocated
Memory
3 GB used — 63.57 GB allocated
Storage
28.32 GB used — 825.5 GB allocated

12. Reprotect the Recovery Plan after the test.



Plan status: Reprotect in progress

97%

Description: Reprotect in progress

Conclusion

Configuring SRM 8.7 with stretched storage certification using SRA 5.0.1 and GAD provides a powerful disaster recovery solution that leverages high-availability storage and automated failover capabilities. With seamless integration between VMware SRM, GAD, and Ops Center Protector, this solution delivers robust, reliable, and scalable disaster recovery, ensuring business continuity across sites.

References

- Adding the external storage system for the quorum disk
- Configuring a quorum disk
- Creating a datastore
- Deploying and configuring VCSA
- Download VCSA
- Download VCSA ISO and obtain the ISO image of VCSA from the VMware Customer Connect portal
- Hitachi Ops Center Protector
- Hitachi Vantara Support
- Mapping resources, creating TAG, and creating storage policies
- SRM installation guide

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com