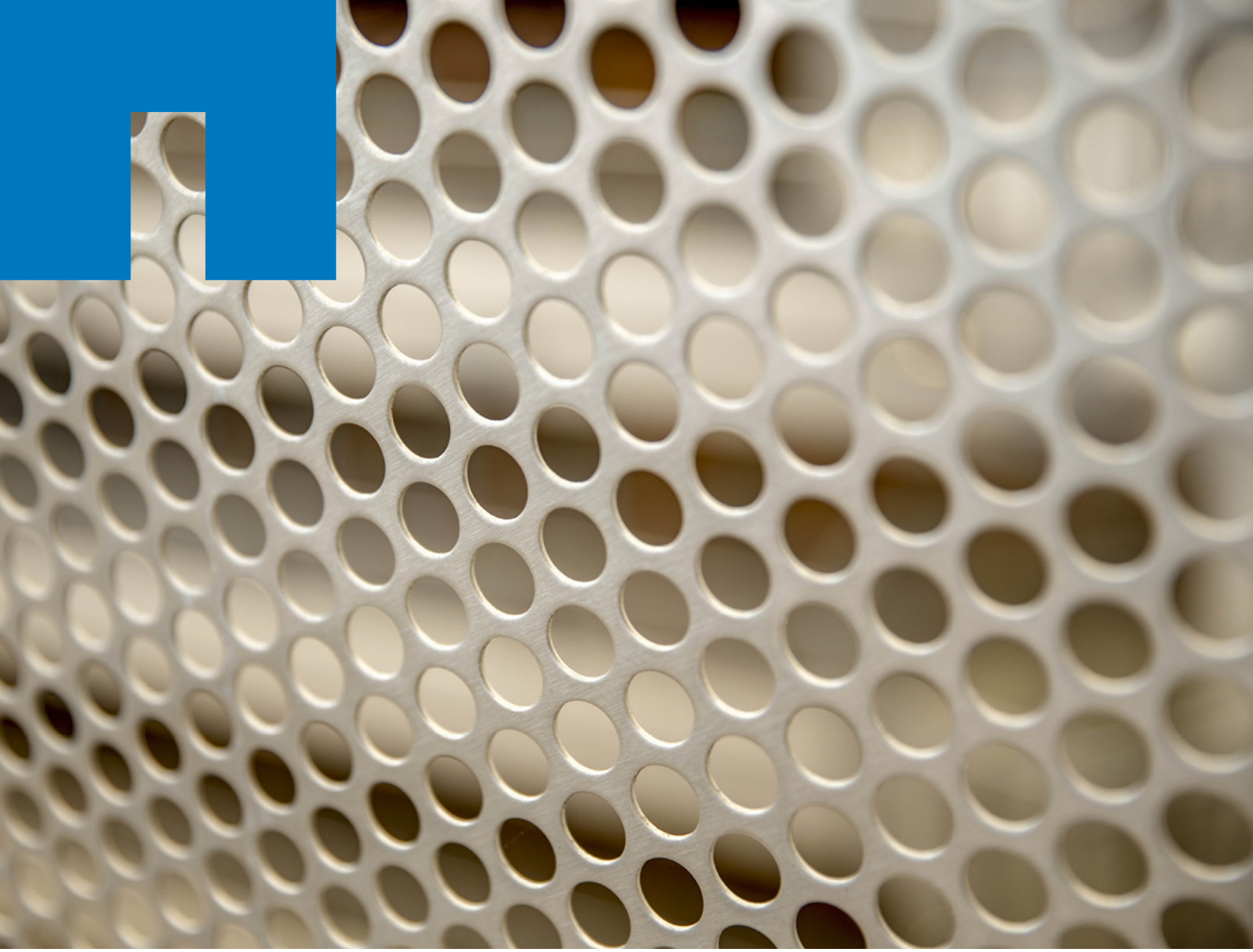


NetApp Learning Services

ONTAP Data Protection Administration

Exercise Guide
Content Version 7

NetApp®

NetApp Learning Services

ONTAP Data Protection Administration Exercise Guide

Course ID: STRSW-ILT-DATAPROT-REV07
Catalog Number: STRSW-ILT-DATAPROT-REV07-EG

ATTENTION

The information contained in this course is intended only for training. This course contains information and activities that, while beneficial for the purposes of training in a closed, non-production environment, can result in downtime or other severe consequences in a production environment. This course material is not a technical reference and should not, under any circumstances, be used in production environments. To obtain reference materials, refer to the NetApp product documentation that is located at http://mysupport.netapp.com/.

Table of Contents

Welcome **EG1**
Module 0: Getting Started **M0**
Module 1: ONTAP Integrated Data Protection **M1**
Module 2: SnapMirror Fundamentals **M2**
Module 3: SnapMirror Operation **M3**
Module 4: SVM DR **M4**
Module 5: MetroCluster Software **M5**
Module 6: SnapMirror Business Continuity **M6**
Module 7: NDMP and Tape Backup **M7**
Module 8: Cloud-Based Data Protection **M8**
Module 9: Course Review **M9**

Getting Started

Study-Aid Icons

In your exercises, you might see one or more of the following icons.

Warning
If you misconfigure a step marked with this icon, later steps might not work properly. Check the step carefully before you move forward.

Attention
Review this step or comment carefully to save time and avoid errors.

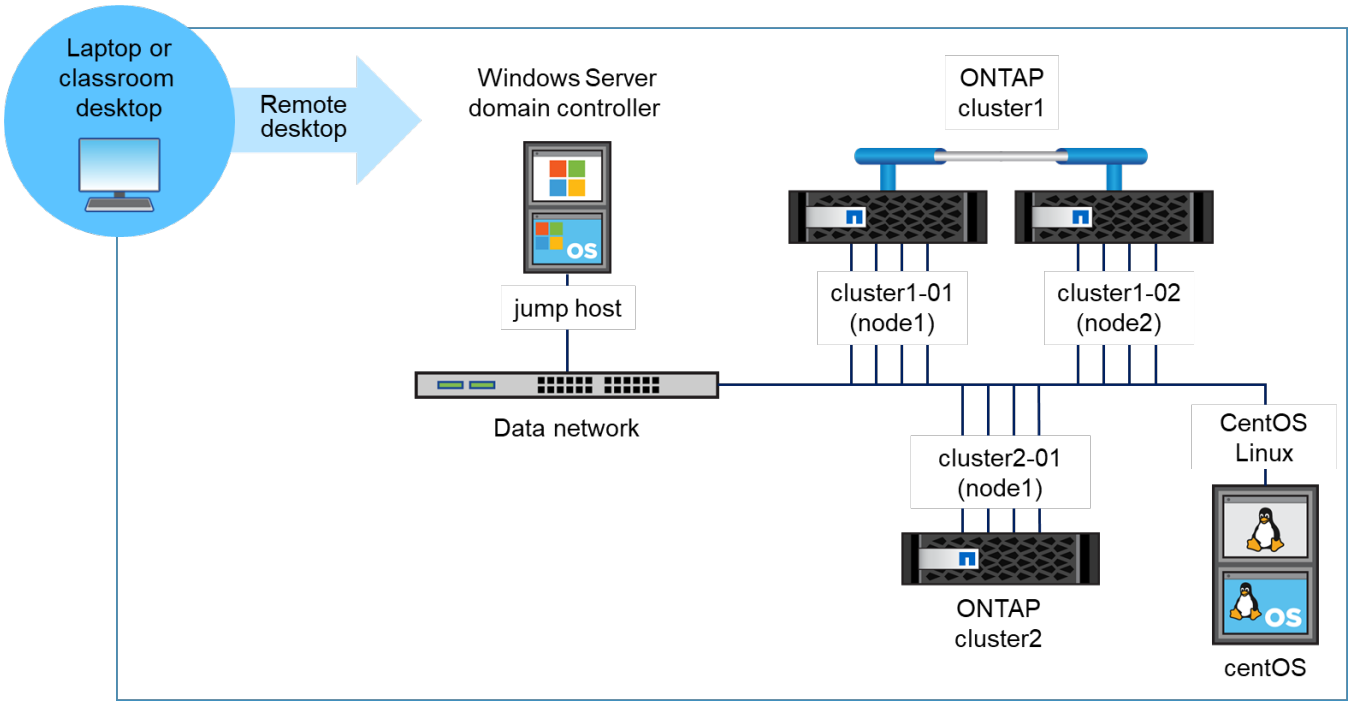
Information
Review information about the topic or procedure.

Exercise Equipment Diagram

Your exercise environment contains one of each of the following virtual machines:

- Windows Server 2012 R2 system with domain controller and DNS Server Manager
- NetApp ONTAP 2-node cluster (cluster1)
- ONTAP single-node cluster (cluster2)
- CentOS Linux 6.5 server system

Use the connection information that your instructor provides. When you sign in to the portal through your web browser, you are connected to a Windows Server jump host through a web-based Remote Desktop Protocol (RDP) connection. From this jump host, you connect to all other servers in your exercise environment.



System	Host Name	IP Addresses	User Name	Password
Windows Server 2012 R2	JUMPHOST	192.168.0.5	demo\Administrator	Netapp1!
ONTAP cluster-management LIF	cluster1	192.168.0.101	admin (case-sensitive)	Netapp1!
node 1	cluster1-01	192.168.0.111	admin (case-sensitive)	Netapp1!
node 2	cluster1-02	192.168.0.112	admin (case-sensitive)	Netapp1!
ONTAP cluster-management LIF	cluster2	192.168.0 102	admin (case-sensitive)	Netapp1!
node 1	cluster-01	192.168.0 113	admin (case-sensitive)	Netapp1!
Linux Server	centos65	192.168.0.21	root	Netapp1!

Exercise 0: Checking the Exercise Equipment

In this exercise, you familiarize yourself with your equipment, synchronize system time, assign a Network Time Protocol (NTP) time server, and ensure that licenses are installed.

Objectives

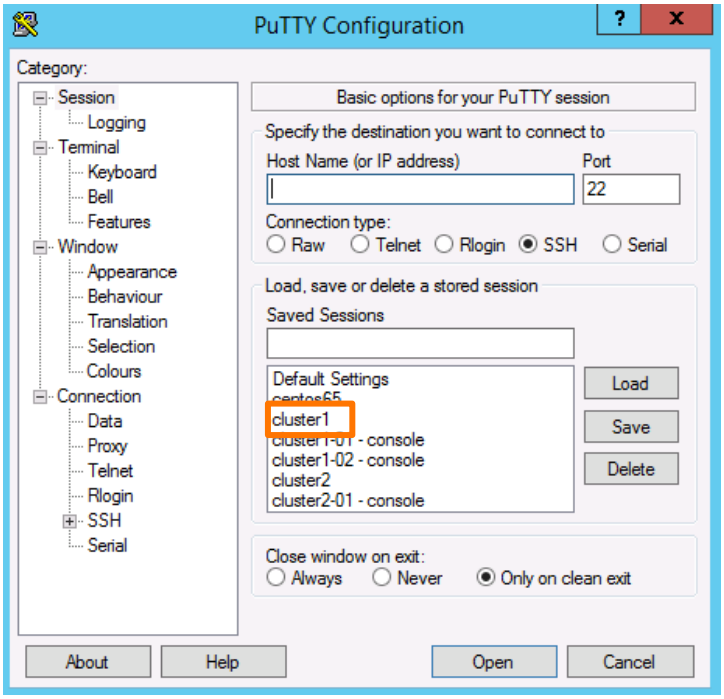
This exercise focuses on enabling you to do the following:

- Ensure connectivity to an ONTAP cluster
- Synchronize system time between the ONTAP clusters and the Windows domain controller
- Verify that required licenses are installed on the ONTAP clusters

Task 1: Ensure Connectivity to Your ONTAP Cluster

In this task, you familiarize yourself with the Windows Server 2012 desktop environment. You ensure connectivity to the ONTAP cluster and verify the health of the ONTAP cluster.

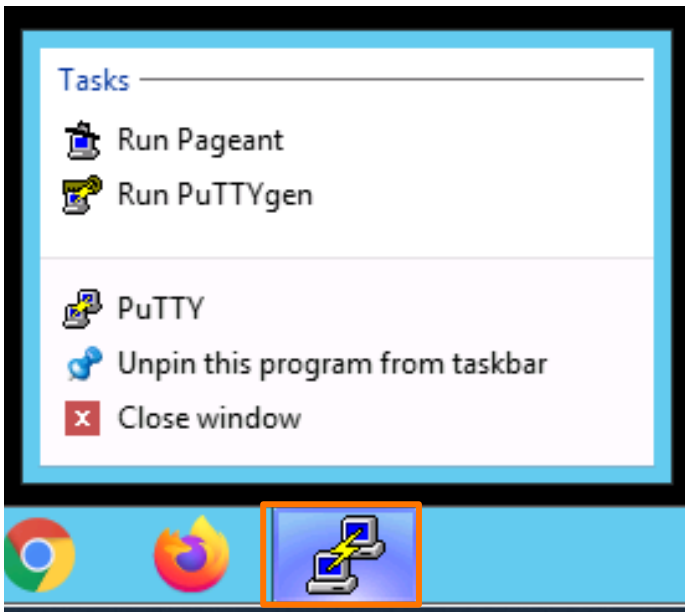
Step	Action
1-1	To connect to ONTAP System Manager, launch either a Chrome or Firefox browser. The UI for each cluster opens automatically in a separate browser tab. To connect to the CLI of the ONTAP cluster, use PuTTY. PuTTY is a UI for the Telnet and Secure Shell (SSH) protocols.
1-2	On the jump host desktop taskbar, locate and click the shortcut to the PuTTY program. 

Step	Action
1-3	In the PuTTY Configuration dialog box, verify that cluster1 is listed under Saved Sessions, and then double-click **cluster1**. 
1-4	At the ONTAP cluster login prompt, provide the cluster1 credentials: ▪ Login: **`admin`** ▪ Password: **`Netapp1!`** The ONTAP cluster CLI prompt and cursor appear.
1-5	If you have difficulty logging in to the ONTAP cluster CLI, see the table in the exercise equipment section, and verify that you are using the correct username and password for the cluster-management LIF on cluster1. Both the username and password are case-sensitive.

1-6	To verify that both nodes of the ONTAP cluster are healthy and eligible, run the **`cluster show`** command:
	`cluster show`
	Sample output:
	`cluster1::> cluster show`
	`Node Health Eligibility`
	`--- --- ---`
	`cluster1-01 true true`
	`cluster1-02 true true`
	`2 entries were displayed.`

Step	Action
1-7	If the health or eligibility of either node is listed as `false`, alert your instructor.

1-8	To view the ONTAP software version on the cluster, run the **`version`** command:
	`version`
	Sample output:
	`cluster1::> version`
	`NetApp Release 9.8P3: Sat Mar 27 08:43:48 UTC 2021`

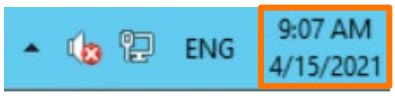
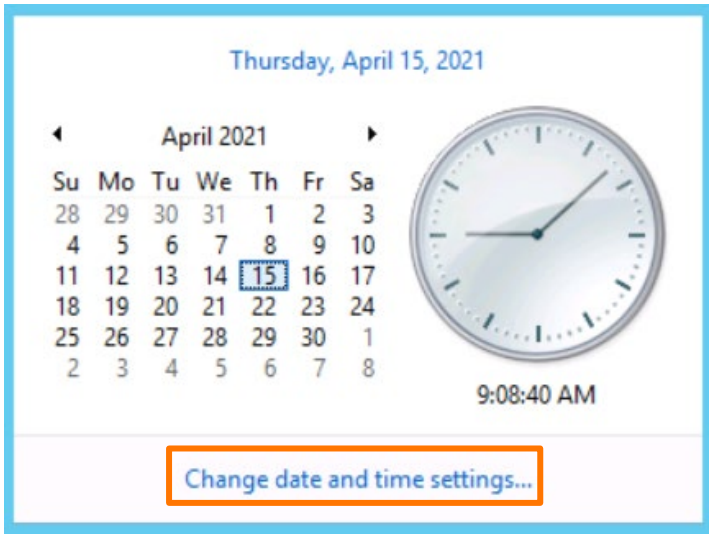
1-9	To open another PuTTY session, right-click the PuTTY icon in the taskbar, and then click **PuTTY**. 

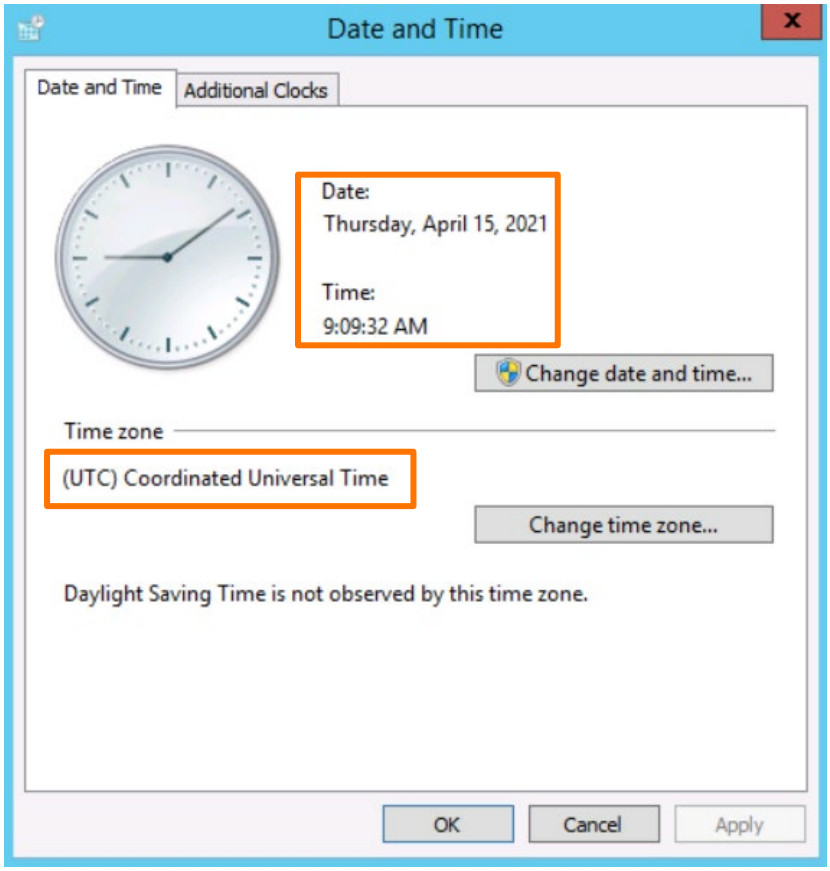
1-10	Log in to the session for **cluster2**. Run the **`cluster show`** command and verify the health of cluster2:
	`cluster show`
	Sample output:
	`cluster2::> cluster show`
	`Node Health Eligibility`
	`--- --- ---`
	`cluster2-01 true true`

1-11	If no CLI activity occurs for some time, the logged-in user is logged out. The default timeout value is 30 minutes.
1-12	To modify the timeout intervals for CLI sessions, run the **`system timeout modify`** command on each cluster to set the timeout value for CLI sessions to 0 (zero). **`system timeout modify -timeout 0`**

Task 2: Verify Time Synchronization Between the Jump Host and the ONTAP Clusters

In this task, you verify that the the time zone, system date, and time on the Windows Server 2012 system match those settings on the two ONTAP clusters. This task is optional. Perform the task if you need to synchronize the date and time between the ONTAP clusters and the Windows domain controller (IP address 192.168.0.253).

Step	Action
2-1	Windows domains must be synchronized to within 5 minutes of all member servers. If the time of the ONTAP cluster is not synchronized with a domain controller, the ONTAP cluster cannot join or remain joined to the Windows domain. Without synchronization, computers in the Windows domain cannot access resources in the ONTAP cluster, and resources in the cluster cannot access the Windows domain.
2-2	Click the time and date display in the lower-right corner of the desktop window to display the date and time on the Windows Server 2012 desktop. 
2-3	Click **Change date and time settings** to display the time zone, date, and time. 

Step	Action
2-4	Review the date, time, and time zone on the Windows Server 2012 system. 
2-5	**Etc/UTC Time Zone:** UTC is the primary time standard by which the world regulates clocks and time. UTC is one of several replacements for Greenwich Mean Time (GMT). The zone information database, which is a collaborative compilation of time zone information, has a special area called “Etc.” The Etc area is for administrative zones, particularly for “Etc/UTC,” which represents UTC.

2-6	To display the configured time zone on the ONTAP cluster, run the **`timezone`** command:
	`timezone`
	Sample output:
	`cluster1::> timezone`
	`    Timezone: Etc/UTC`

Step	Action

2-7	To display the date, time, and time zone in the ONTAP cluster, run the **date** command:
	date
	Sample output:
	`cluster1::> date`
	`Node Date Time zone`
	`--------- ------------------------ ------------------------`
	`cluster1-01`
	`Thu Apr 15 09:09:36 2021 Etc/UTC`
	`cluster1-02`
	`Thu Apr 15 09:09:36 2021 Etc/UTC`
	`2 entries were displayed.`

2-8	You can also run the `cluster date show` command to view the date and time information on a cluster. To change the time zone, you can run the `timezone -timezone` *timezone* command.
2-9	Compare the date and time in the ONTAP cluster to the date and time on the Windows Server 2012 system.
2-10	If the system date and time and the cluster date and time are not synchronized to within 5 minutes, you must correct the ONTAP cluster date and time.
2-11	Run the **date** command, using the accurate date and 24-hour time format with the specified syntax: **date <*YYYY*><*MM*><*DD*><*HH*><*MM*>** For example: **date 202104121015**
2-12	When you run the `date` command on any node in the ONTAP cluster, the command sets the date and time on all nodes in the cluster. The NTP service synchronizes the date and time for all nodes in the cluster. If an NTP time server is configured, all nodes in the cluster remain time-synchronized with the NTP time server.
2-13	Connect to cluster2, and then repeat the steps that you used to verify the time zone for cluster1.

Task 3: Verify That Required License Codes Are Installed

Many advanced features of ONTAP software require licenses to work. In later exercises, you use several licensed features of ONTAP software. In this task, you verify that the necessary licenses are installed.

You can check licenses in ONTAP System Manager or the ONTAP CLI. Your instructor provides you with license codes for any software that you need to install.

Step	Action
3-1	In the cluster1-mgmt CLI, run the **`license show`** command: **`license show`**
3-2	Verify that (at least) the following required license codes (that is, codes for the licenses that enable the features of the ONTAP software and that are required for later exercises) are installed: ▪ Cluster Base License ▪ NFS ▪ CIFS ▪ iSCSI ▪ SnapRestore ▪ SnapMirror ▪ SnapMirror Synchronous ▪ FlexClone ▪ SnapVault ▪ SnapManager
3-3	 If any license is not installed, contact NetApp Learning Services Support for assistance.

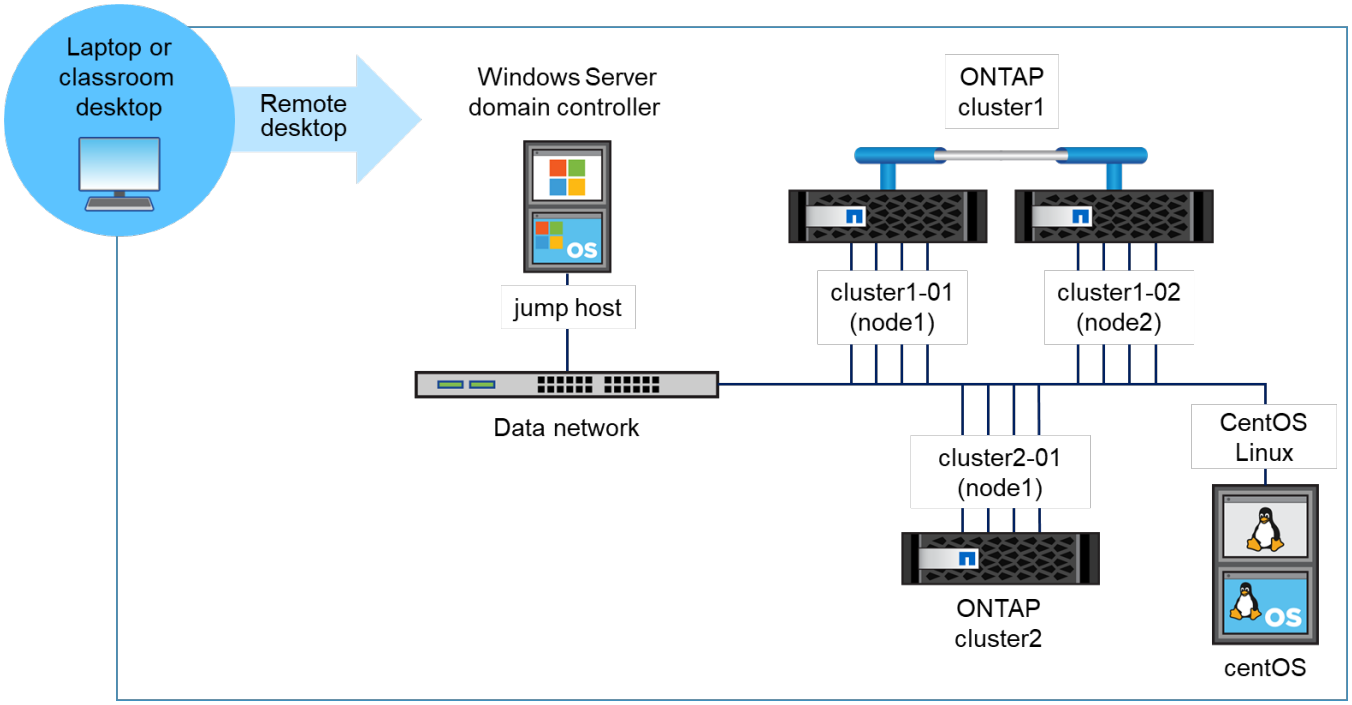
End of exercise

Module 1: ONTAP Integrated Data Protection

Module 1 contains no exercises.

Module 2: SnapMirror Fundamentals

Exercise Equipment Diagram



System	Host Name	IP Addresses	User Name	Password
Windows Server 2012 R2	JUMPHOST	192.168.0.5	demo\Administrator	Netapp1!
ONTAP cluster-management LIF	cluster1	192.168.0.101	admin (case-sensitive)	Netapp1!
node 1	cluster1-01	192.168.0.111	admin (case-sensitive)	Netapp1!
node 2	cluster1-02	192.168.0.112	admin (case-sensitive)	Netapp1!
ONTAP cluster-management LIF	cluster2	192.168.0 102	admin (case-sensitive)	Netapp1!
node 1	cluster-01	192.168.0 113	admin (case-sensitive)	Netapp1!
Linux Server	centos65	192.168.0.21	root	Netapp1!

Exercise 1: Configuring a Load-Sharing Mirror Relationship

In this exercise, you create and initialize a load-sharing mirror relationship for a root volume in a NetApp ONTAP cluster.

Objectives

This exercise focuses on enabling you to do the following:

- Create a load-sharing mirror relationship between a storage VM (storage virtual machine, also known as SVM) root volume and destination volumes
- Initialize and update a load-sharing mirror relationship

Task 1: Create and Initialize a Load-Sharing Mirror Relationship

In this task, you use the ONTAP CLI to create a load-sharing mirror volume on node 2 of cluster1. The volume protects the root volume of the SVM svm1 on cluster1. You then use the ONTAP CLI to initialize the load-sharing mirror relationship and view its status.

Step	Action
1-1	 When you perform the exercises in this course, you often switch between System Manager tabs for cluster1 and cluster2. To help you avoid mistakes, exercise steps that require you to switch between clusters include the corresponding cluster label. Steps that occur on cluster1 begin with a **Cluster1** label. Steps that occur on cluster2 begin with a **Cluster2** label.
1-2	**Cluster 1** Log in to the PuTTY session for cluster1.

1-3	On cluster1, run the **`volume create`** command to create a destination volume for the load-sharing mirror relationship:
	`volume create -vserver svm1 -volume svm1_root_LS -aggregate n2_data_001 -size 1gb -state online -type DP`
	Sample output:
	`cluster1::> volume create -vserver svm1 -volume svm1_root_LS -aggregate n2_data_001 -size 1gb -state online -type DP`
	`[Job 1163] Job succeeded: Successful`

Step	Action

1-4	To view the created volume, run the **volume show** command:
	volume show -vserver svm1
	Sample output:
	`cluster1::> volume show -vserver svm1`
	`Vserver Volume Aggregate State Type Size Available Used%`
	`svm1 smb1_share_CIFS_volume n2_data_001 online RW 1GB 971.4MB 0%`
	`svm1 svm1_root n1_data_001 online RW 20MB 17.65MB 7%`
	`svm1 svm1_root_LS n2_data_001 online DP 1GB 1023MB 0%`
	`3 entries were displayed.`

1-5	Note that the volume svm1_root_LS is of type DP.

1-6	On cluster1, run the **snapmirror create** command to create a load-sharing mirror relationship between the SVM root volume and the destination volume:
	snapmirror create -source-path svm1:svm1_root -destination-path svm1:svm1_root_LS -type LS -schedule hourly
	Sample output:
	`cluster1::> snapmirror create -source-path svm1:svm1_root -destination-path svm1:svm1_root_LS -type LS -schedule hourly`
	`[Job 1164] Job is queued: snapmirror create for the relationship with destination`
	`[Job 1164] Job succeeded: SnapMirror: done`

1-7	After the job is complete, run the **snapmirror initialize** command to initialize the load-sharing mirror relationship:
	snapmirror initialize-ls-set -source-path svm1:svm1_root
	Sample output:
	`cluster1::> snapmirror initialize-ls-set -source-path svm1:svm1_root`
	`[Job 1166] Job is queued: snapmirror initialize-ls-set for source "cluster1://svm1/svm1_root".`

Step	Action

1-8	Run the **`snapmirror show`** command to view the status of the load-sharing mirror relationship:
	`snapmirror show`
	Sample output:
	`cluster1::> snapmirror show`
	
	`Source Destination Mirror Relationship Total Progress`
	`Path Type Path State Status Progress Healthy Last Updated`
	`----------- ---- ------------ ------- -------------- --------- ------- --------`
	`cluster1://svm1/svm1_root`
	`LS cluster1://svm1/svm1_root_LS`
	`Snapmirrored`
	`Idle - true -`

1-9	The type attribute of the load-sharing mirror volume changes from DP to LS. You can also create a custom schedule for a load-sharing mirror relationship.
1-10	You can manually update a load-sharing mirror set to make changes on the root volume visible before the next scheduled update. For example, when a new volume is mounted on the root volume of the SVM, you should update the set of load-sharing mirror volumes.

1-11	Run the **`snapmirror update-ls-set`** command to manually update the load-sharing mirror set for the root volume of svm1:
	`snapmirror update-ls-set -source-path svm1:svm1_root`
	Sample output:
	`cluster1::> snapmirror update-ls-set -source-path svm1:svm1_root`
	`[Job 1167] Job is queued: snapmirror update-ls-set for source "cluster1://svm1/svm1_root".`

End of exercise

Exercise 2: Configuring Cluster Peering and SVM Peering

In this exercise, you use NetApp ONTAP System Manager to set up the prerequisite configurations for data protection between primary and secondary ONTAP clusters.

Objectives

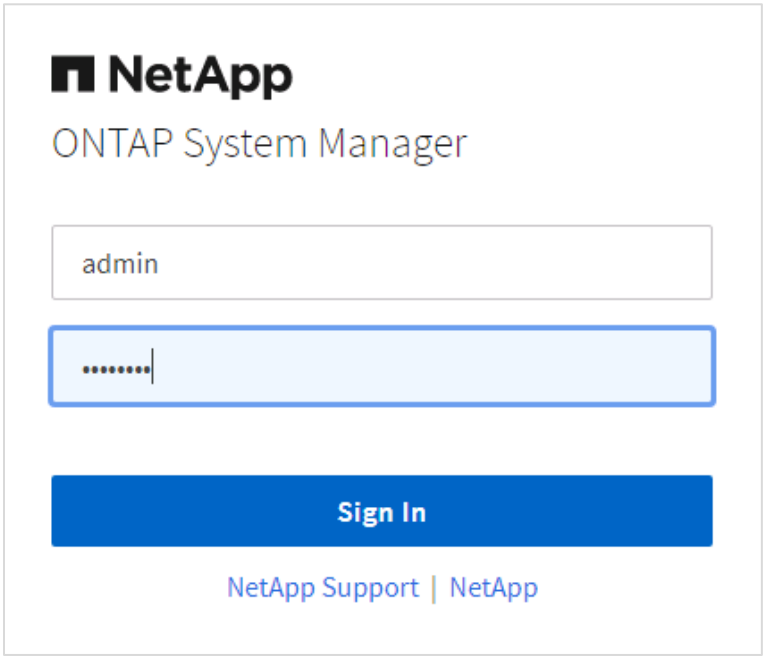
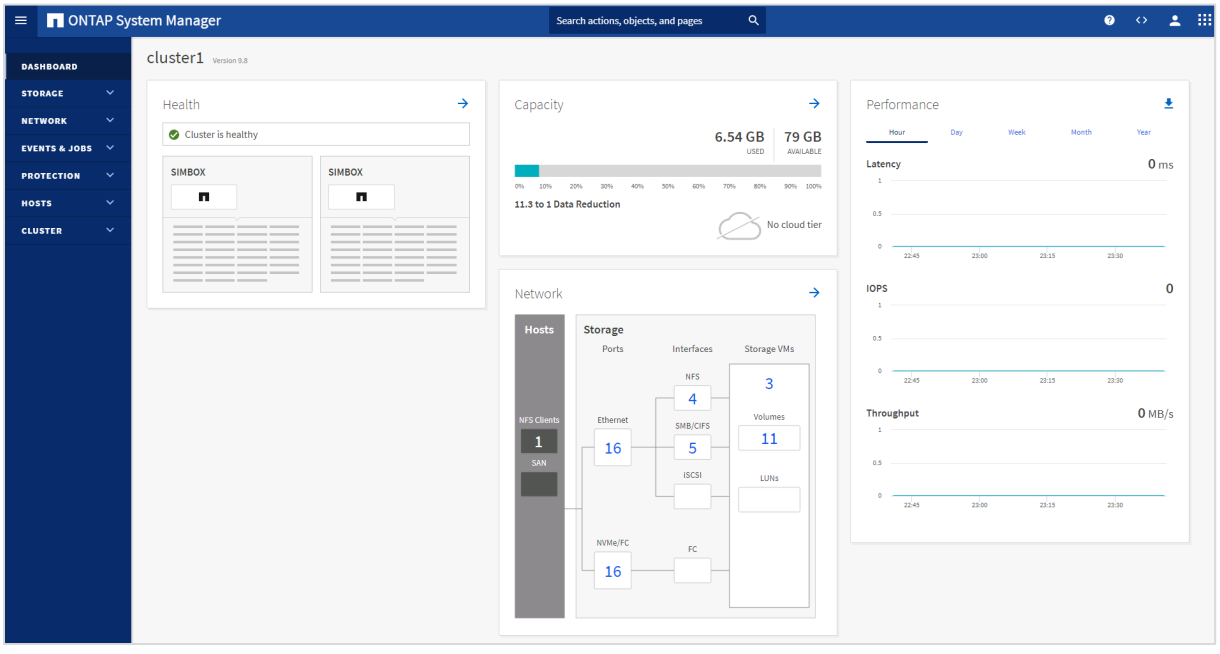
This exercise focuses on enabling you to do the following:

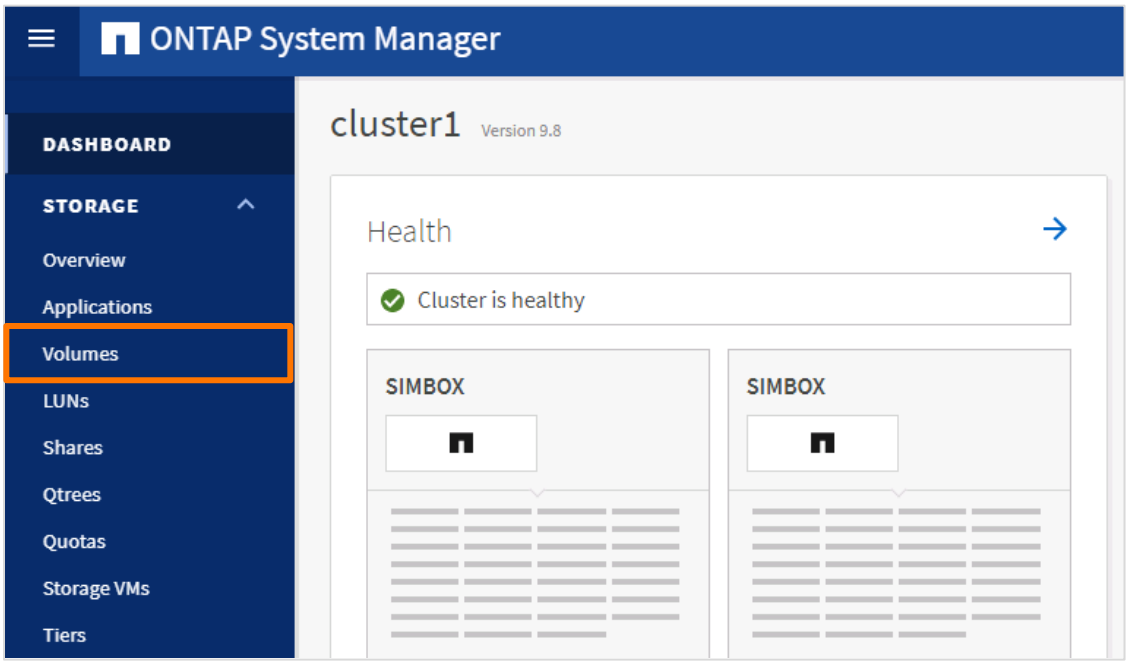
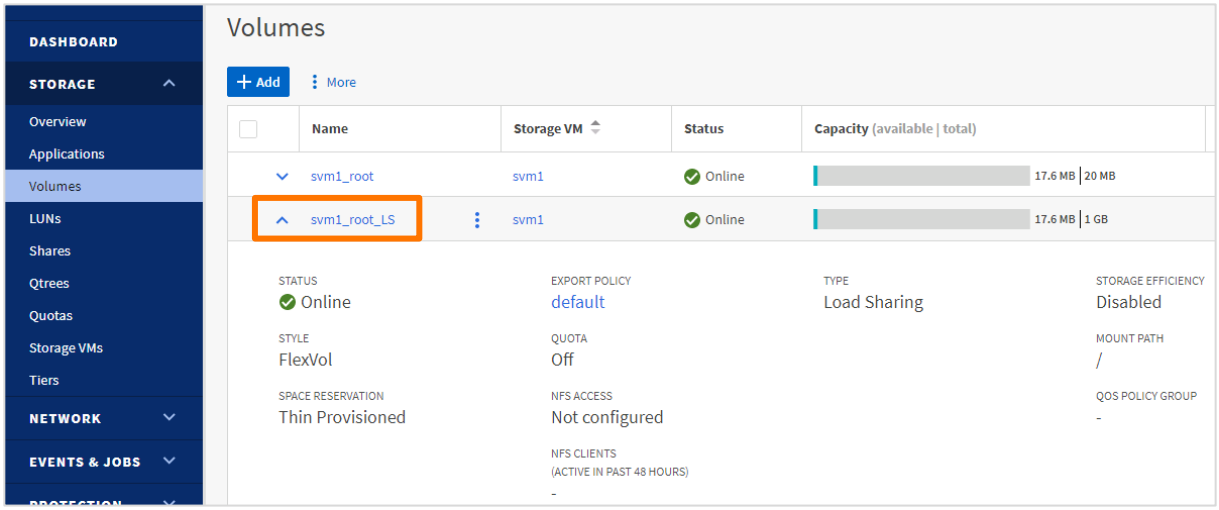
- Create intercluster LIFs for both clusters
- Prepare the storage environment on cluster2 as the secondary target
- Configure cluster peering
- Configure SVM peering
- Review the exercise environment

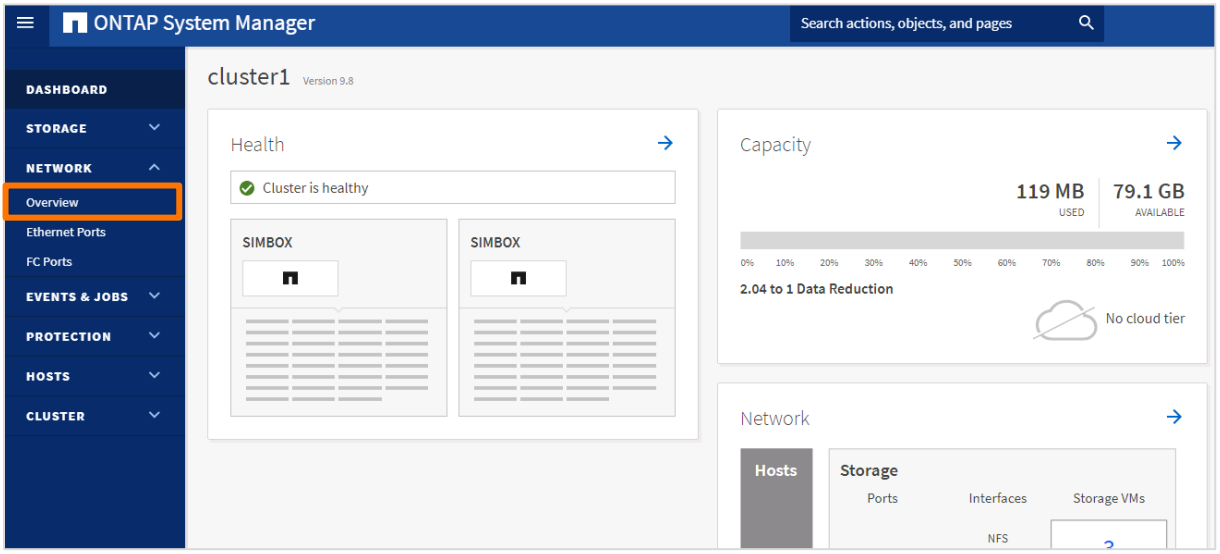
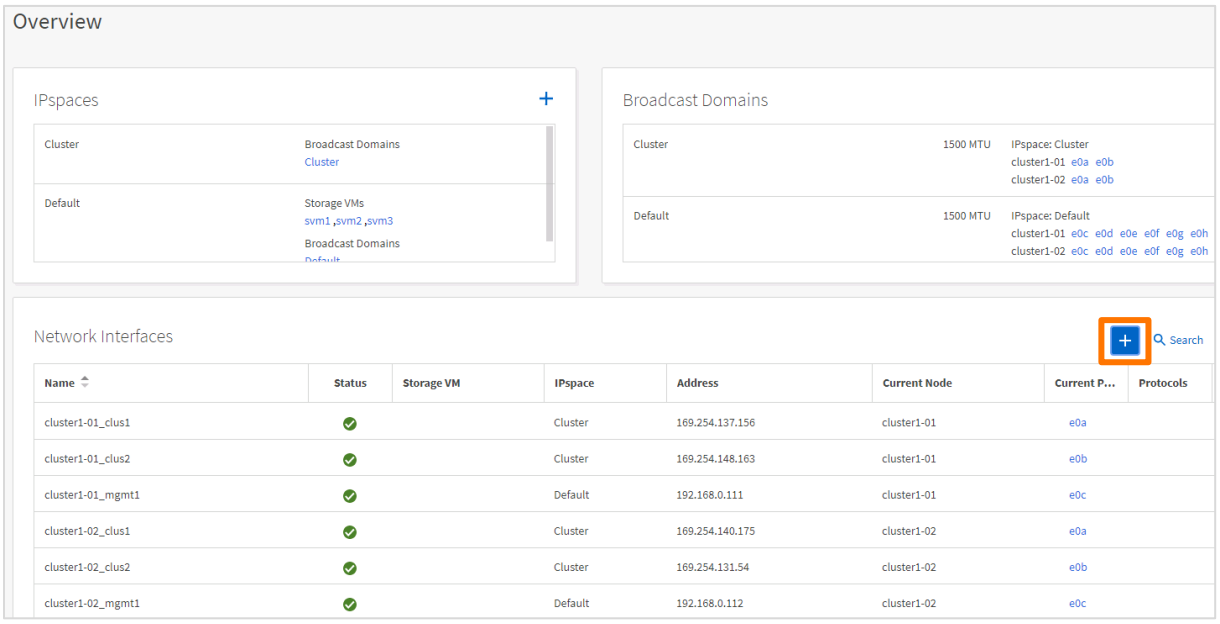
Task 1: Create Intercluster LIFs

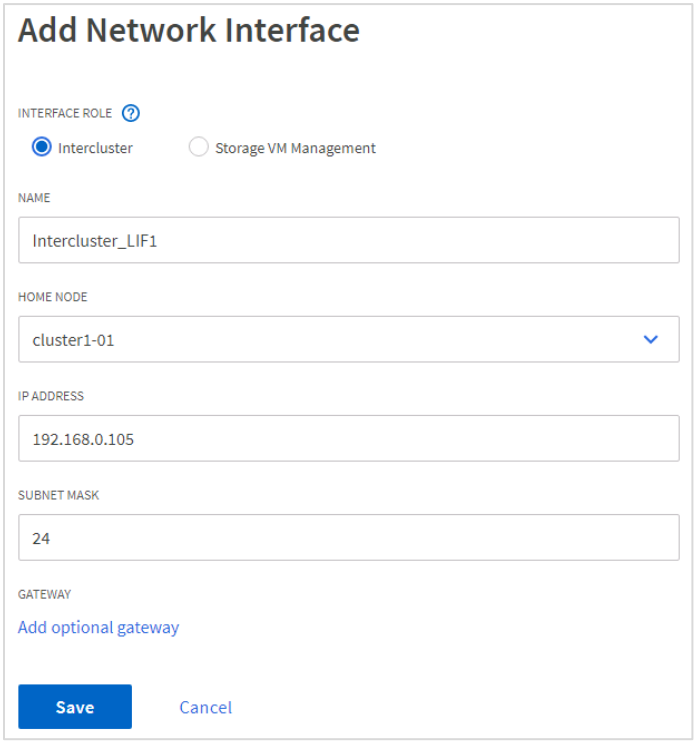
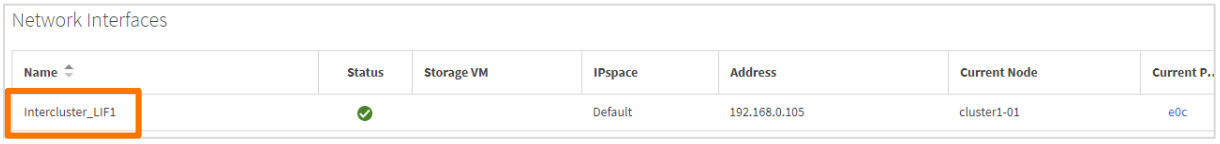
In this task, you add redundant intercluster LIFs to cluster1.

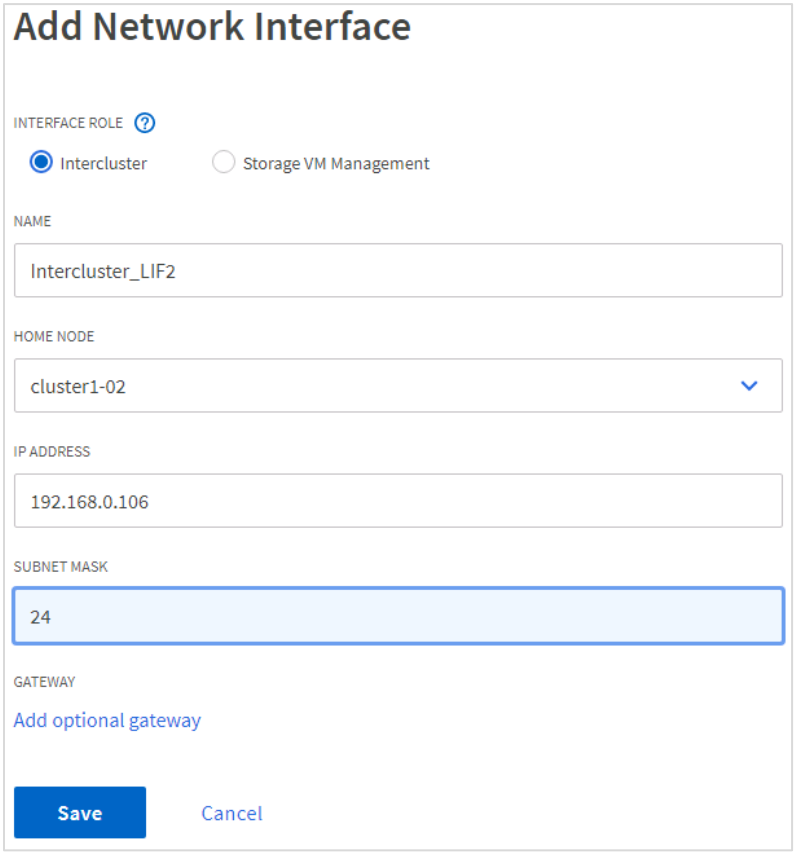
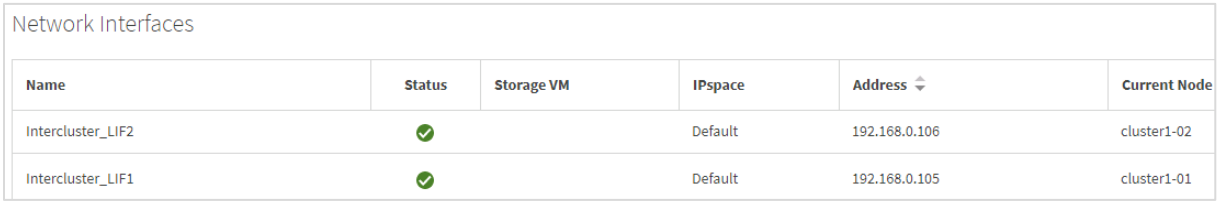
Step	Action
1-1	On the jump host desktop taskbar, click either the Chrome or Firefox icon to open a browser. 
1-2	When you launch a browser, a System Manager tab for each cluster opens. System Manager URL for cluster1: **https://cluster1.demo.netapp.com/sysmgr/v4** System Manager URL for cluster2: **https://cluster2.demo.netapp.com/sysmgr/v4**
1-3	When you perform the exercises in this course, you often switch between System Manager tabs for cluster1 and cluster2. To help you avoid mistakes, exercise steps that require you to switch between clusters include the corresponding cluster label. Steps that occur on cluster1 begin with a **Cluster1** label. Steps that occur on cluster2 begin with a **Cluster2** label.
1-4	**Cluster1** Ignore any security warning that might appear and proceed to the login screen.

Step	Action
1-5	Log in to System Manager for cluster1 by using the following credentials: ▪ Username: **admin** ▪ Password: **Netapp1!** 
1-6	On the System Manager dashboard, review information about cluster health, capacity, performance, and network configuration. 

Step	Action
1-7	In the System Manager navigation pane, select **Storage** > **Volumes**. 
1-8	Perform the following steps: a. Review the list of all the volumes in all the SVMs. b. Note that the load-sharing mirror volume **svm1_root_LS** for svm1 is also listed. c. Click the arrow in front of the volume name to view the details. 
1-9	You are implementing the network connectivity to enable peering relationships between clusters. In the following steps, you create intercluster LIFs for cluster1 and cluster2.

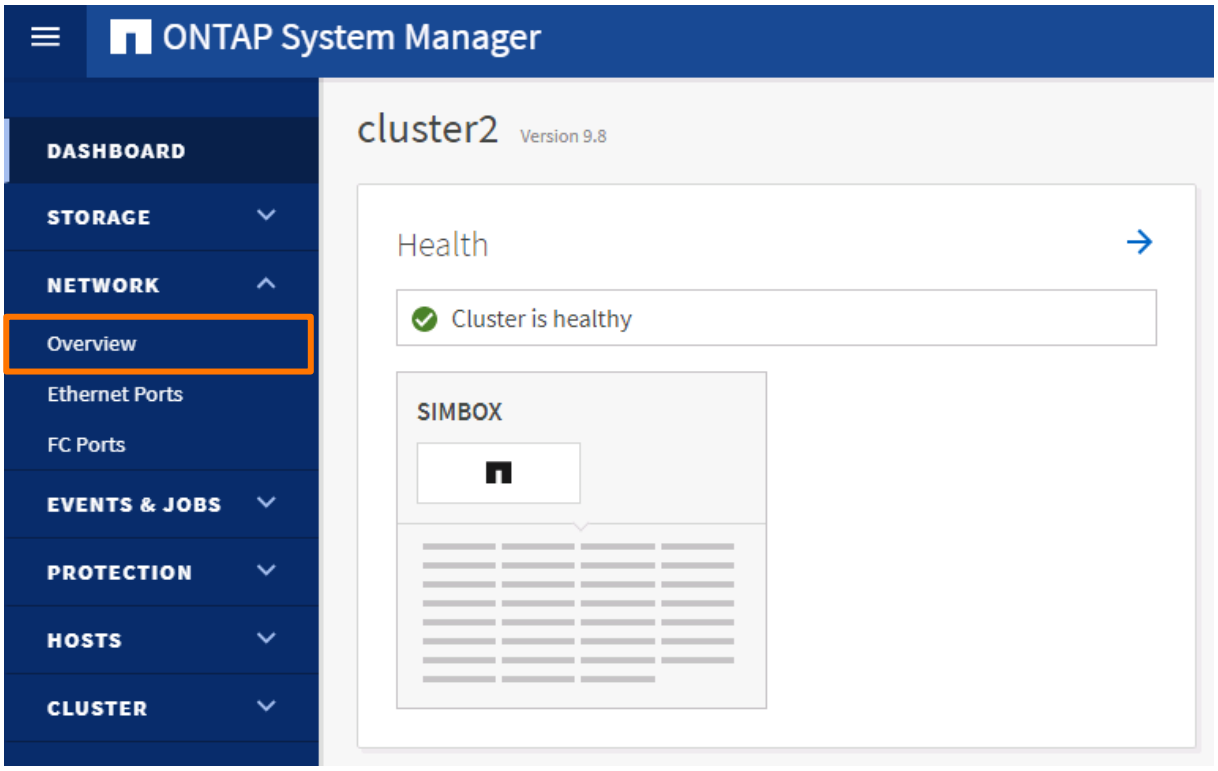
Step	Action
1-10	**Cluster1** In the System Manager navigation pane, select **Network** > **Overview**. 
1-11	In the Overview > Network Interfaces pane, click the **+** icon. 

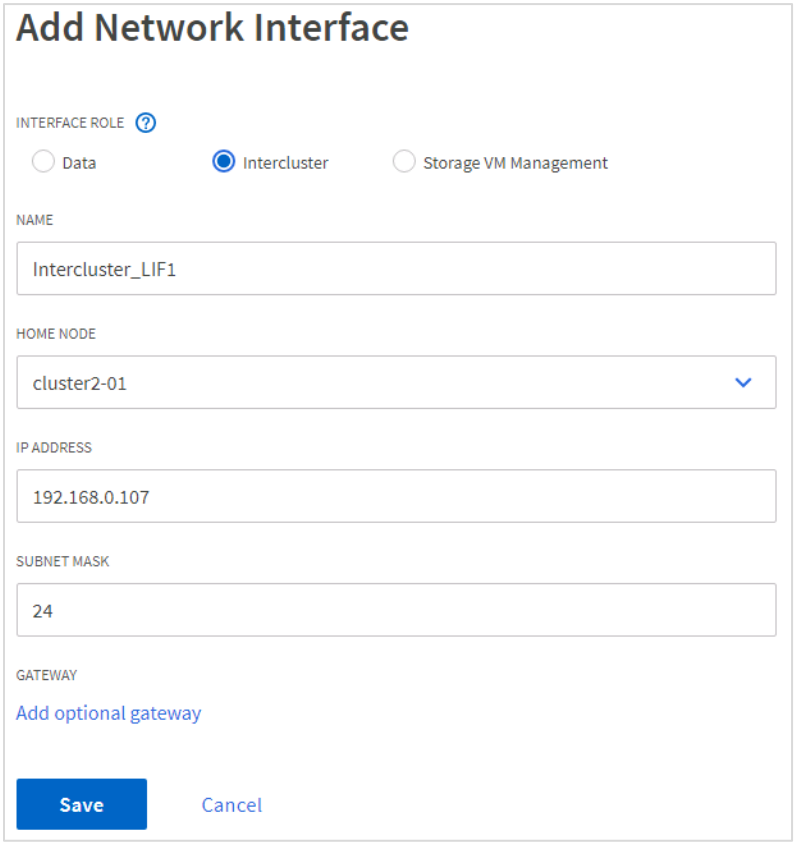
Step	Action
1-12	In the Add Network Interface dialog box, specify the following values: ▪ Interface Role: **Intercluster** ▪ Name: **`Intercluster_LIF1`** ▪ Home Node: **cluster1-01** ▪ IP Address: **`192.168.0.105`** ▪ Subnet Mask: **`24`** 
1-13	Click **Save**.
1-14	System Manager 9.8 does not expose subnet-based network interfaces. To manually configure these settings, use the ONTAP CLI. ONTAP 9.8 software can automatically select a port for new network interfaces. Therefore, the port selection option is not presented during provisioning in System Manager 9.8. To manually pick a port, use the ONTAP CLI. You can move or rehome a port through the UI after the original provisioning.
1-15	Verify that Intercluster_LIF1 appears in the Network Interfaces list. 
1-16	For fault tolerance, each node of the cluster must have an intercluster LIF. In the next step, you create an intercluster LIF named Intercluster_LIF2 on node 2.
1-17	In the Overview > Network Interfaces pane, click the **+** icon.

Step	Action
1-18	In the Add Network Interface dialog box, specify the following values: ▪ Interface Role: **Intercluster** ▪ Name: **`Intercluster_LIF2`** ▪ Home Node: **cluster1-02** ▪ IP Address: **`192.168.0.106`** ▪ Subnet Mask: **`24`** 
1-19	Click **Save**.
1-20	Verify that the two new intercluster LIFs (Intercluster_LIF1 and Intercluster_LIF2) are listed on cluster1. 

Task 2: Prepare the Storage Environment on Cluster2 as the Secondary Target

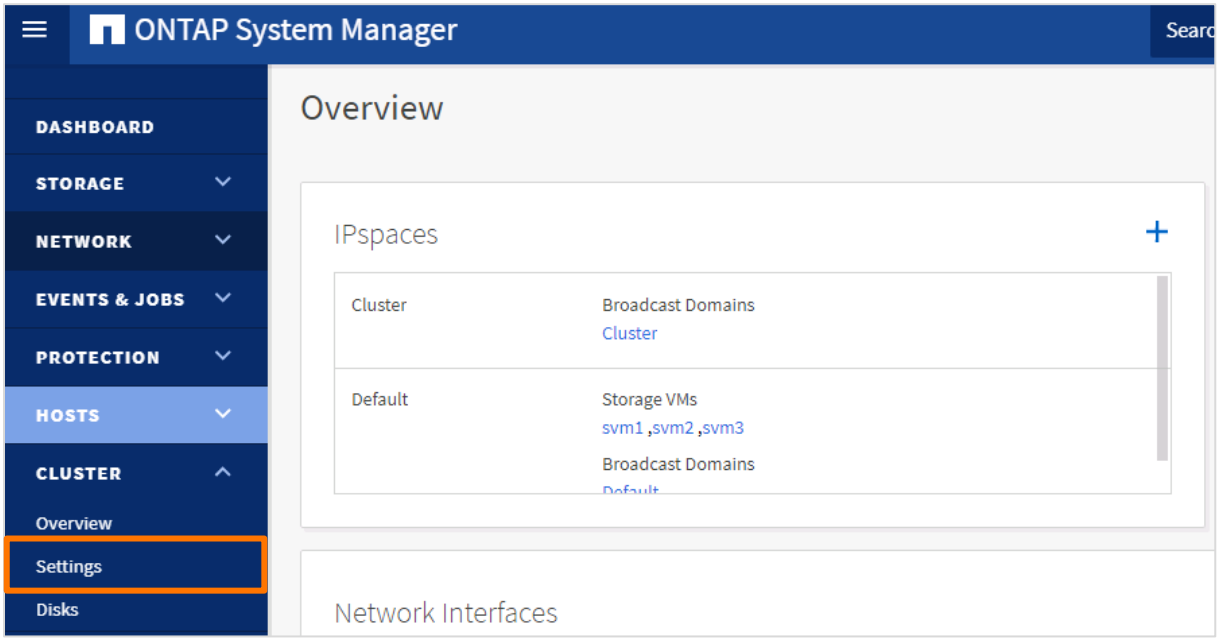
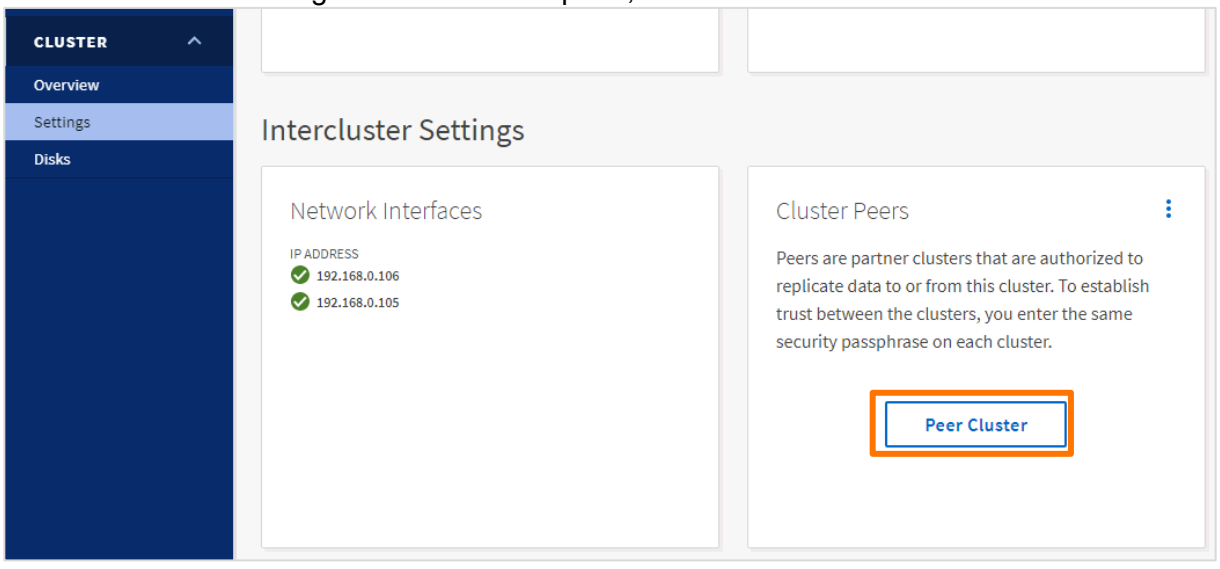
In this task, you repeat the steps that you used in Task 1 to create an intercluster LIF on the secondary cluster (cluster2).

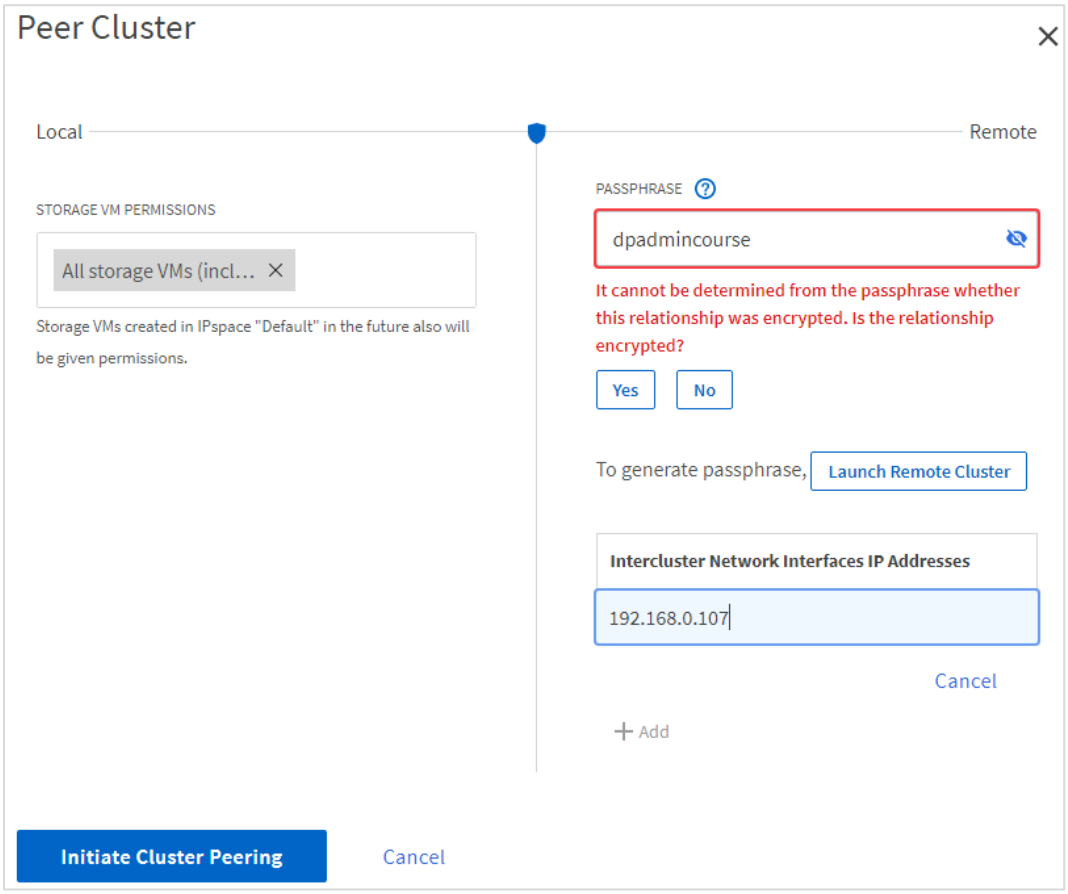
Step	Action
2-1	**Cluster2** In your browser, open the System Manager tab for cluster2. Ignore any security warning that might appear and proceed to the login.
2-2	Log in to System Manager for cluster2 by using the following credentials: ▪ User name: **`admin`** ▪ Password: **`Netapp1!`**
2-3	In the System Manager navigation pane, select **Network** > **Overview**. 
2-4	In the Overview > Network Interfaces pane, click the **+** icon.

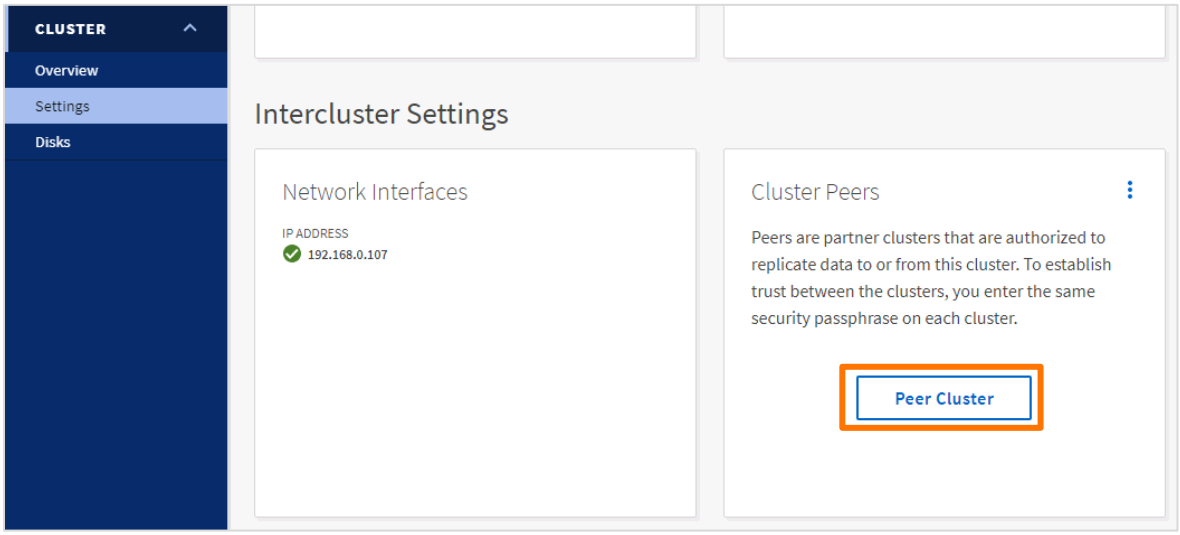
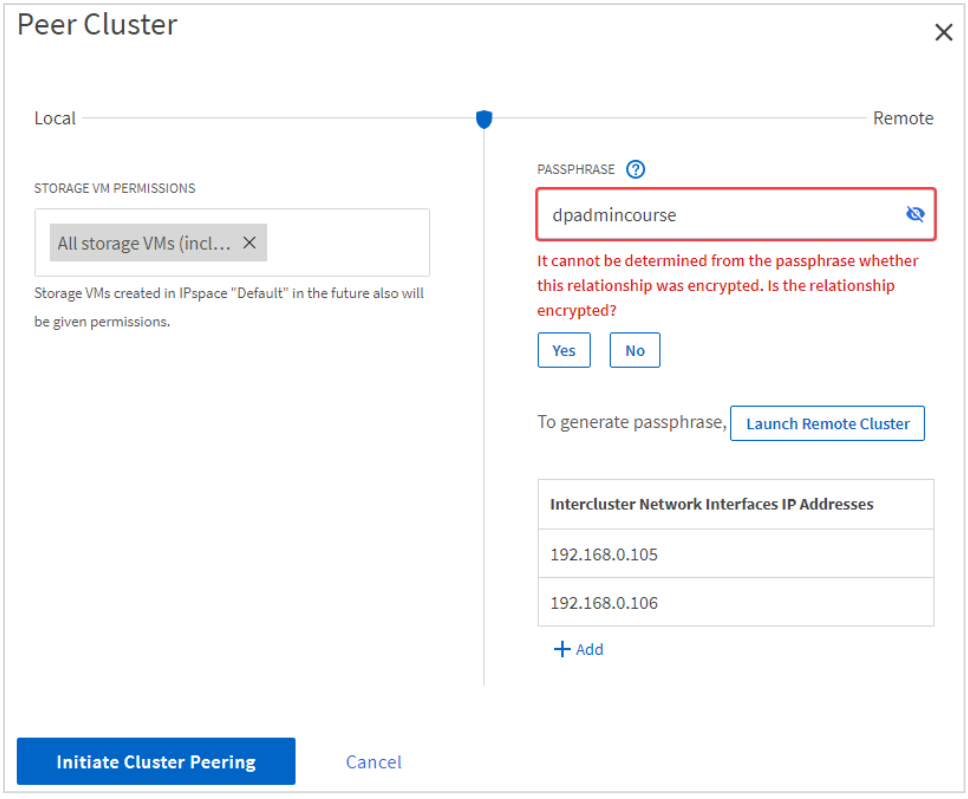
Step	Action
2-5	In the Add Network Interface dialog box, specify the following values: ▪ Interface Role: **Intercluster** ▪ Name: **`Intercluster_LIF1`** ▪ Home Node: **cluster2-01** ▪ IP Address: **`192.168.0.107`** ▪ Subnet Mask: **`24`** 
2-6	Click **Save**.
2-7	Verify that Intercluster_LIF1 appears in the Network Interfaces list. 

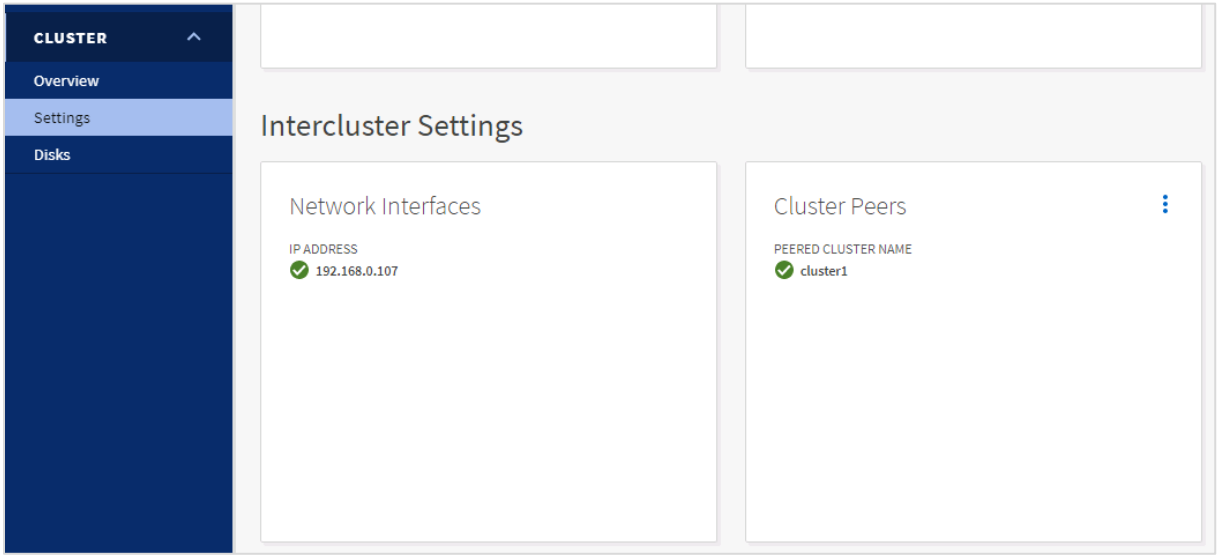
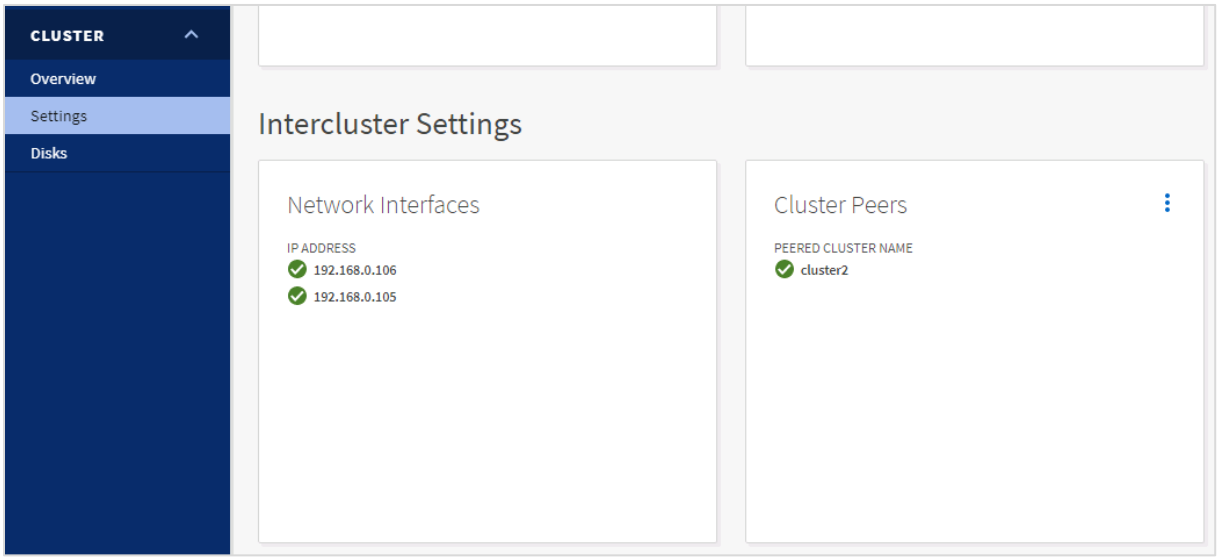
Task 3: Configure Cluster Peering

Cluster peering is a requirement of intercluster communication. In this task, you configure a peer relationship between cluster1 and cluster2. You must create the peer relationship on cluster1 and then use the same steps to create the relationship on cluster2.

Step	Action
3-1	**Cluster1** On cluster1, in the System Manager navigation pane, select **Cluster** > **Settings**. 
3-2	Perform the following steps: a. In the Intercluster Settings > Network Interfaces pane, scroll down and verify the intercluster LIF details for cluster1. b. In the Intercluster Settings > Cluster Peers pane, click **Peer Cluster**. 

Step	Action
3-3	On the Peer Cluster page, perform the following steps: a. For Passphrase, enter **`dpadmincourse`**. b. In the Passphrase textbox, click the eyeball icon c. In response to the question “Is the relationship encrypted?”, click **Yes**. d. Click **+Add**. e. In the Intercluster Network Interfaces IP Addresses field, enter **`192.168.0.107`**. f. Click outside the textbox. 
3-4	The passphrase must be at least eight characters. You can use any passphrase, but you must use the same passphrase on both clusters.
3-5	Click **Initiate Cluster Peering**.

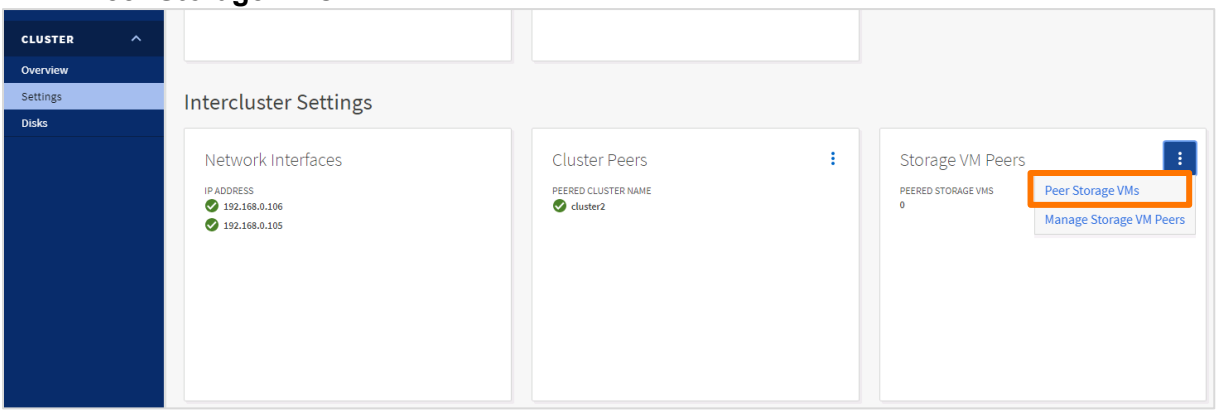
Step	Action
3-6	**Cluster2** Perform the following steps: a. In the System Manager navigation pane, select **Cluster** > **Settings**. b. In the Intercluster Settings > Cluster Peers pane, click **Peer Cluster**. 
3-7	On the Peer Cluster page, perform the following tasks: a. For Passphrase, enter **`dpadmincourse`**. b. For relationship encryption, click **Yes**. c. Add two Intercluster Network Interfaces IP Addresses: **`192.168.0.105`** and **`192.168.0.106`**. 

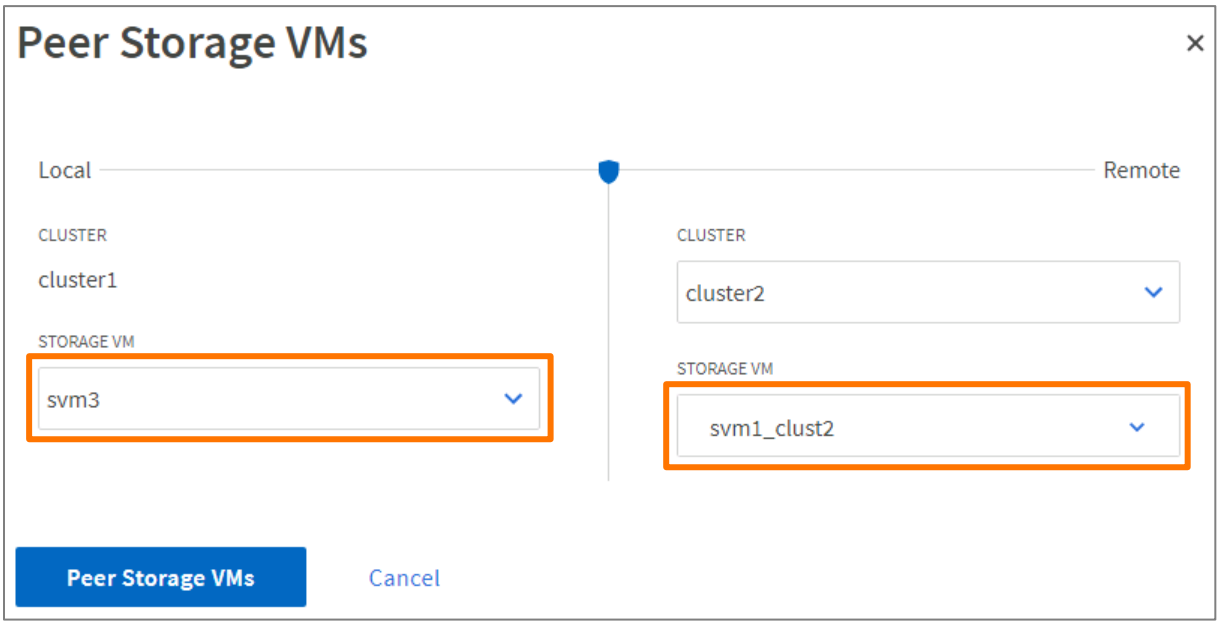
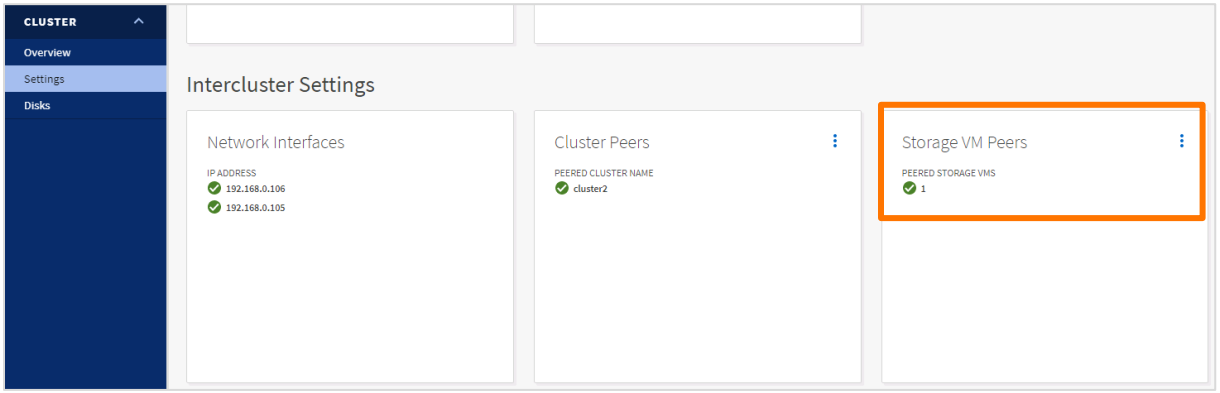
Step	Action
3-8	Click **Initiate Cluster Peering**.
3-9	In the Intercluster Settings > Cluster Peers pane, verify that cluster1 appears, indicating that the cluster peering is successful on cluster2. Wait a few seconds for the peering operation to complete. 
3-10	**Cluster1** On cluster1, in the System Manager navigation pane, select **Cluster** > **Settings**.
3-11	In the Intercluster Settings > Cluster Peers pane, verify that cluster peering is successful on cluster1. Wait a few seconds for the status icon to turn green. If necessary, refresh the screen. 

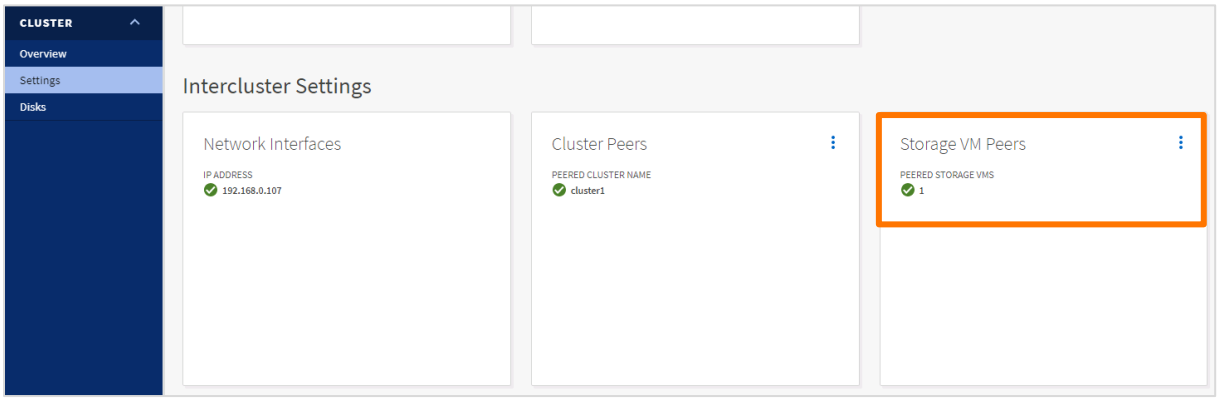
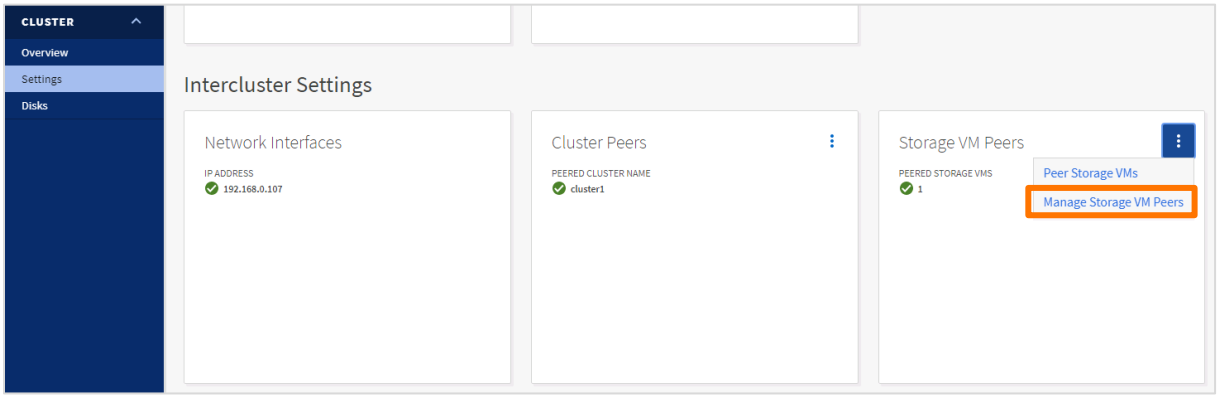
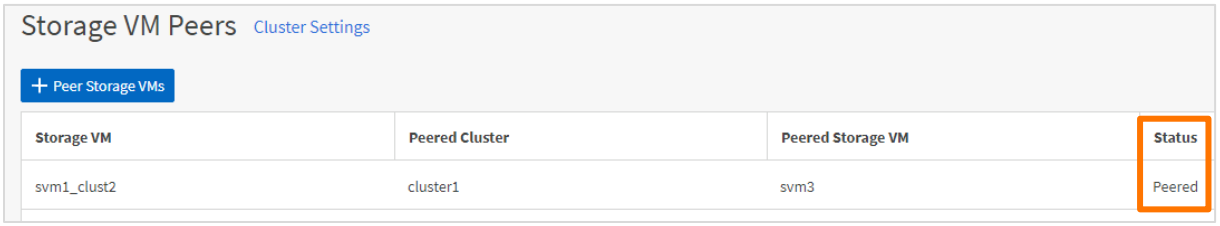
Step	Action
3-12	In the CLI for both cluster1 and cluster2, run the following commands to review the cluster peering status: • `cluster peer show` • `cluster peer health show` • `cluster peer ping`
3-13	You continue with SVM peering in Task 4.

Task 4: Configure SVM Peering

In this task, you create a peer relationship between svm3 on cluster1 and svm1_clust2 on cluster2.

Step	Action
4-1	**Cluster1** Perform the following steps: a. In the System Manager navigation pane, select **Cluster** > **Settings**. b. In the Intercluster Settings > Storage VM Peers pane, click the three vertical dots, and then select **Peer Storage VMs**. 

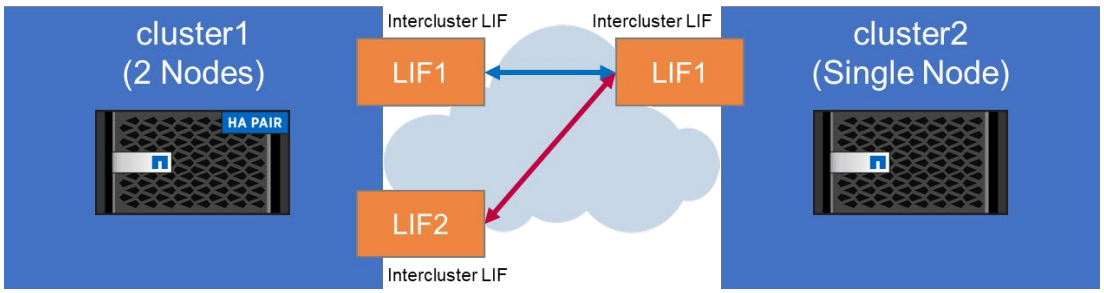
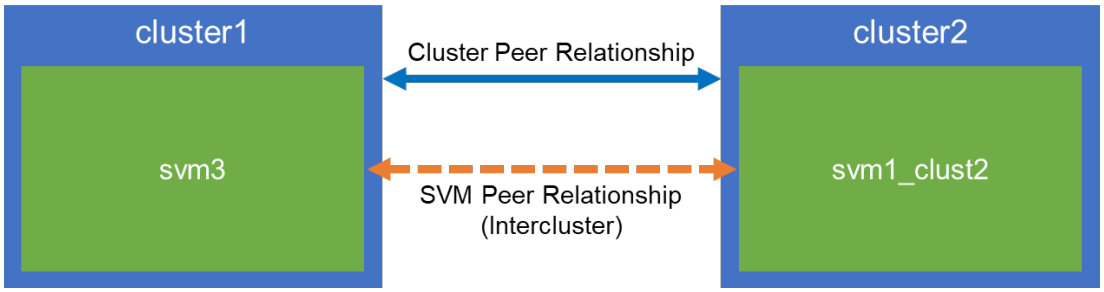
Step	Action
4-2	On the Peer Storage VMs page, provide the following information: ▪ cluster1 Storage VM: **svm3** ▪ cluster2 Storage VM: **svm1_clust2** *(selected)* 
4-3	Click **Peer Storage VMs**.
4-4	Verify that the peering is successful and is listed under Storage VM Peers. 
4-5	**Cluster2** In the System Manager navigation pane, select **Cluster** > **Settings**.

Step	Action
4-6	In the Intercluster Settings > Storage VM Peers pane, verify that the peering is successful and is listed. If necessary, refresh the screen. 
4-7	In the Intercluster Settings > Storage VM Peers pane, click the three vertical dots, and then select **Manage Storage VM Peers**. 
4-8	On the Storage VM Peers page, verify that the SVM peer relationship is listed and that the status is Peered. 
4-9	**Cluster1** In the System Manager navigation pane, select **Cluster** > **Settings**.
4-10	In the Intercluster Settings > Storage VM Peers pane, click the three vertical dots, and then select **Manage Storage VM Peers**.

Step	Action
4-11	On the Storage VM Peers page, verify that the SVM peer relationship is listed and that the status is Peered. 

Task 5: Review the Exercise Environment

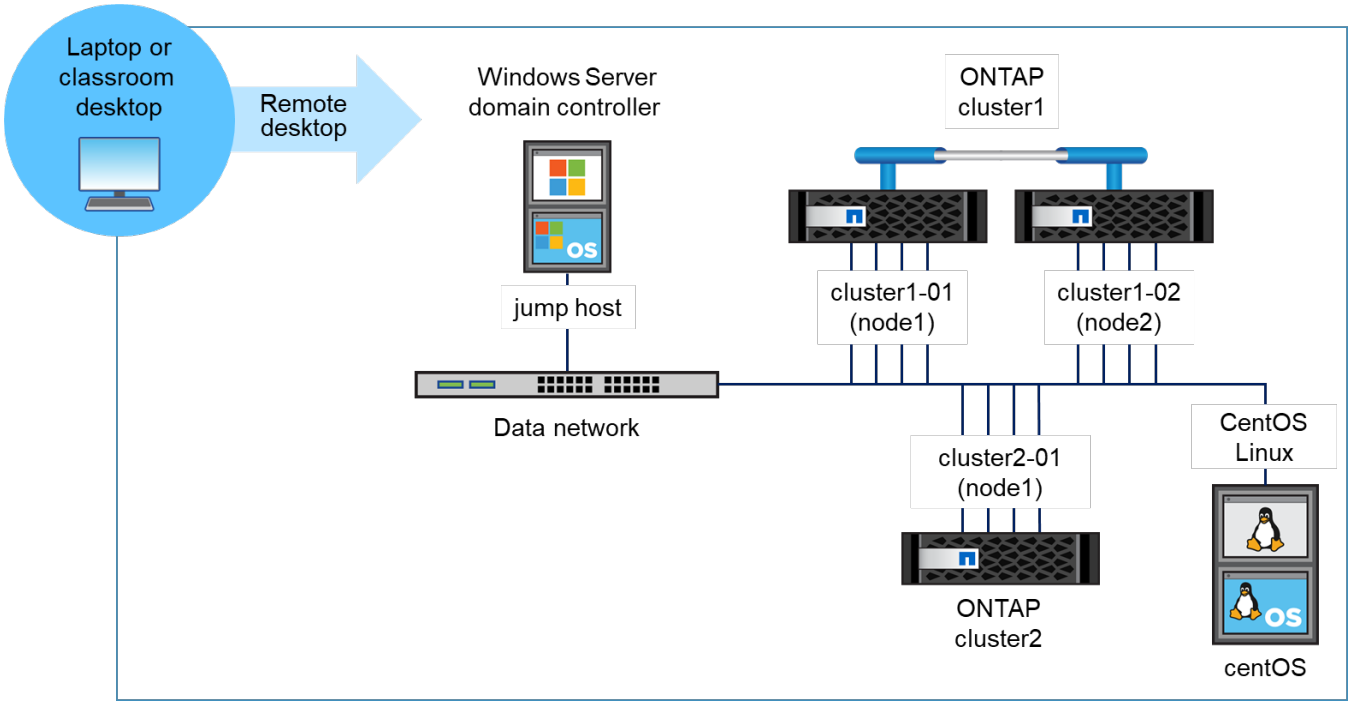
In this task, you review the exercise environment that you created in the previous tasks.

Step	Action
5-1	Verify that you configured intercluster LIFs on each node of the two ONTAP clusters. 
5-2	Verify that the following actions occurred: ▪ You established peer relationships between the cluster1 and cluster2 ONTAP clusters. ▪ You created a peer relationship between the svm3 and svm1_clust2 SVMs on each cluster. 

End of exercise

Module 3: SnapMirror Operation

Exercise Equipment Diagram



System	Host Name	IP Addresses	User Name	Password
Windows Server 2012 R2	JUMPHOST	192.168.0.5	demo\Administrator	Netapp1!
ONTAP cluster-management LIF	cluster1	192.168.0.101	admin (case-sensitive)	Netapp1!
node 1	cluster1-01	192.168.0.111	admin (case-sensitive)	Netapp1!
node 2	cluster1-02	192.168.0.112	admin (case-sensitive)	Netapp1!
ONTAP cluster-management LIF	cluster2	192.168.0 102	admin (case-sensitive)	Netapp1!
node 1	cluster-01	192.168.0 113	admin (case-sensitive)	Netapp1!
Linux Server	centos65	192.168.0.21	root	Netapp1!

Exercise 1: Using SnapMirror Asynchronous to Mirror FlexVol Volumes

In this exercise, you create and implement a SnapMirror Asynchronous relationship between a source volume on cluster1 and a destination volume on cluster2. You follow a SnapMirror implementation workflow to implement the solution. Then you verify data transfer.

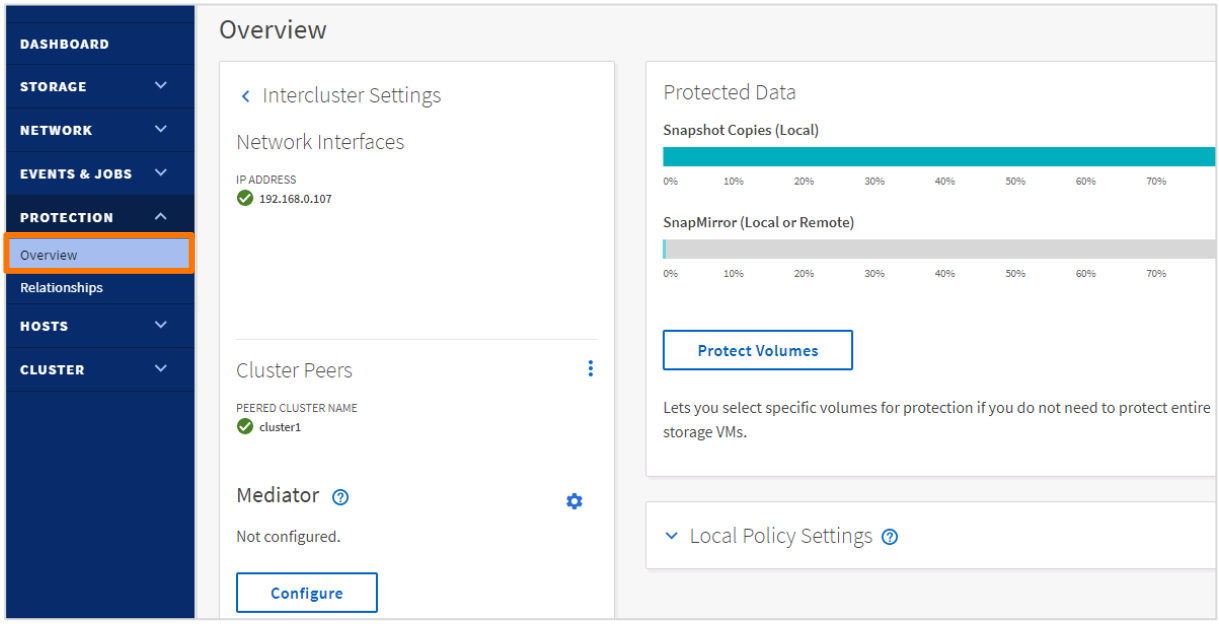
Objectives

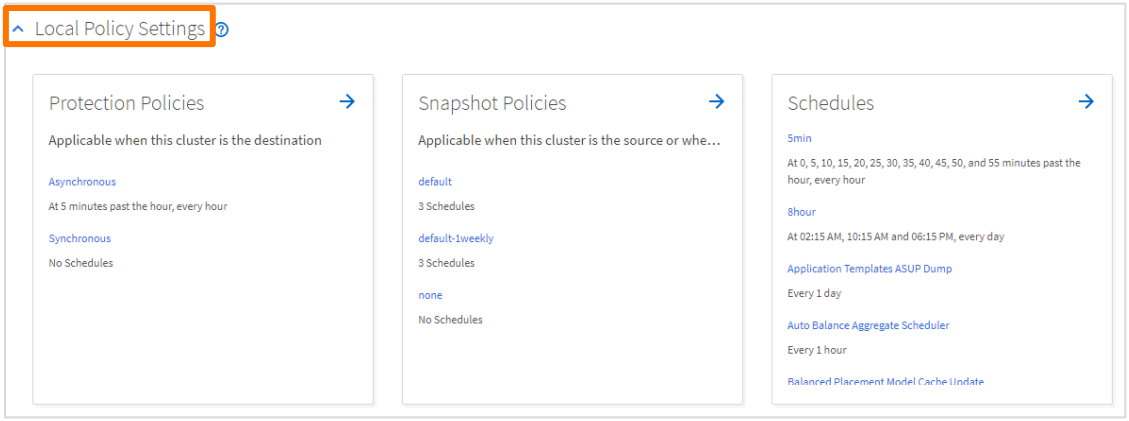
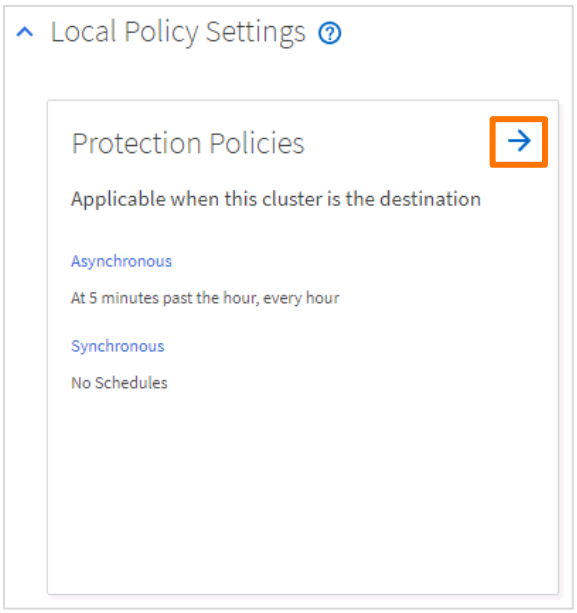
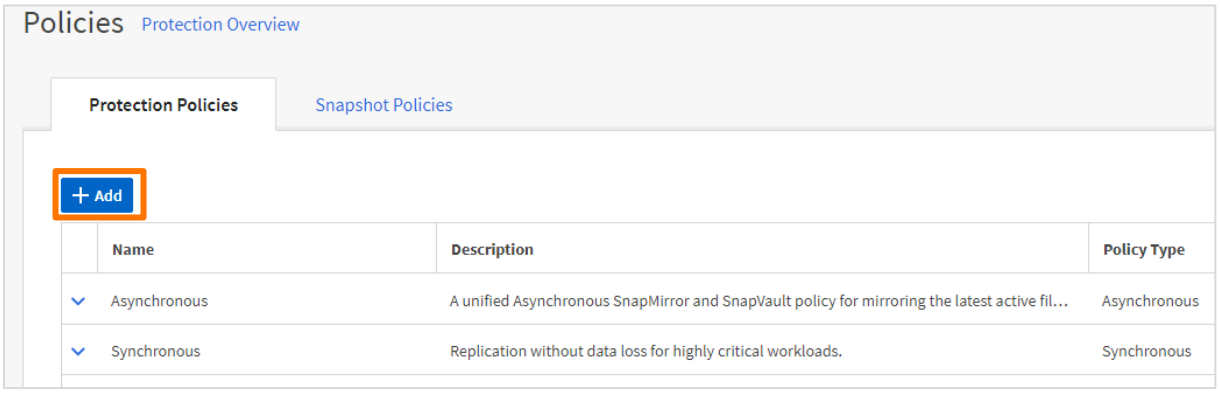
This exercise focuses on enabling you to do the following:

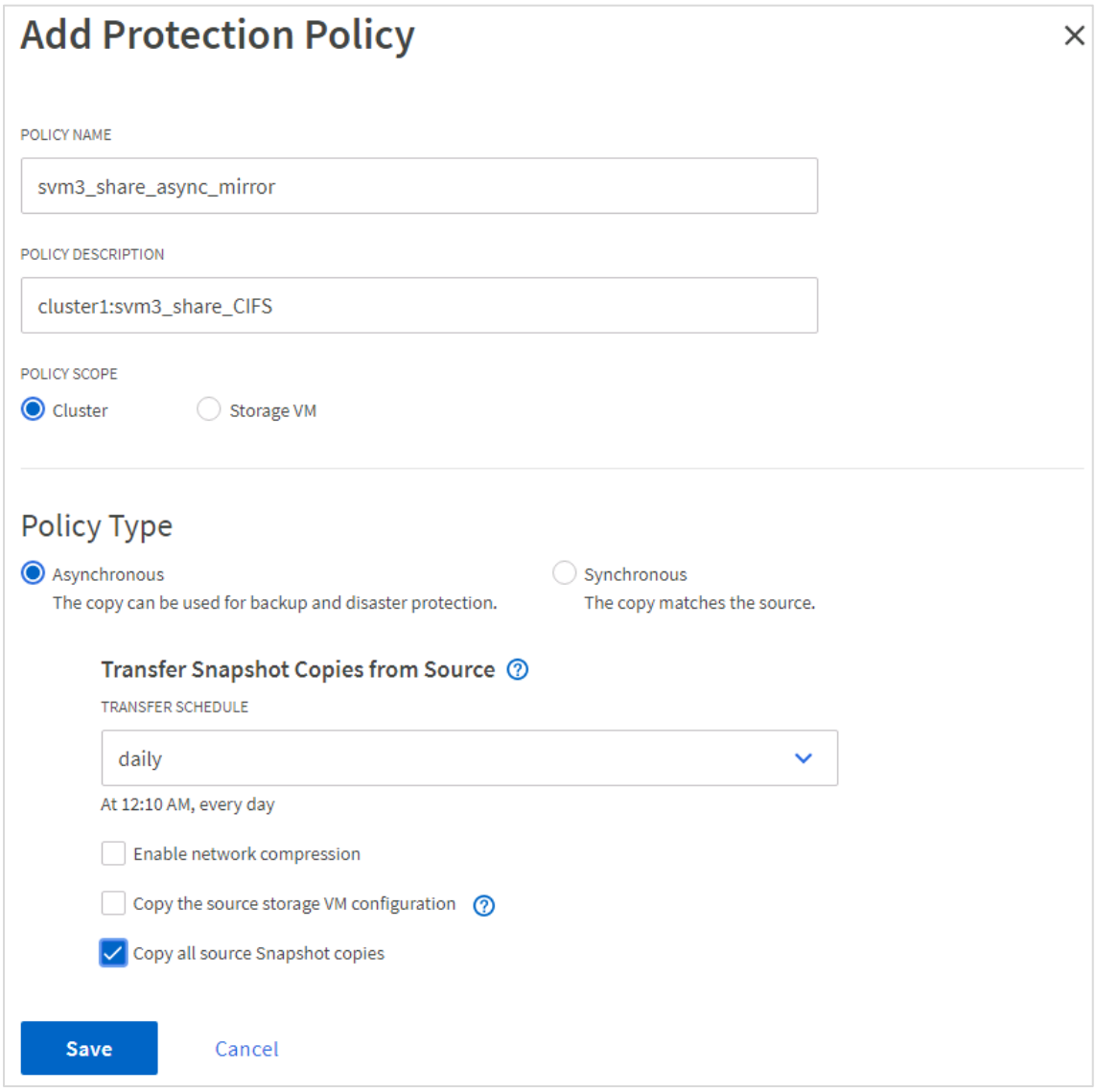
- Create a SnapMirror policy
- Create a SnapMirror relationship
- Perform an initial SnapMirror transfer
- Perform a manual SnapMirror update
- Schedule automatic SnapMirror updates
- Verify data transfer

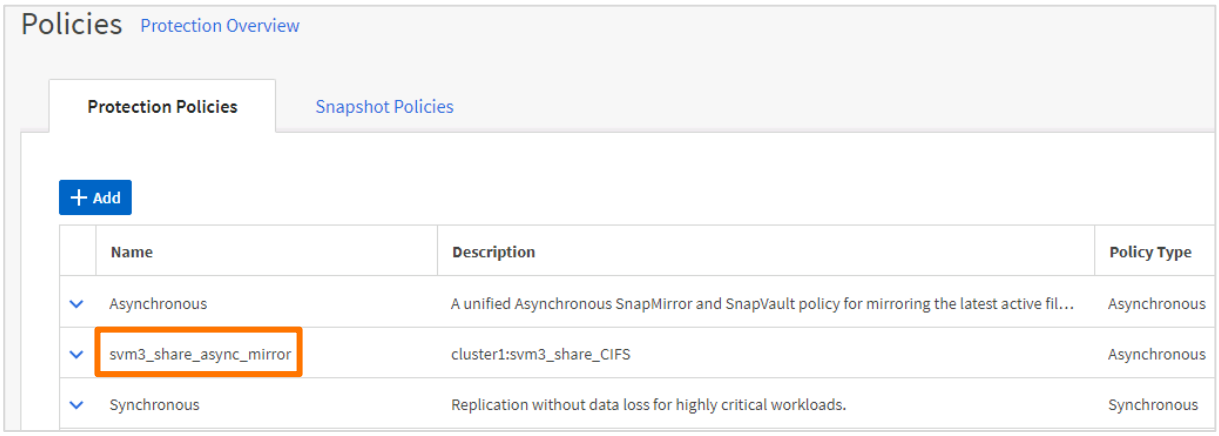
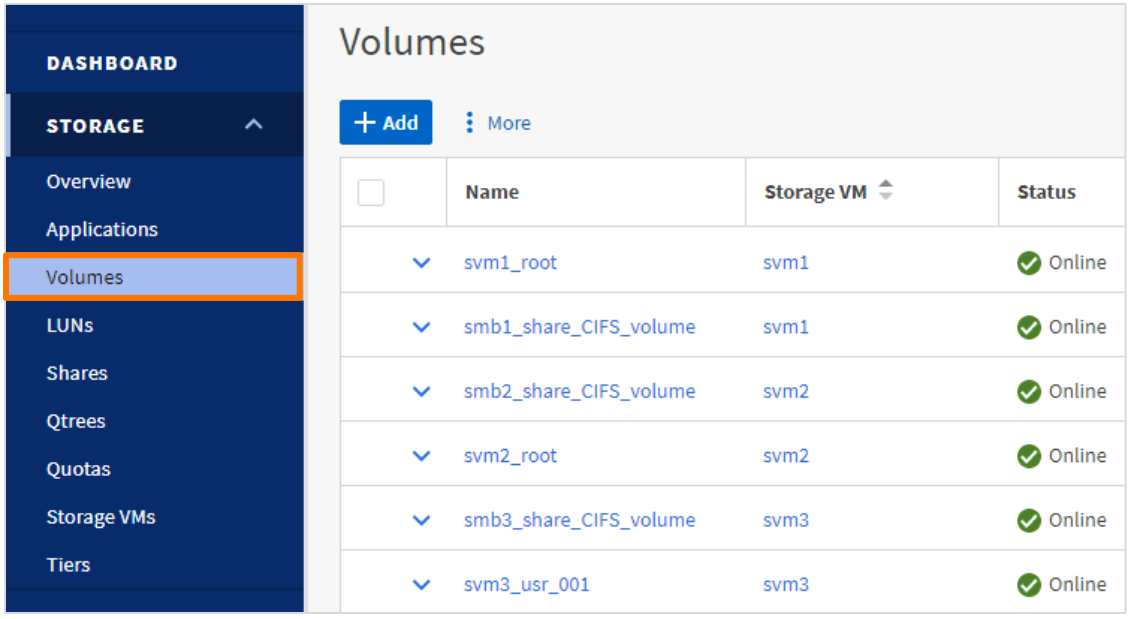
Task 1: Create a SnapMirror Asynchronous Policy and Configure a SnapMirror Relationship

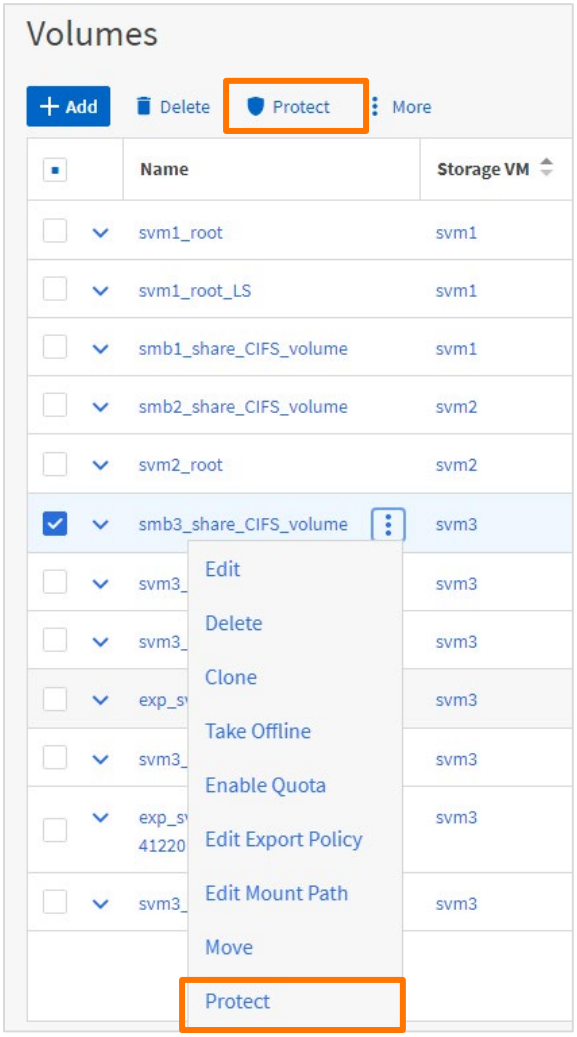
In this task, you use NetApp ONTAP System Manager to create a SnapMirror policy and relationship, and you configure SnapMirror updates.

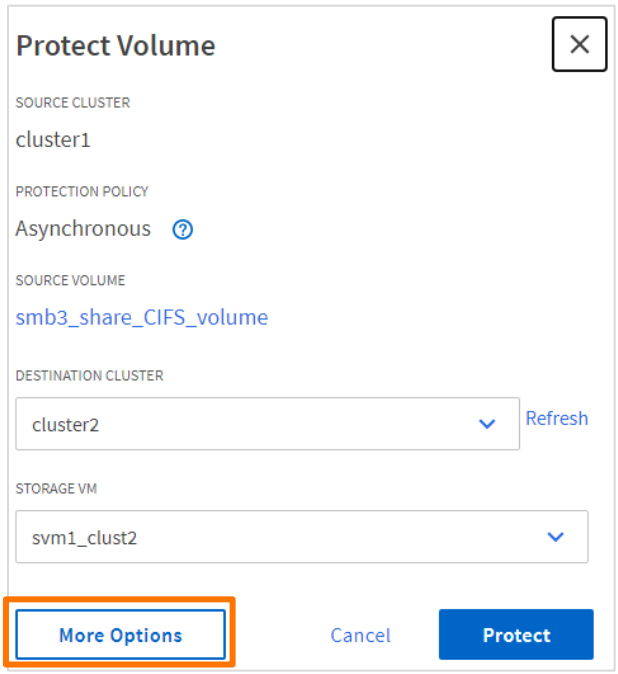
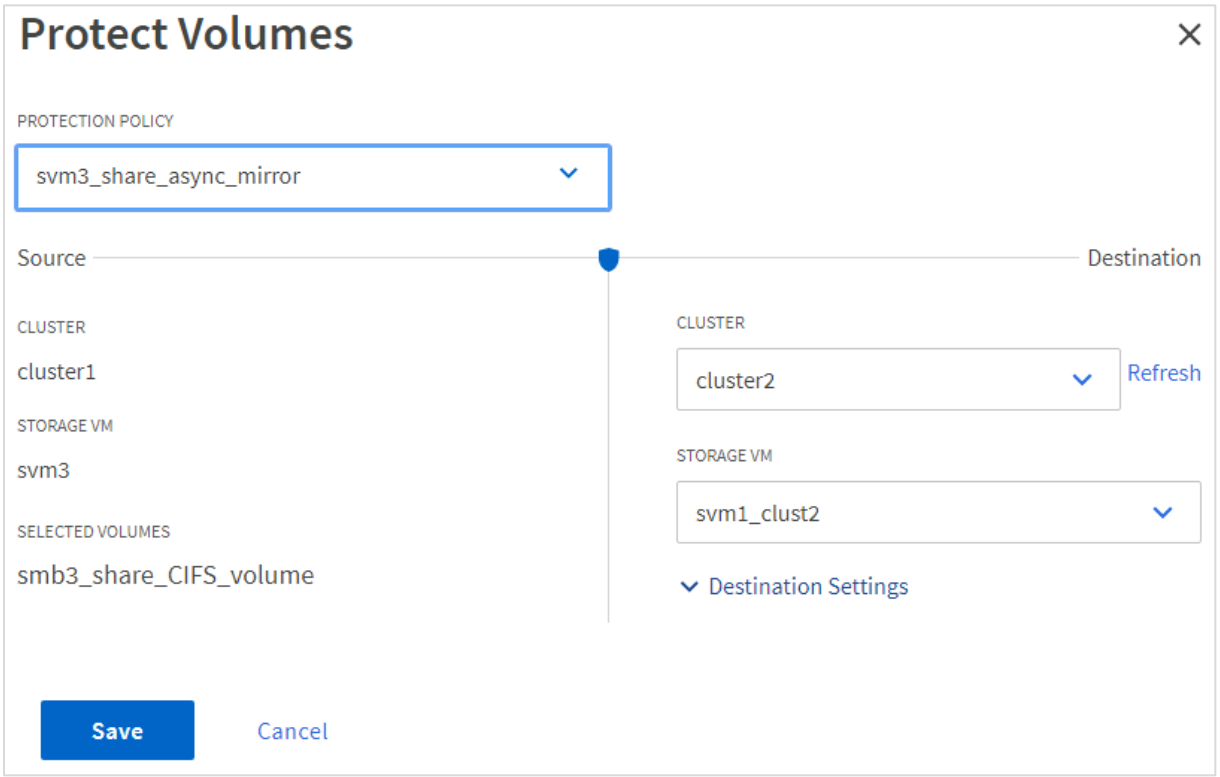
Step	Action
1-1	Cluster2 is the destination cluster for the protection relationship. You create the custom SnapMirror policy on the destination cluster.
1-2	**Cluster2** In the System Manager navigation pane, select **Protection** > **Overview**. 

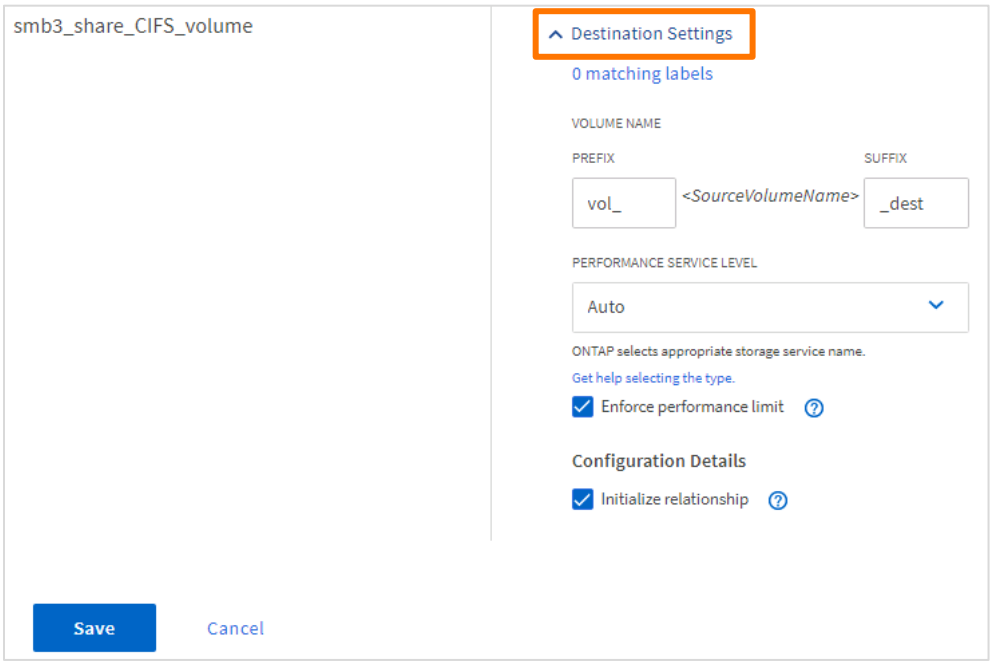
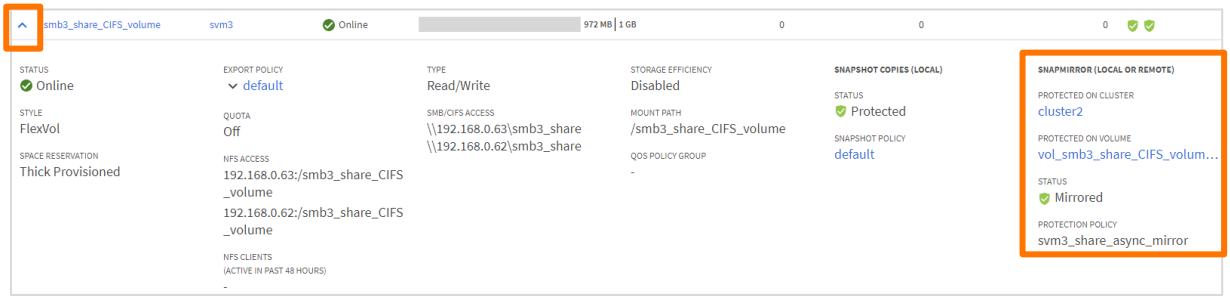
Step	Action
1-3	Expand **Local Policy Settings**. 
1-4	In the **Local Policy Settings** > **Protection Policies** pane, click the arrow in the upper-right corner. 
1-5	In the Policies > Protection Policies pane, click **+Add** to create a policy. 

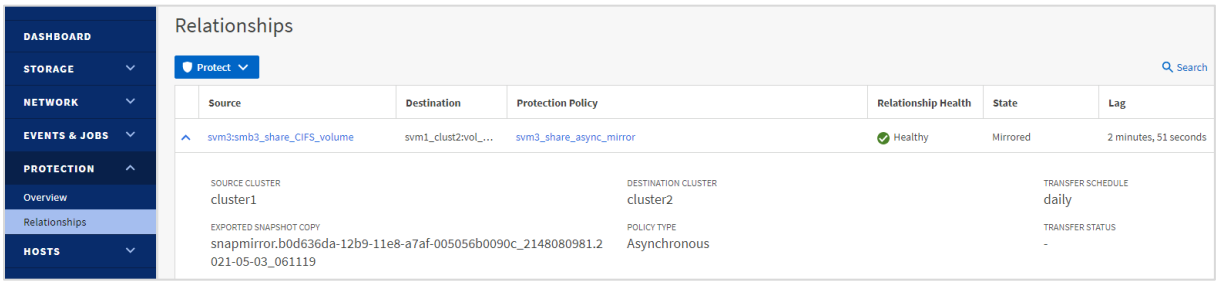
Step	Action
1-6	In the Add Protection Policy dialog box, specify the following values: ▪ Policy Name: **`svm3_share_async_mirror`** ▪ Policy Description: **`cluster1:svm3_share_CIFS`** ▪ Policy Scope: **Cluster** ▪ Policy Type: **Asynchronous** ▪ Transfer Schedule: **daily** ▪ Enable network compression checkbox: *clear* ▪ Copy the source storage VM configuration checkbox: *clear* ▪ Copy all source Snapshot copies checkbox: *selected* 
1-7	Click **Save**.

Step	Action
1-8	Verify that the policy was created successfully. 
1-9	Cluster1 is the source cluster in the protection relationship. Next, you protect the volume smb3_share_CIFS_volume on svm3 with the SnapMirror policy that you created.
1-10	**Cluster1** In the System Manager navigation pane, select **Storage** > **Volumes**. 
1-11	In the Protection column, observe the status of all the volumes. 

Step	Action
1-12	In the Protection column, the first icon in the column indicates protection with Snapshot copies and the second icon indicates protection with SnapMirror (local or remote).
1-13	Click the three vertical dots to the right of smb3_share_CIFS_volume, and then select **Protect**. Alternatively, you can select the **smb3_share_CIFS_volume** checkbox to select the volume, and then click **Protect** at the top of the Volumes list. 

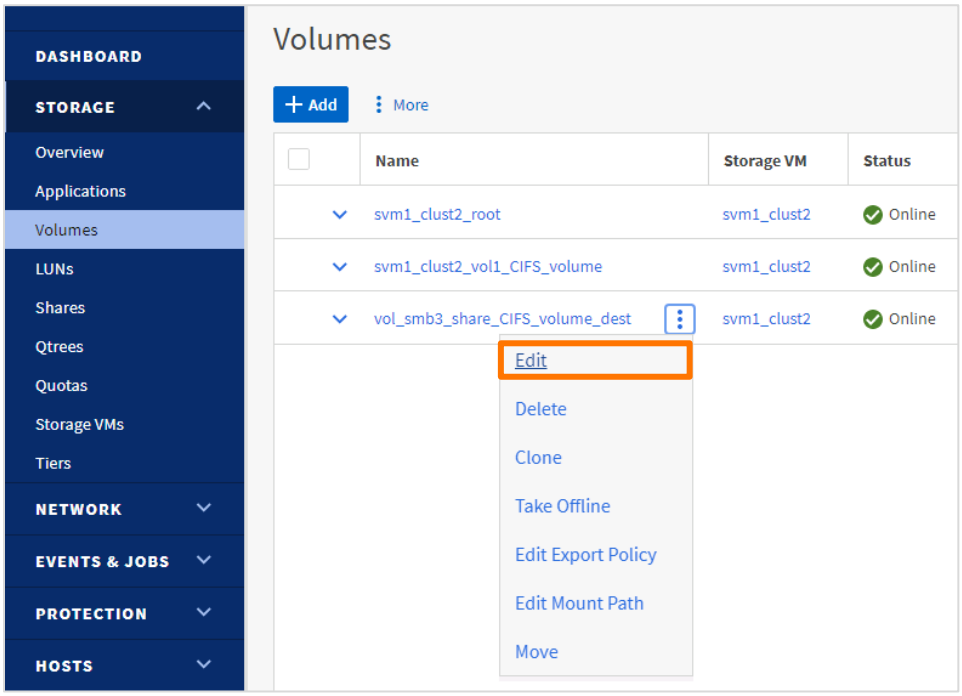
Step	Action
1-14	In the Protect Volume dialog box, click **More Options**. 
1-15	In the Protect Volumes pane, specify the following values: ▪ Protection Policy: **svm3_Share_async_mirror** ▪ Destination > Cluster: **cluster2** ▪ Destination > Storage VM: **svm1_clust2** 

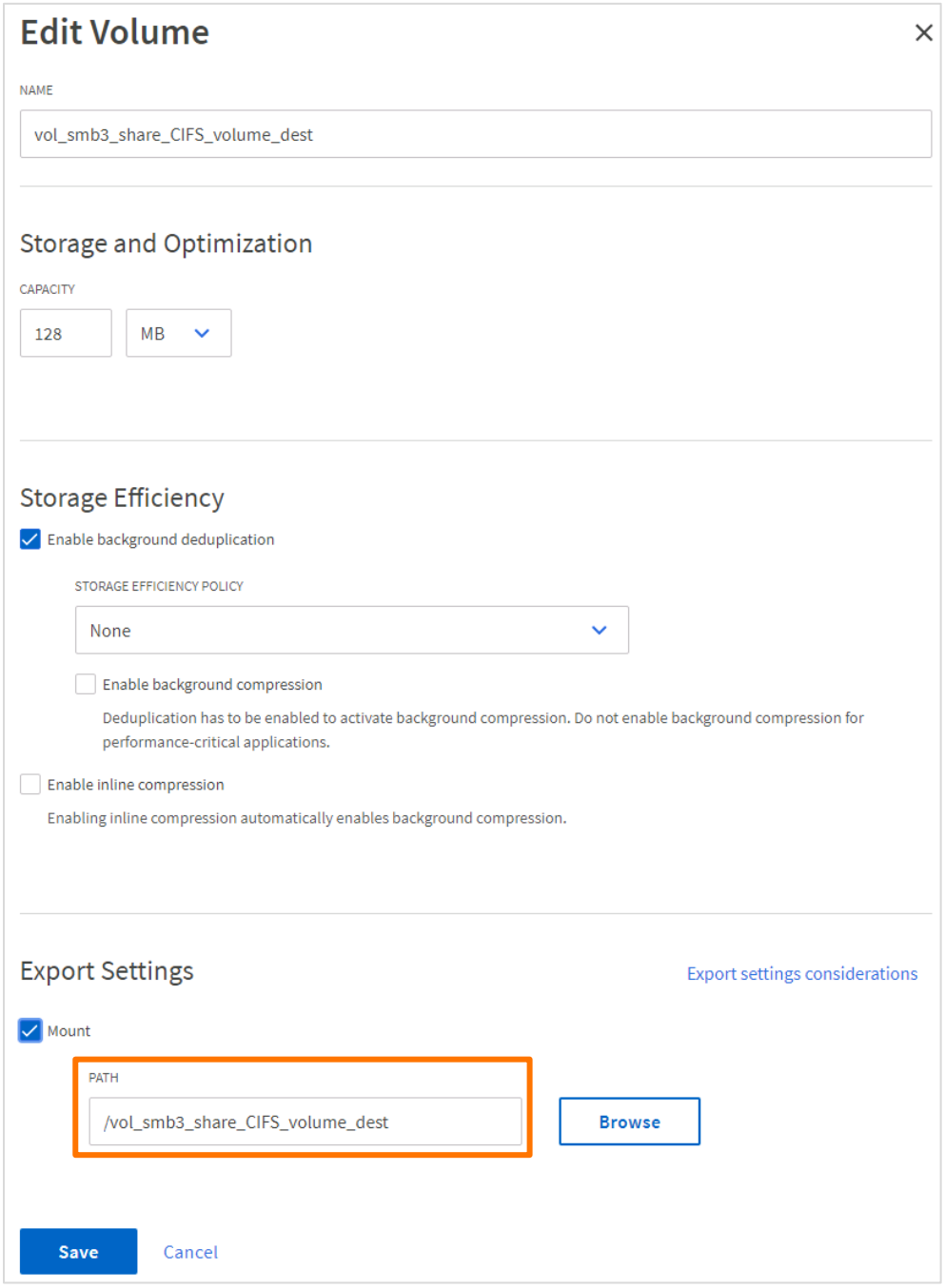
Step	Action
1-16	Expand **Destination Settings**. 
1-17	Review the Destination Settings values, but do not make any changes.
1-18	Click **Save**.
1-19	Note the appearance of the Adding Relationship status box for a few seconds. Optionally, you may click **Run in Background**.
1-20	In the Volumes pane, note the Protection status for smb3_share_CIFS_volume.
1-21	In the Volumes pane, click the down arrow to the left of the volumes smb3_share_CIFS_volume to view details and verify that the protection relationship was created successfully. 
1-22	**Cluster2** Return to System Manager on cluster2.
1-23	In the navigation pane, select **Protection** > **Relationships**.

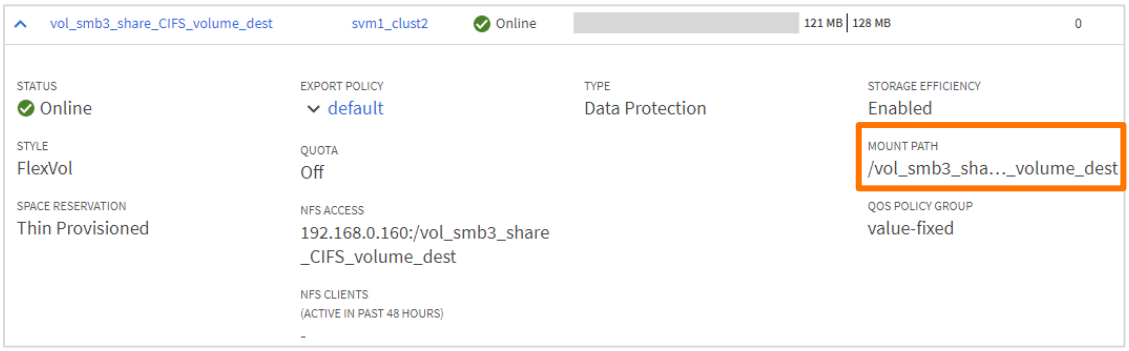
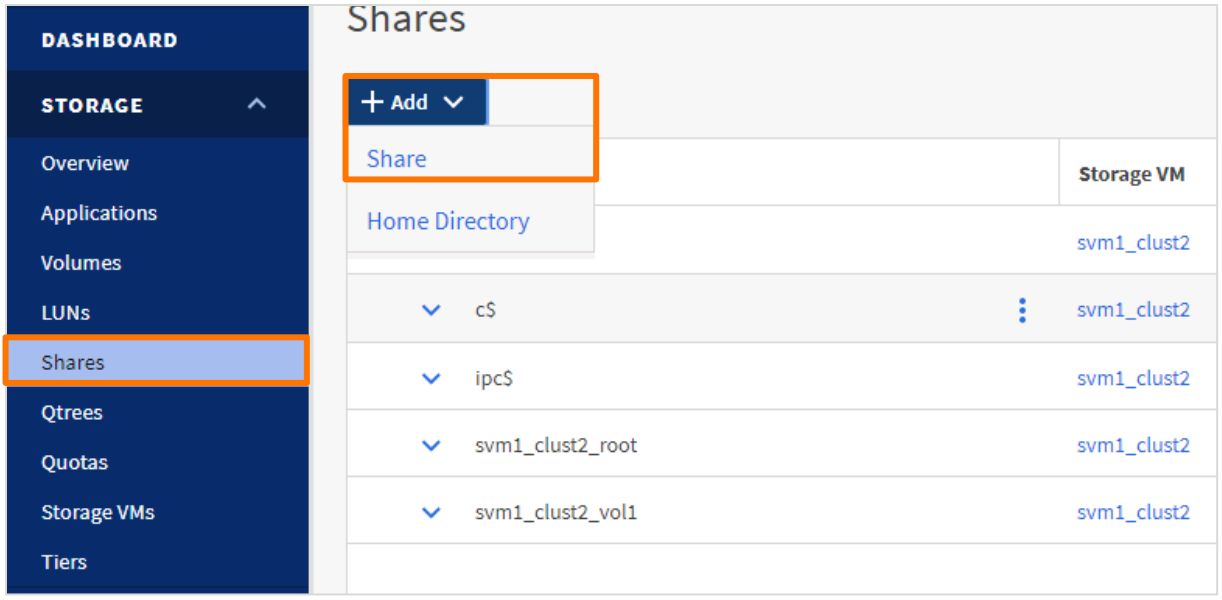
Step	Action
1-24	To confirm the SnapMirror status, expand the listed relationship. 
1-25	Answer the following questions: ▪ Is the relationship healthy? _____ ▪ What is the relationship state? _____ ▪ What is the policy type? _____

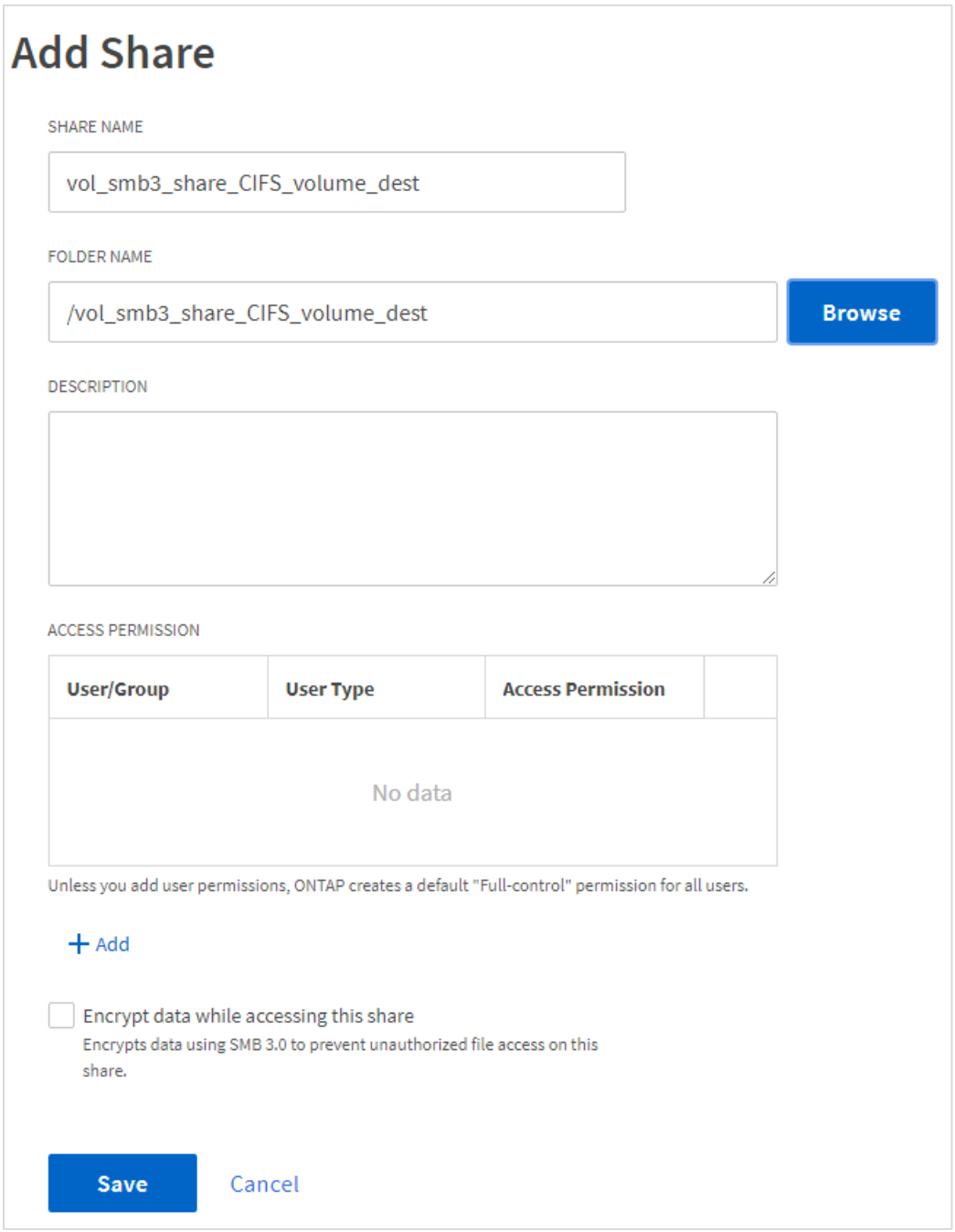
Task 2: Verify Data Transfer

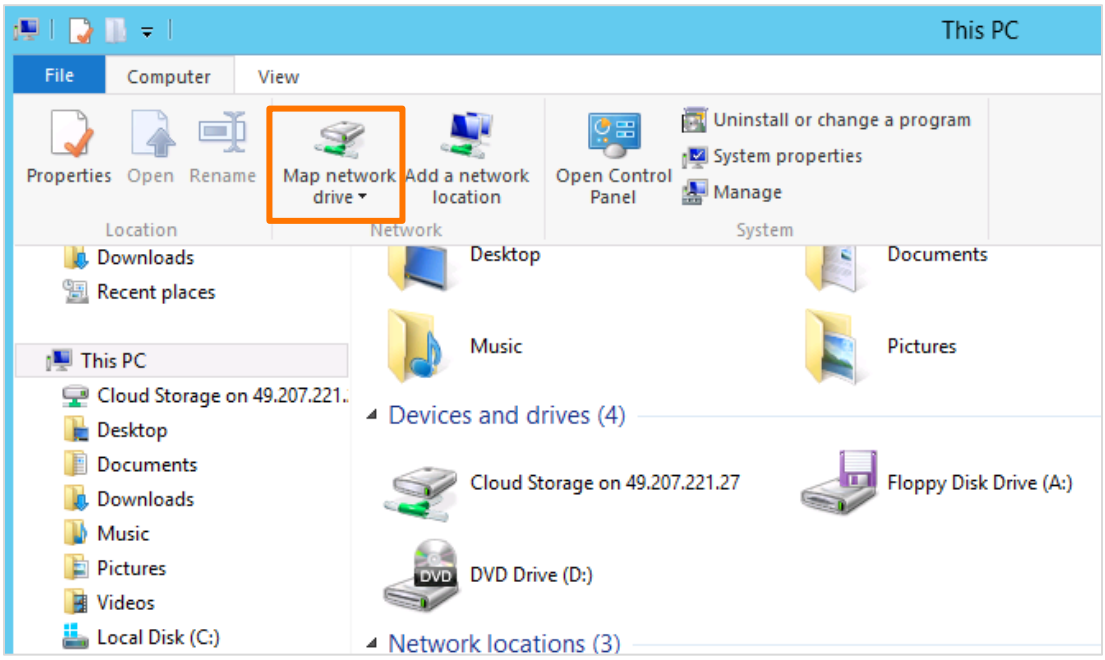
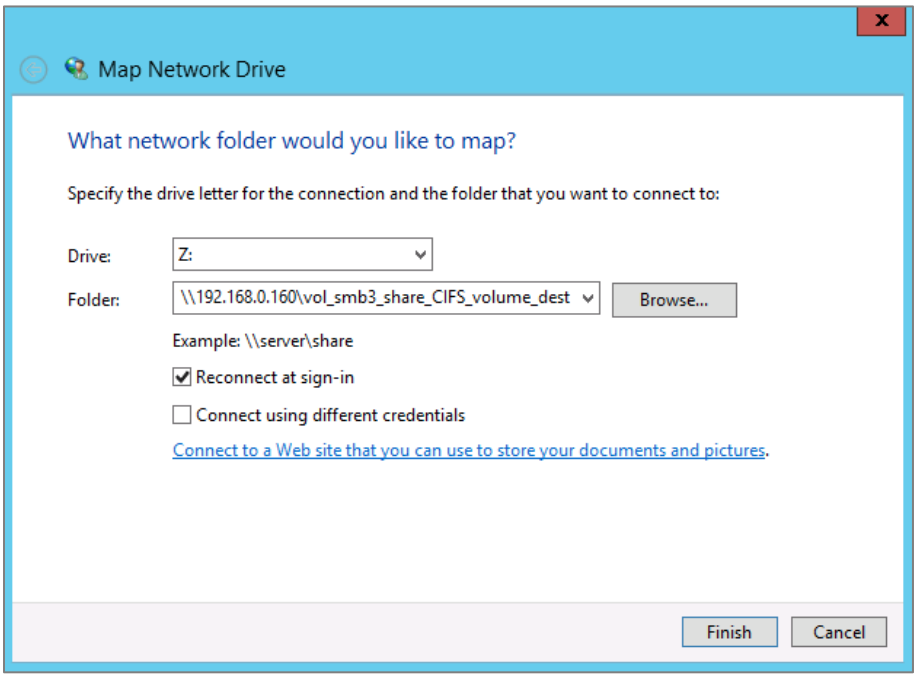
In this task, you first look at the SnapMirror destination volume to see the initialized data. You then create data on the primary volume. You perform a manual update and then verify that the new data was transferred to the SnapMirror destination volume.

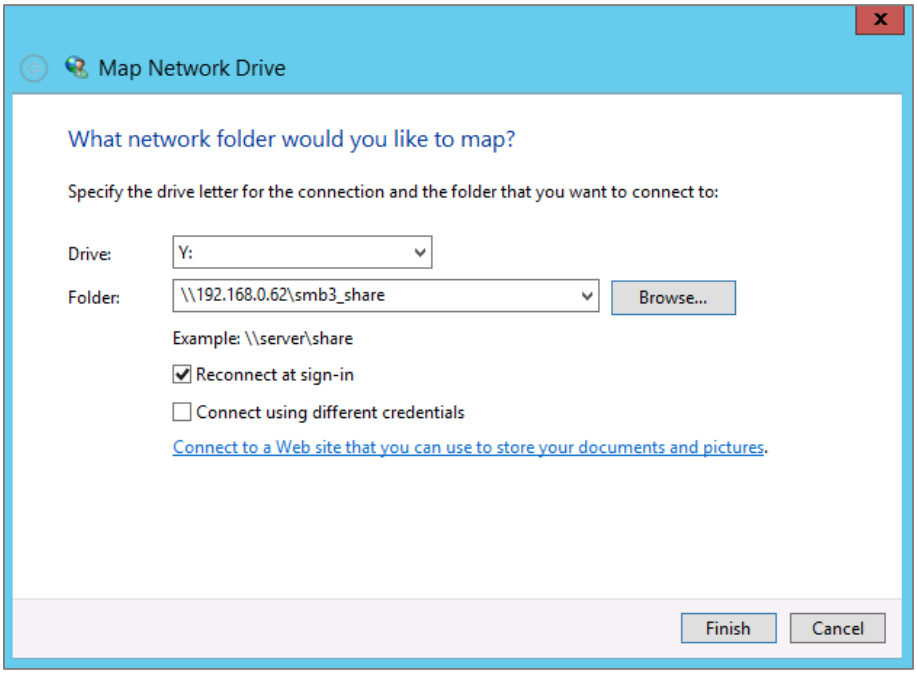
Step	Action
2-1	During the creation and initialization of the SnapMirror relationship, the SnapMirror secondary volume is not automatically mounted. To see the data that is copied to the SnapMirror secondary volume, you must first mount the secondary volume in the cluster namespace. In the following steps, you mount the secondary volume in the cluster2 namespace.
2-2	**Cluster2** In the System Manager navigation pane, select **Storage** > **Volumes**.
2-3	Click the three vertical dots to the right of vol_smb3_share_CIFS_volume_dest, and then select **Edit**. 

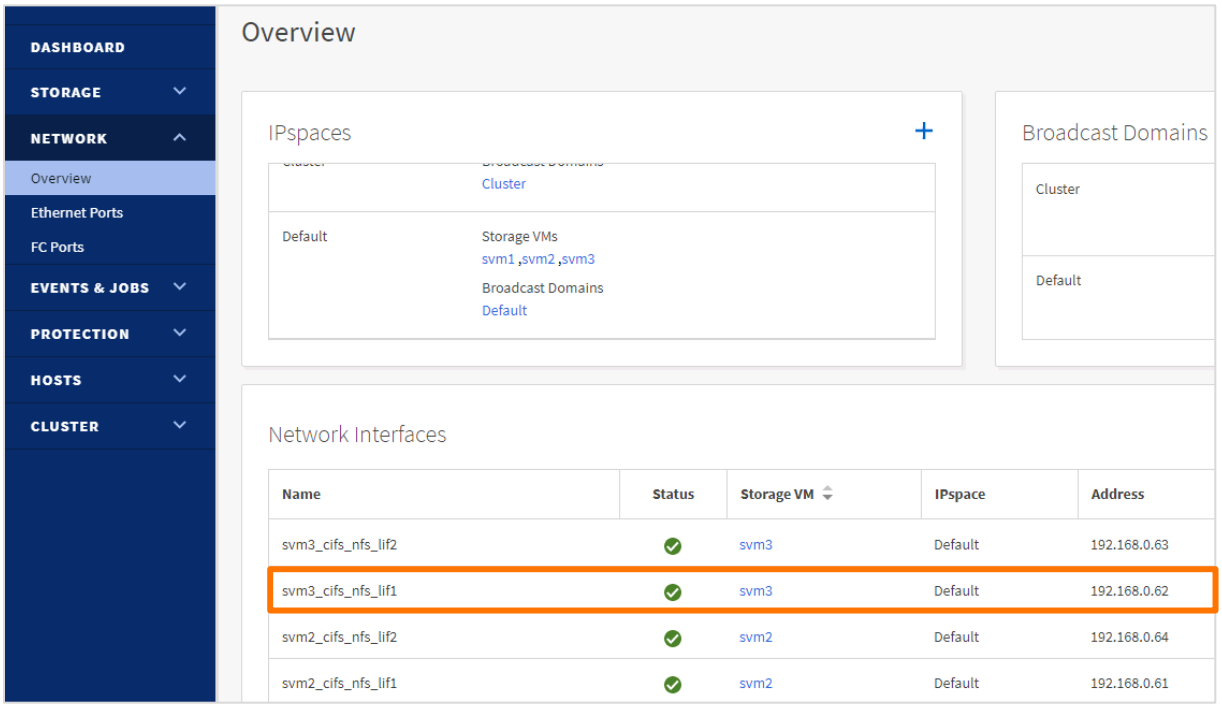
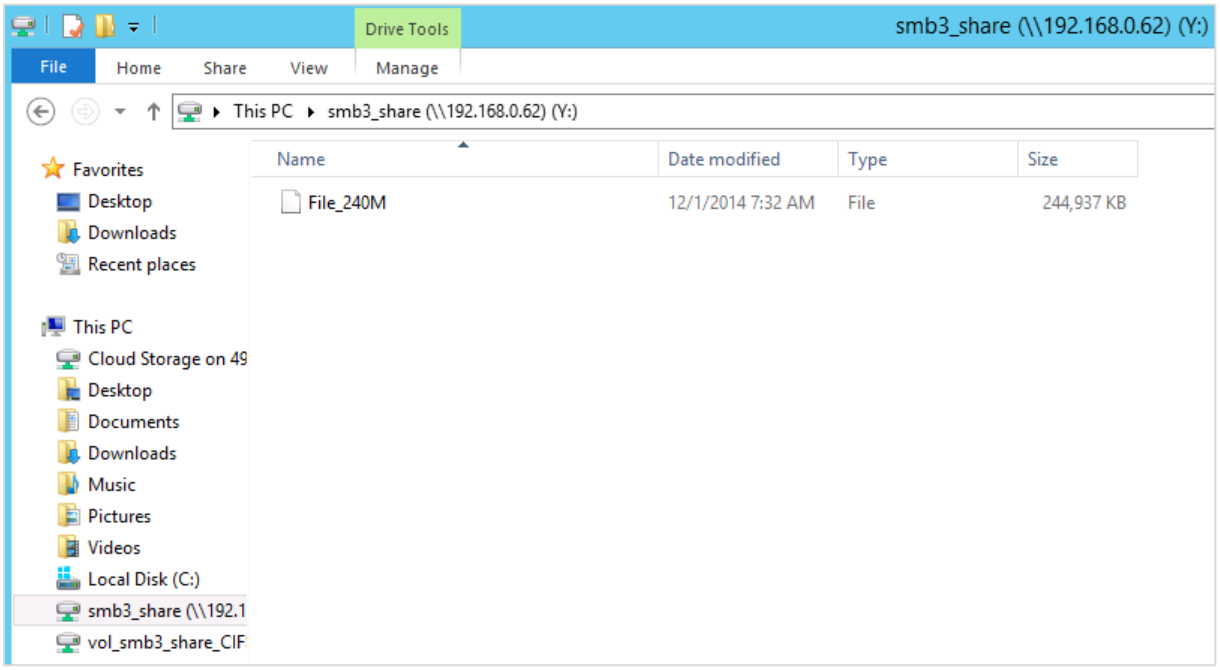
Step	Action
2-4	In the Edit Volume pane, perform the following steps: a. Retain the default values for all the fields. b. Scroll down to the Export Settings section and note the volume mount path (/vol_smb3_share_CIFS_volume_dest). 
2-5	Select the **Mount** checkbox, and then click **Save**.

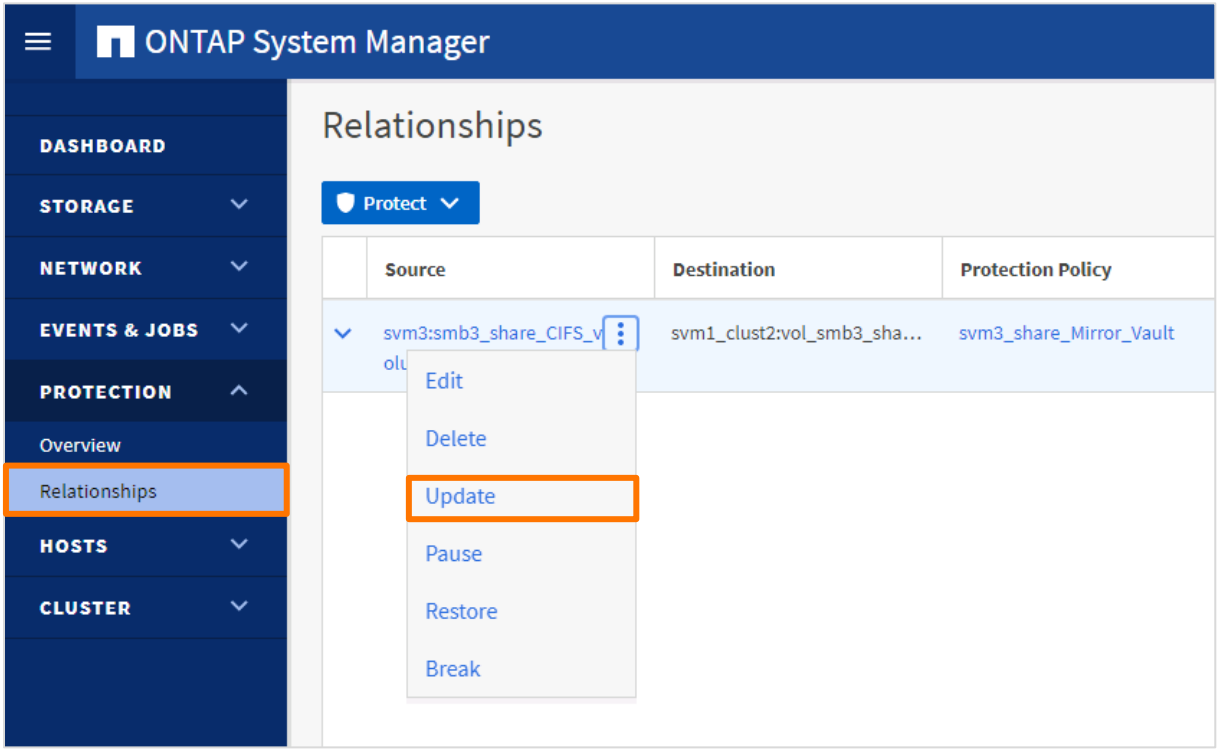
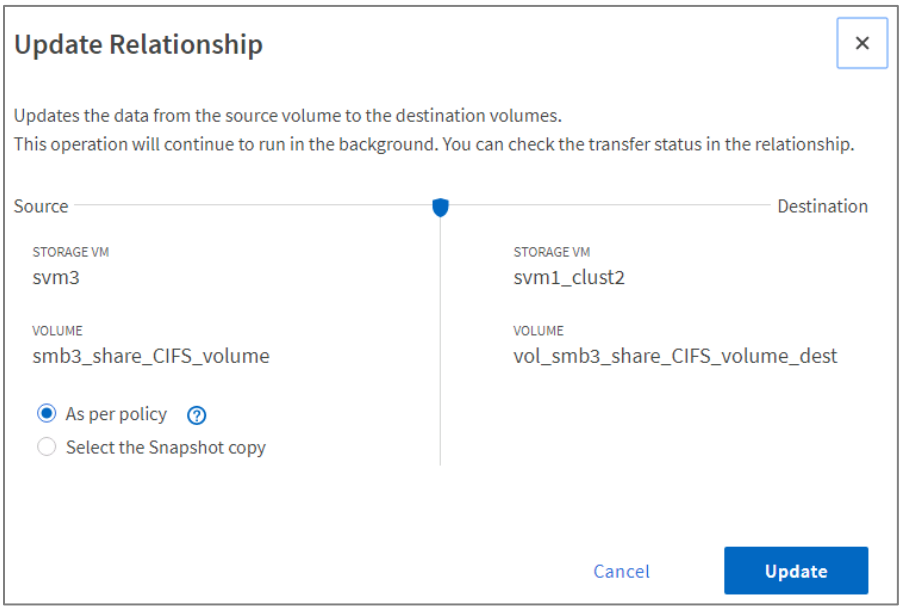
Step	Action
2-6	In the Volumes pane, expand the volume **vol_smb3_share_CIFS_volume_dest** and view its mount path. 
2-7	In the following steps, you create a share for the volume that you added to the namespace.
2-8	**Cluster2** In the System Manager navigation pane, select **Storage** > **Shares**.
2-9	In the Shares pane, click **+Add**, and then select **Share**. 

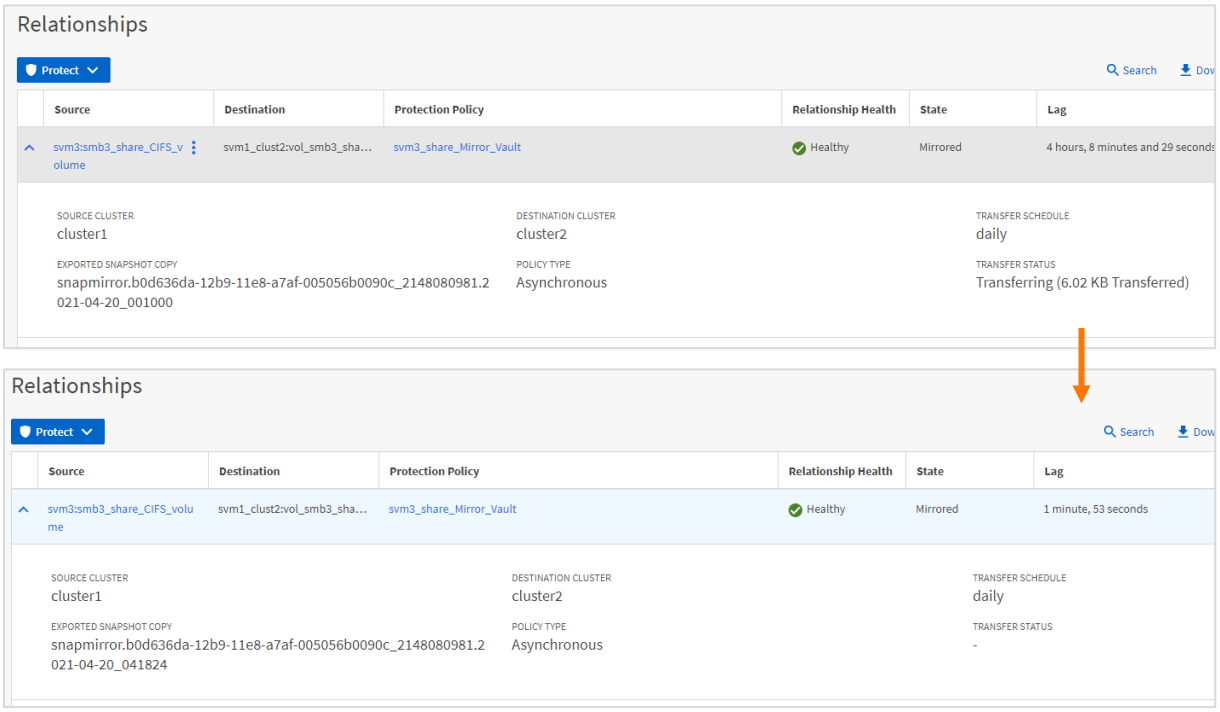
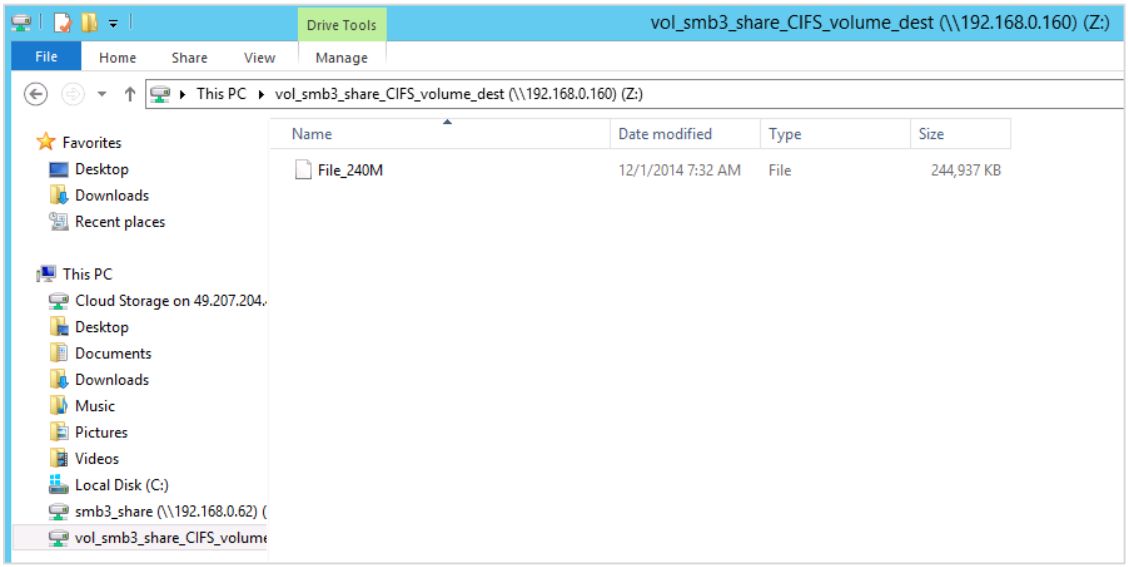
Step	Action
2-10	In the Add Share pane, specify the following values: ▪ Share Name: **`vol_smb3_share_CIFS_volume_dest`** ▪ Folder Name: **`/vol_smb3_share_CIFS_volume_dest`** (Alternatively, you can click **Browse**, and then select the folder.) ▪ Description: *clear* 
2-11	Click **Save**, and then verify that the new share is listed in the Shares pane.
2-12	Next, on the jump host, you map a drive to the destination volume.

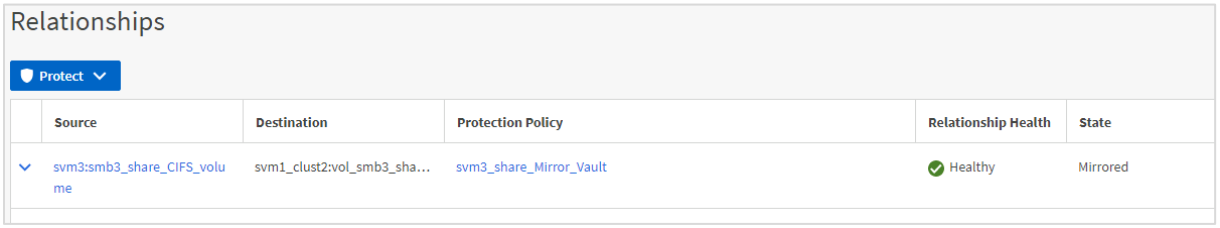
Step	Action
2-13	On the jump host, open **File Explorer**.
2-14	In the ribbon, select **Computer** > **Network** > **Map network drive**. 
2-15	To map a drive to the destination volume on cluster2\svm1_clust2, use the folder path **\\192.168.0.160\vol_smb3_share_CIFS_volume_dest**. 
2-16	Open the folder and note that the folder is empty.

Step	Action
2-17	On the jump host, use File Explorer to map a drive to the source volume on cluster1\svm3. Use the folder path **\\192.168.0.62\smb3_share**. Note that for svm3, an SMB share is set up for the source volume smb3_share_CIFS_volume. 
2-18	Previously, on cluster1, you used one of two IP addresses that are assigned to the svm3 data LIF.
2-19	**Cluster1** In the System Manager navigation pane, select **Network** > **Overview**.

Step	Action
2-20	In the Overview > Network Interfaces pane, verify that you used one of the two IP addresses that are assigned to the svm3 data LIF. 
2-21	Open File Explorer, and then copy **File_240M** from C:\CourseFiles to the mapped drive smb3_share (\\192.168.0.62). 
2-22	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.

Step	Action
2-23	In the Relationships pane, click the three vertical dots to the right of the source volume, and then select **Update** to perform a manual update. 
2-24	In the Update Relationship dialog box, click **Update** without changing any settings. 

Step	Action
2-25	Expand the relationship, and then wait for the Transfer Status to change from Transferring to idle. 
2-26	In File Explorer, open the mapped drive **vol_smb3_share_CIFS_volume_dest (\\192.168.0.160)** and verify that the SnapMirror relationship transferred the file. 
2-27	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.

Step	Action
2-28	In the Relationships pane, monitor the status of SnapMirror data transfers to verify that the transfers occur on the specified schedule: ▪ The Relationship Health must be Healthy. ▪ The State field must be Mirrored. ▪ The Lag Time value must be no greater than the transfer schedule interval. 

End of exercise

Exercise 2: Performing SnapMirror Disaster Recovery

In this exercise, you simulate a disaster on the source volume. You make the destination volume data accessible to clients. You then repair the simulated disaster and return the SnapMirror relationship to its original configuration.

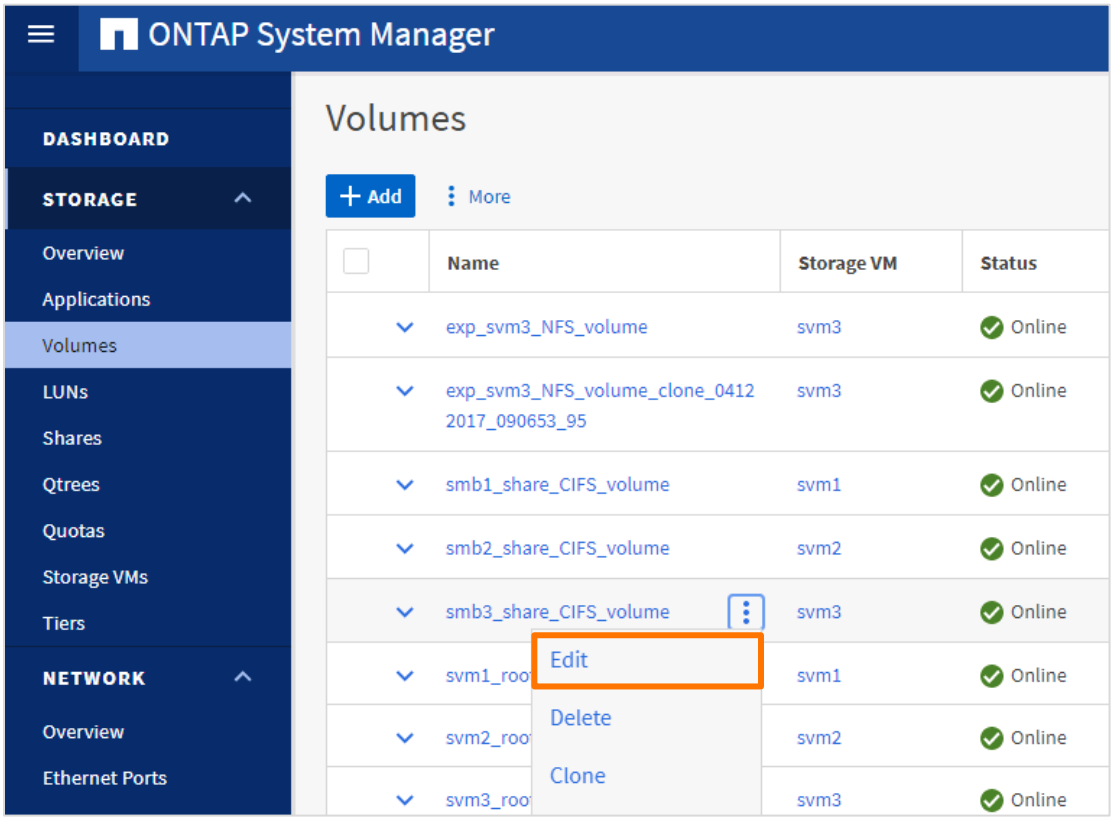
Objectives

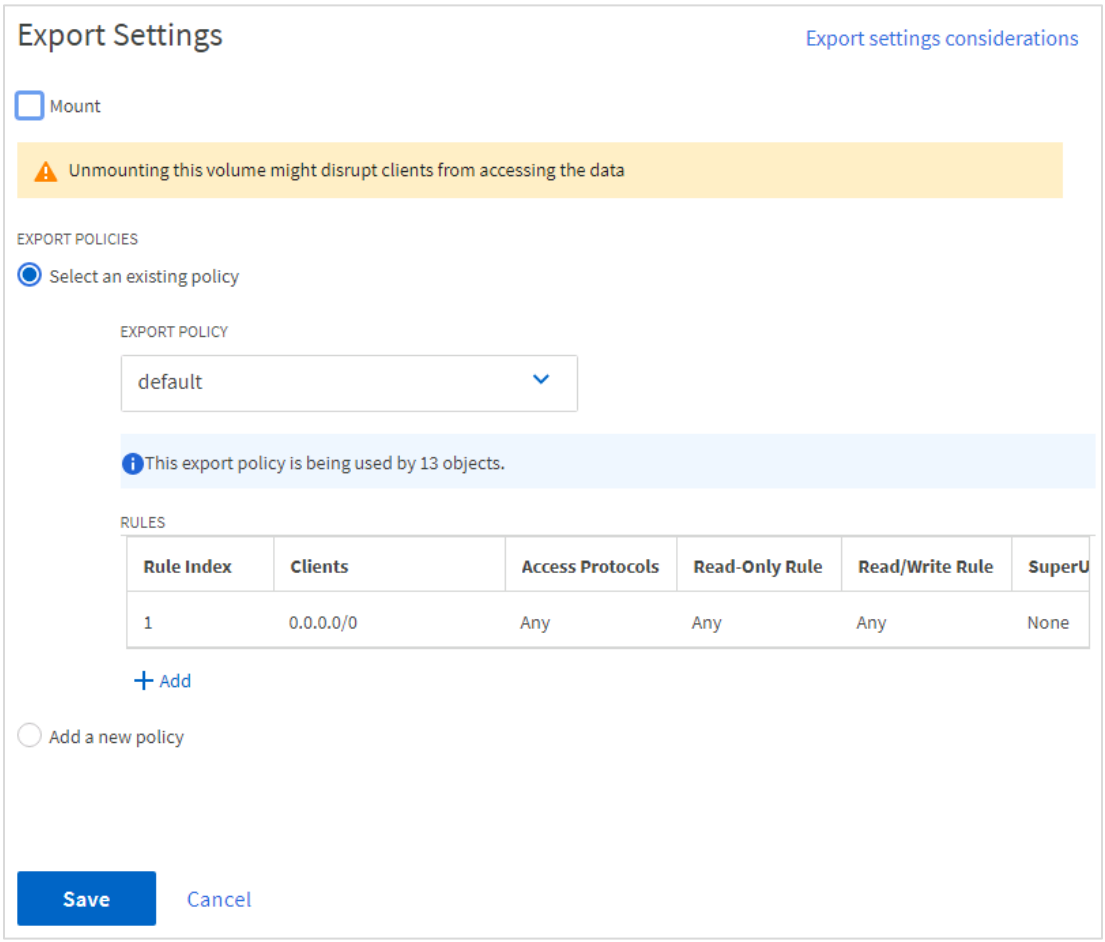
This exercise focuses on enabling you to do the following:

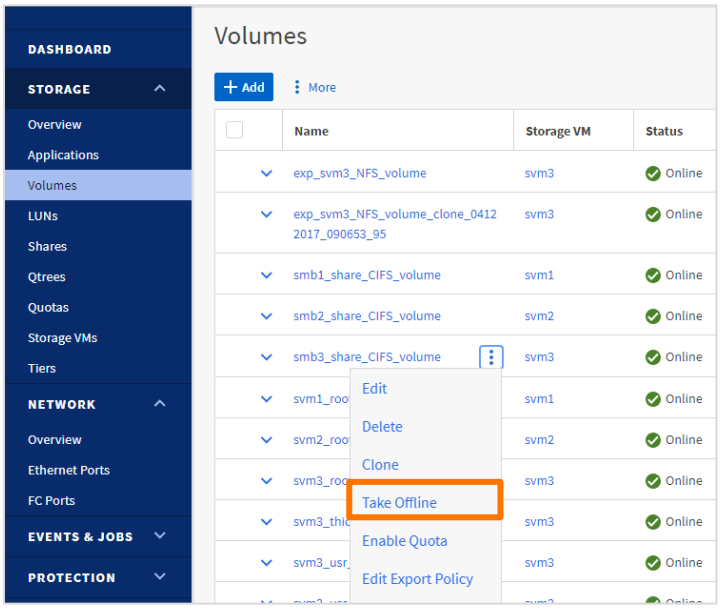
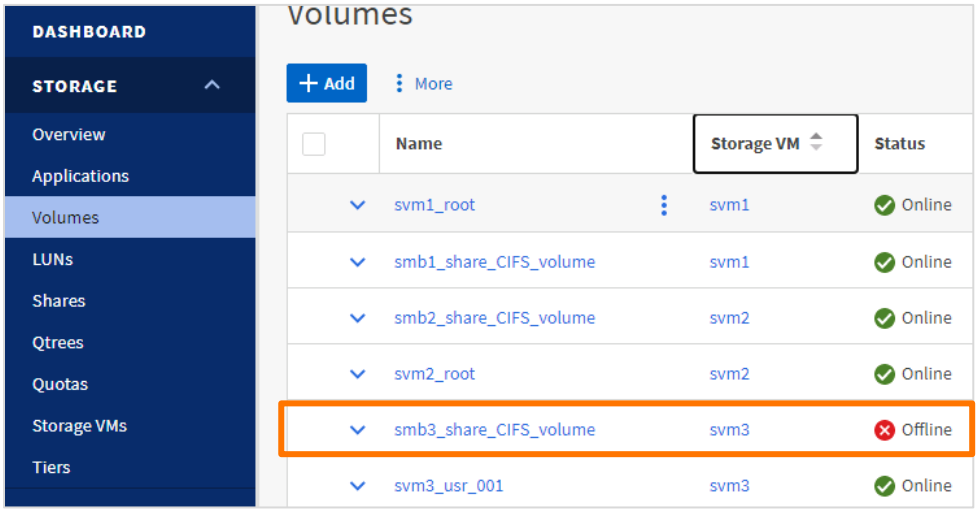
- Take a source volume offline
- Activate a destination volume
- Reactivate the original source volume
- Restore the original SnapMirror relationship

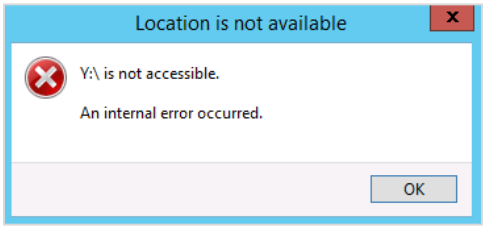
Task 1: Take the Source Volume Offline

In this task, you take the source volume on cluster1 offline. Before you can take a shared volume offline, you must remove the volume from the namespace.

Step	Action
1-1	**Cluster1** In the System Manager navigation pane, select **Storage** > **Volumes**.
1-2	In the Volumes pane, click the three vertical dots to the right of smb3_share_CIFS_volume, and then select Edit. 

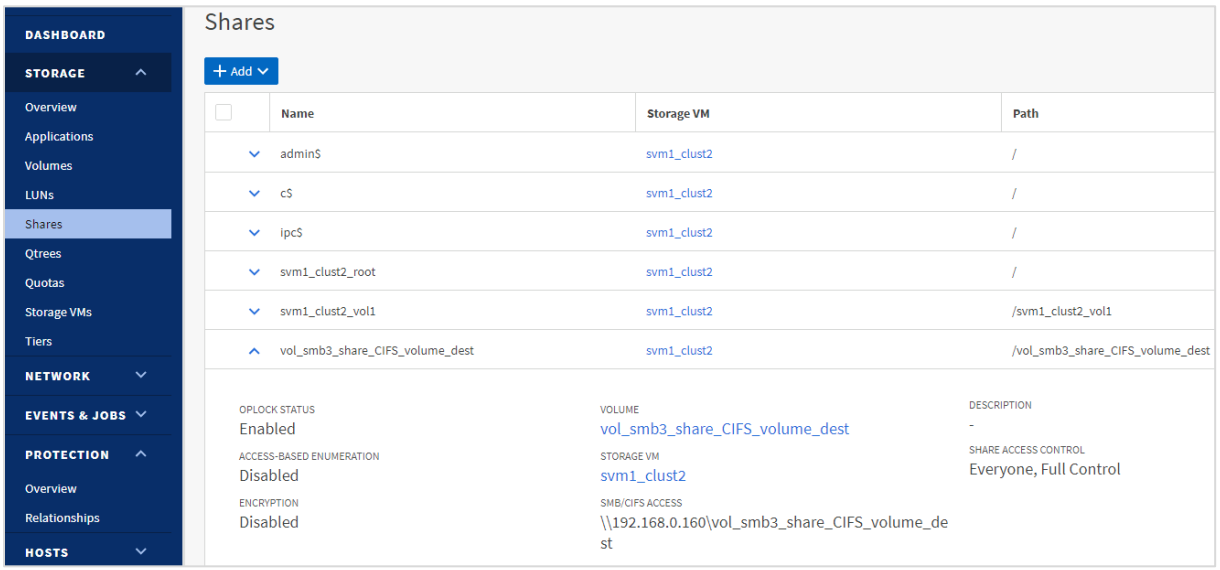
Step	Action
1-3	In the Edit Volume pane, scroll down to the Export Settings section, and then clear the **Mount** checkbox. 
1-4	Click **Save**.
1-5	To unmount the source volume from the CLI, enter the following command: `volume unmount -vserver svm3 -volume smb3_share_CIFS_volume`

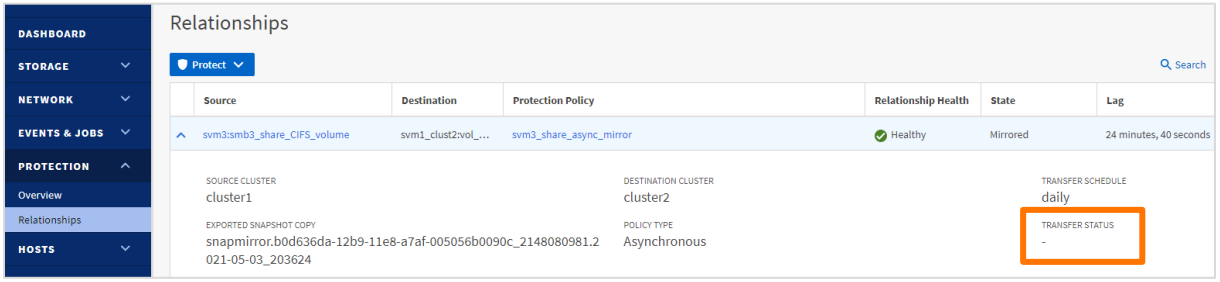
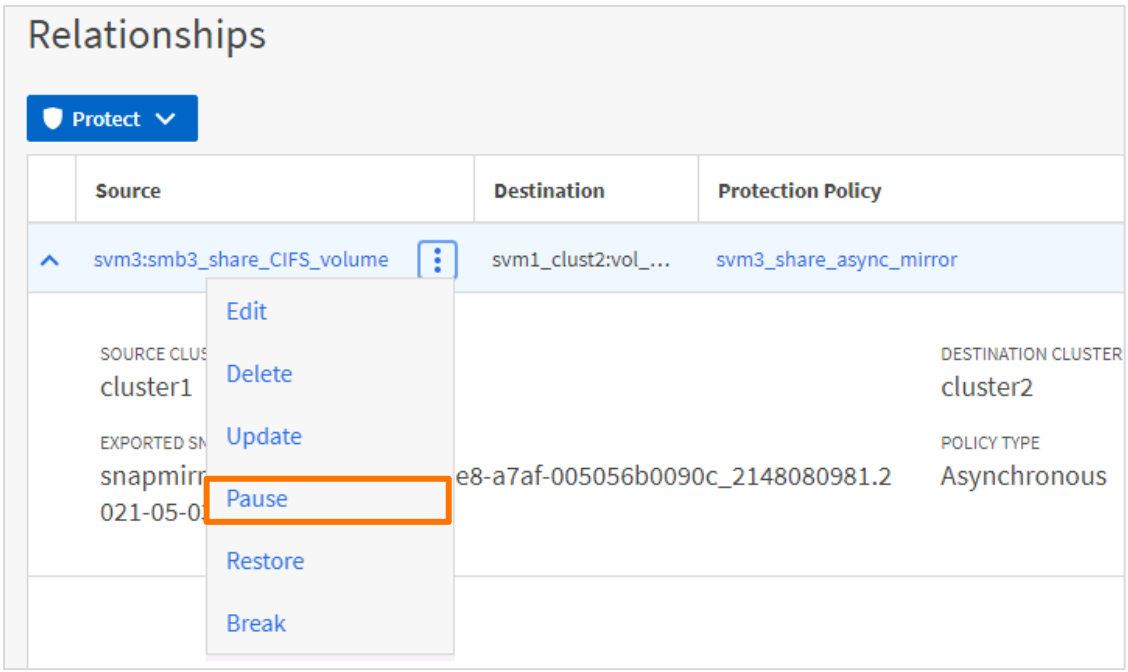
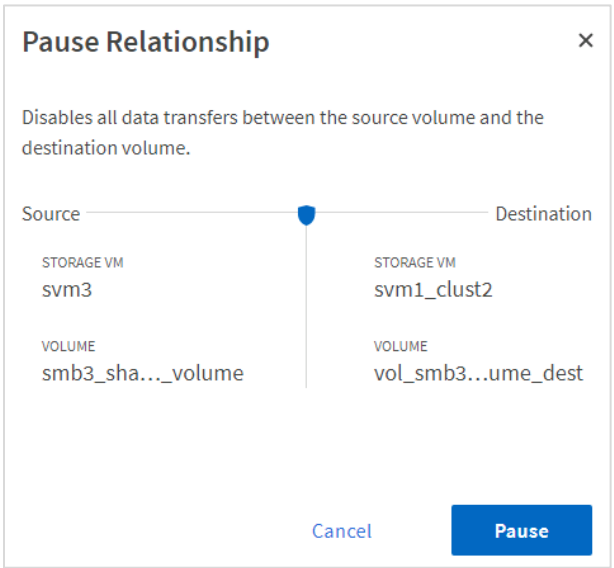
Step	Action
1-6	In the Volumes pane, click the three vertical dots to the right of smb3_share_CIFS_volume, and then select **Take Offline**. 
1-7	Verify that the status of the volume is Offline, as signified by the red status icon. 
1-8	To take the source volume offline from the CLI, enter the following command: **volume offline -vserver svm3 -volume smb3_share_CIFS_volume**
1-9	On your Windows desktop, try to access the mapped drive smb3_share (\\192.168.0.62).

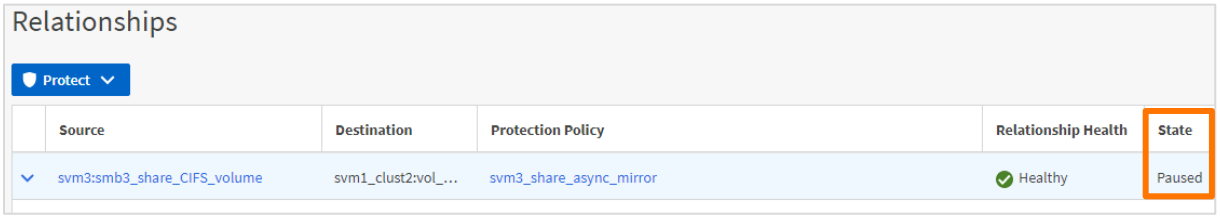
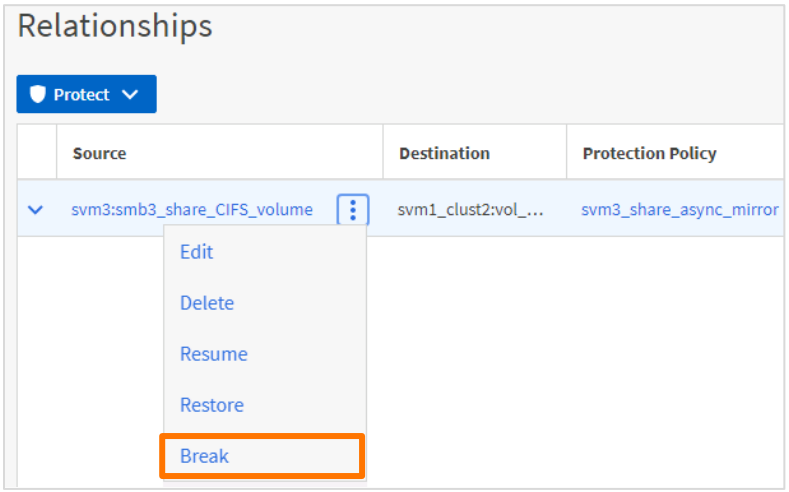
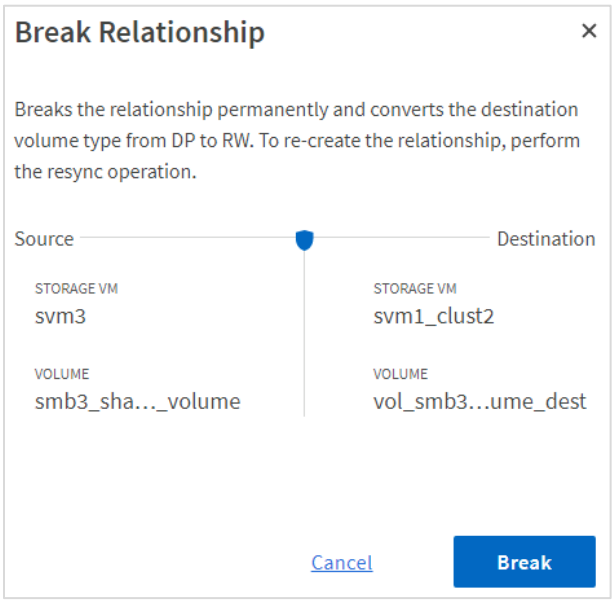
Step	Action
1-10	After some time, Windows should display an error message that the drive is unavailable. Example: 

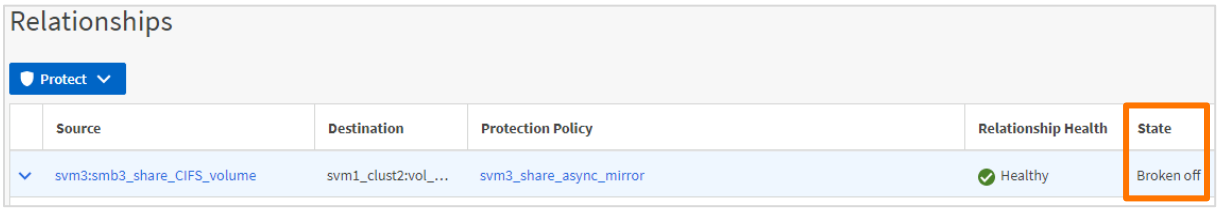
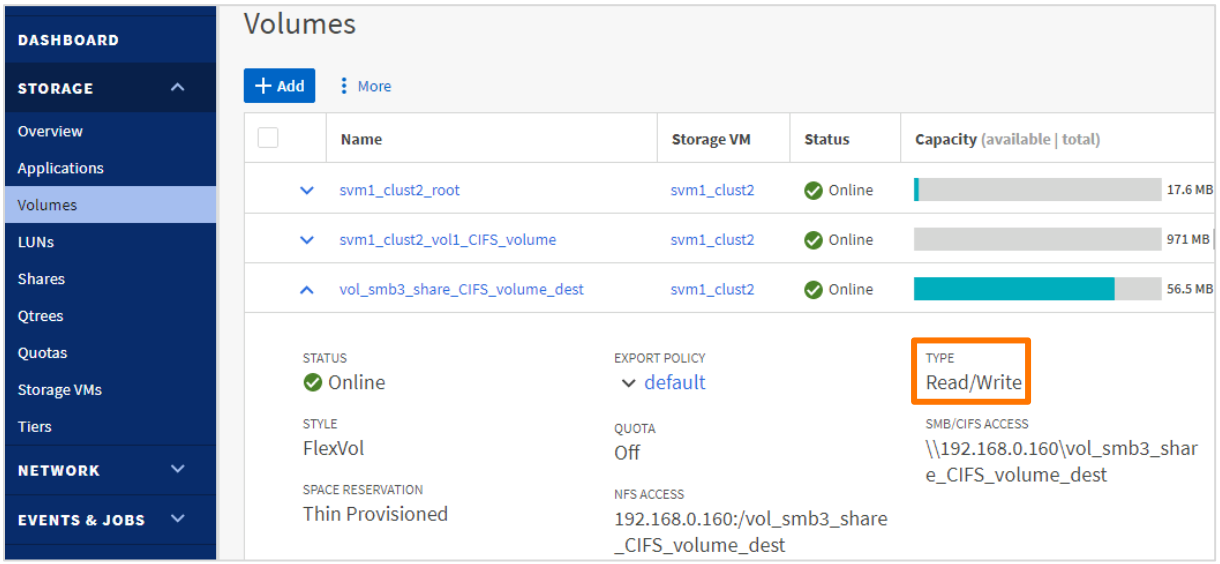
Task 2: Activate the Destination Volume

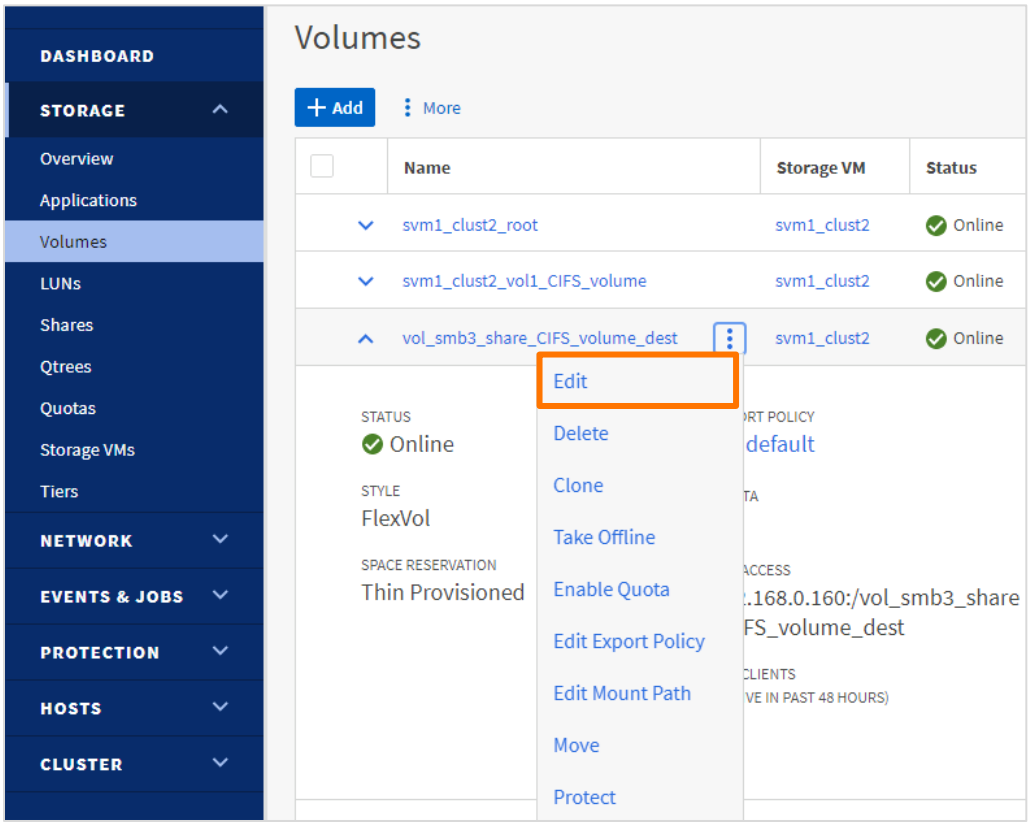
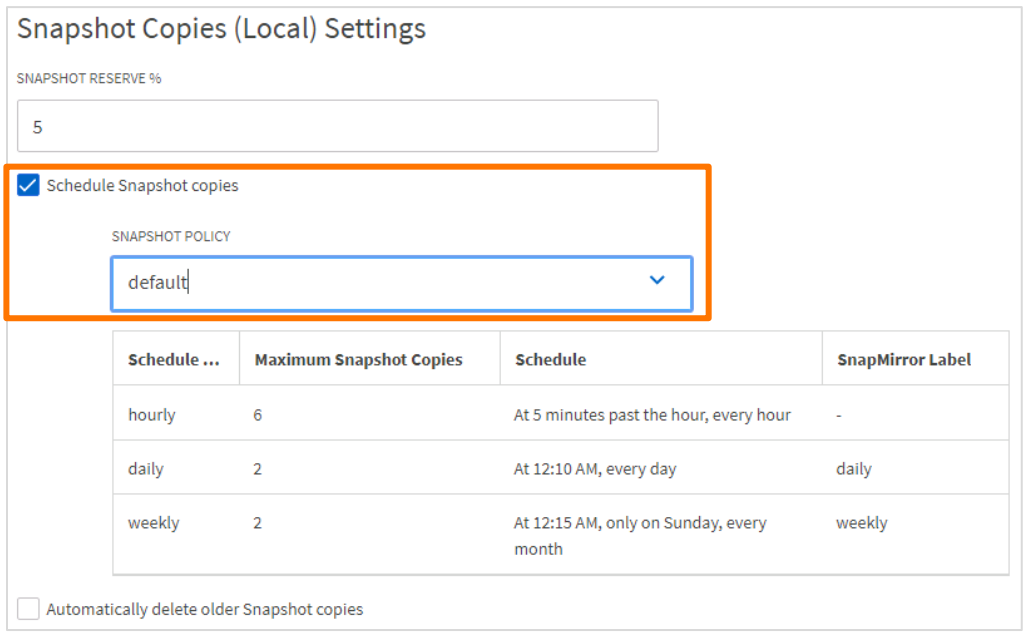
In the previous task, you took the source volume offline and rendered the shared data unavailable. In this task, you activate the destination volume and use a best practices workflow to configure the volume for data access.

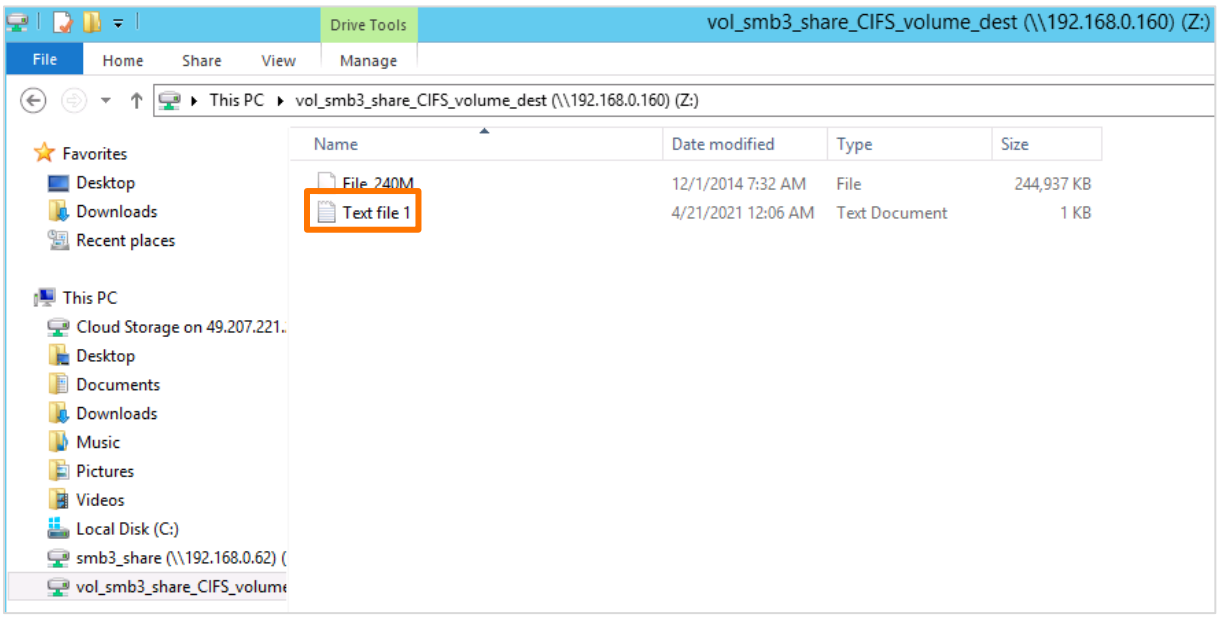
Step	Action
2-1	The first steps of the volume disaster workflow include verifying the source volume status, quiescing and breaking the SnapMirror relationship, and verifying the destination volume status.
2-2	You must always break the SnapMirror relationship from the destination volume. On the destination storage VM (storage virtual machine, also known as SVM), check the status of the SnapMirror relationship to determine whether a transfer is in progress. The SnapMirror relationship must be in an idle state before you can break the relationship.
2-3	**Cluster2** In the System Manager navigation pane, select **Storage** > **Shares**.
2-4	Expand the destination volume **vol_smb3_share_CIFS_volume_dest** and verify that it is mounted on the destination SVM namespace. 
2-5	In the navigation pane, select **Protection** > **Relationships**.

Step	Action
2-6	Expand the relationship and verify that the Transfer Status is idle. 
2-7	To disable future data transfers, click the three vertical dots to the right of the source volume, and then select **Pause**. 
2-8	In the Pause Relationship dialog box, click **Pause**. 

Step	Action
2-9	You must ensure that the transfer status of the SnapMirror relationship is paused before you break the SnapMirror relationship. If a transfer is in progress, the quiesce operation might take some time.
2-10	In the Relationships pane, verify that the relationship state is **Paused**. 
2-11	Click the three vertical dots to the right of the source volume, and then select **Break**. 
2-12	In the Break Relationship dialog box, click **Break**. 

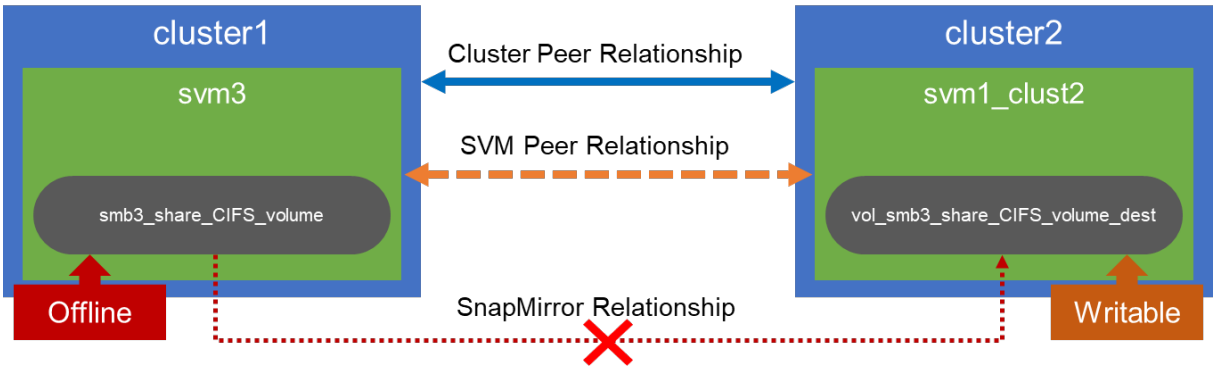
Step	Action
2-13	Verify that the relationship state is Broken Off. 
2-14	During typical SnapMirror operations, the secondary volume is a data-protection volume of the read-only type. In the next step, you look at the volume type of the secondary volume to determine whether it is still read-only or has changed to read/write.
2-15	In the System Manager navigation pane, select **Storage** > **Volumes**.
2-16	Expand the volume **vol_smb3_share_CIFS_volume_dest** and verify that the value in the Type field is Read Write. 
2-17	The SnapMirror relationship is now broken. The SnapMirror primary volume is offline and unavailable to read and write requests from clients. The SnapMirror secondary volume is now writable.

Step	Action
2-18	In the Volumes pane, click the three vertical dots to the right of the volume vol_smb3_share_CIFS_volume_dest, and then select **Edit**. 
2-19	In the Edit Volume pane, scroll down to the Snapshot Copies(Local) Settings section, and then specify the following values: ▪ Schedule Snapshot copies checkbox: *selected* ▪ Snapshot Policy: **default** 

Step	Action
2-20	Scroll down, and then click **Save**.
2-21	On your Windows desktop, open the mapped drive **vol_smb3_share_CIFS_volume_dest (\\192.168.0.160)**.
2-22	Create a text document in the folder to verify that you can write to the volume. 

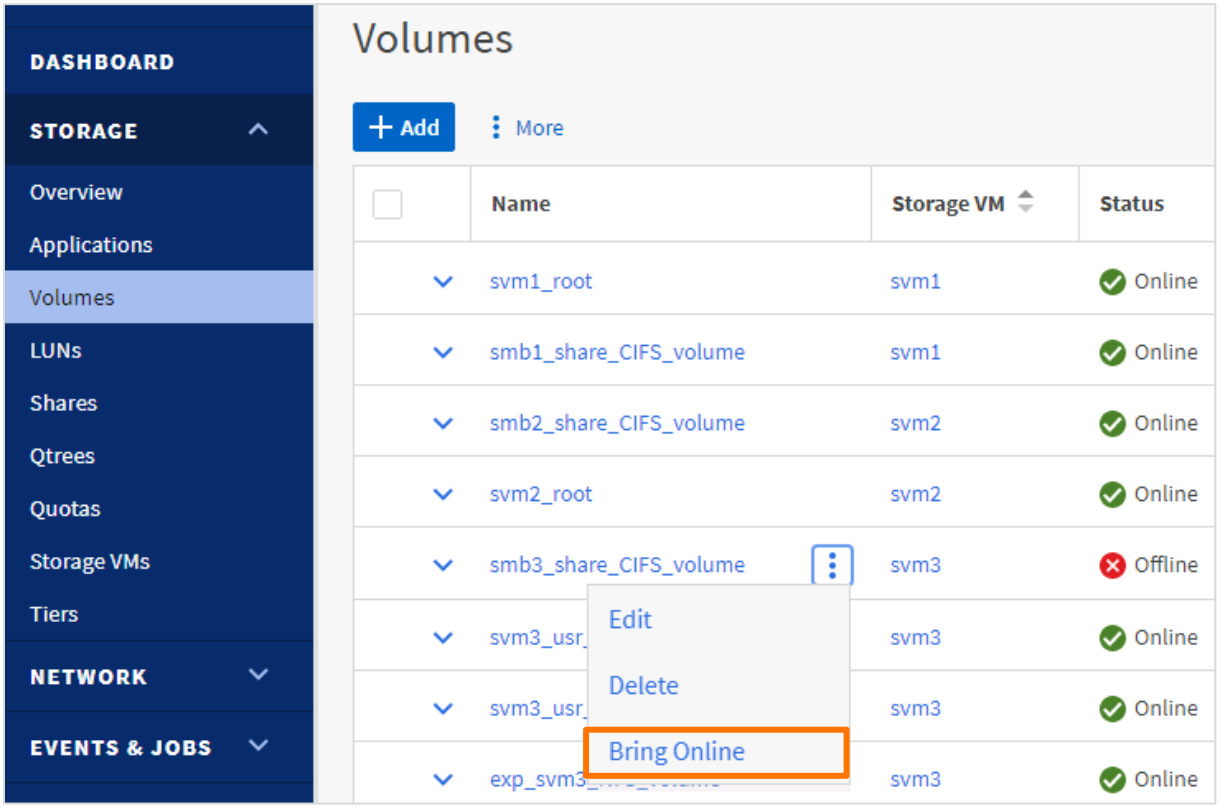
Task 3: Review the Exercise Environment

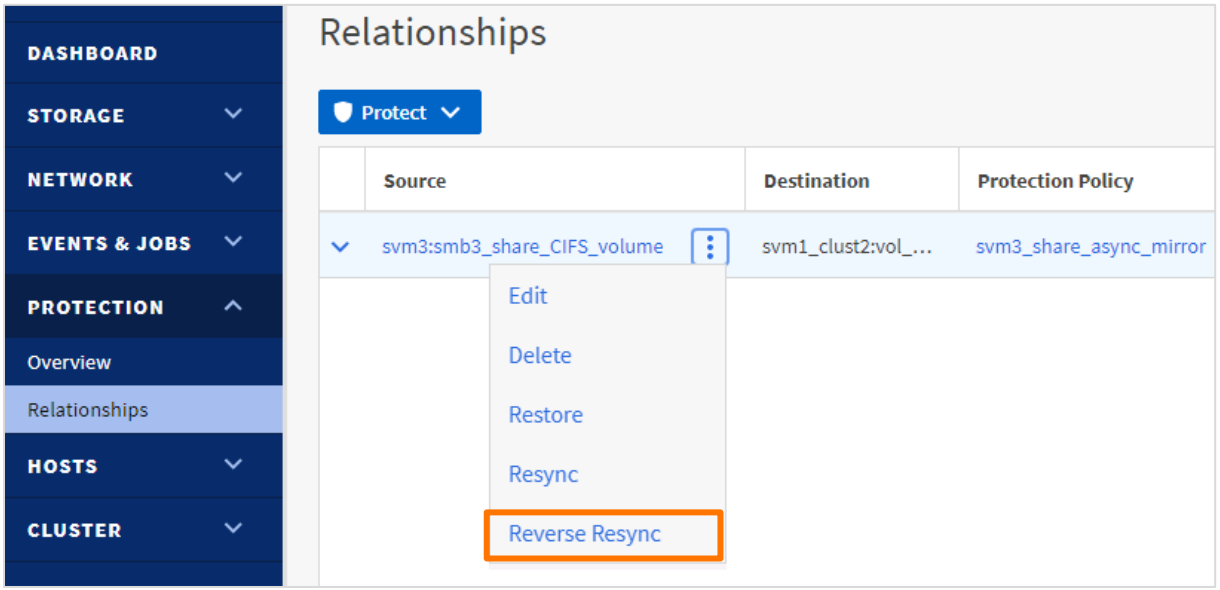
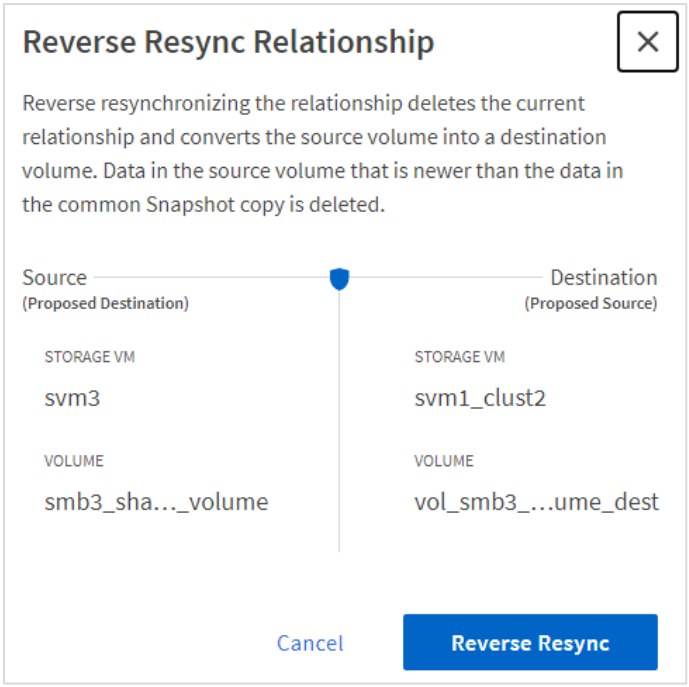
In this task, you review the exercise environment that you created in the previous tasks.

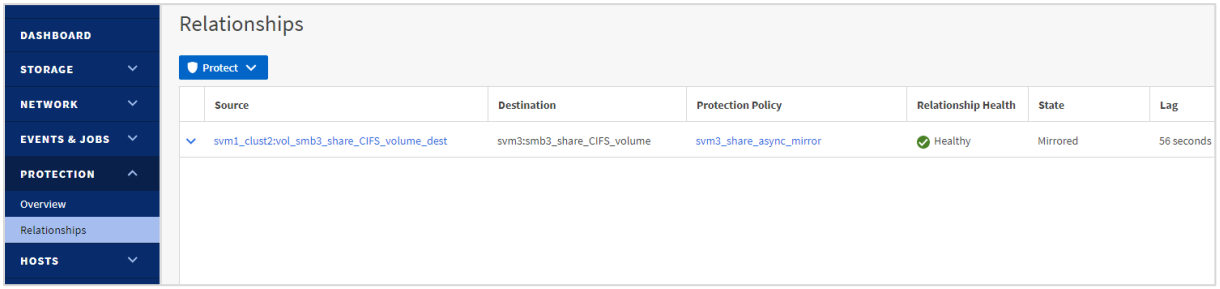
Step	Action
3-1	Verify that the SnapMirror relationship is broken and that the destination volume is in a read/write state. 

Task 4: Reactivate the Original Source Volume

In this task, you bring the primary volume back online. Before normal operations can be restored, you must run a SnapMirror reverse resynchronization to update the primary volume with data that was written to the secondary volume.

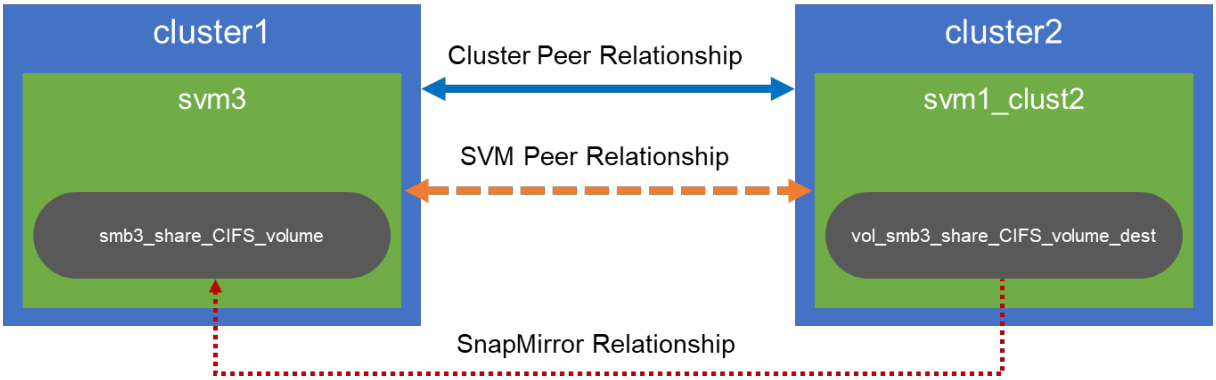
Step	Action
4-1	When the source volume becomes available, you must resynchronize the data from the destination volume to the source volume, update any modifications after the resynchronization, and then activate the source volume. First, you bring the original source volume online.
4-2	**Cluster1** In the System Manager navigation pane, select **Storage** > **Volumes**.
4-3	Click the three vertical dots to the right of smb3_share_CIFS_volume, and then select **Bring Online**. 
4-4	Verify that smb3_share_CIFS_volume is online.
4-5	The primary volume is online. In the next step, on cluster2, you check the SnapMirror status.
4-6	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.

Step	Action
4-7	The status of the SnapMirror relationship is Broken Off. The primary volume is online. However, data is written to the secondary volume. In the next step, you reverse the direction of the SnapMirror relationship to copy data that was written to the secondary volume back to the primary volume. You can run the Reverse Resync operation only from the SnapMirror destination SVM.
4-8	In the Relationships pane, click the three vertical dots to the right of the source volume, and then select **Reverse Resync**. 
4-9	In the Reverse Resync Relationship dialog box, review the provided information, and then click **Reverse Resync**. 
4-10	Note that the SnapMirror relationship is removed from the relationships list on cluster2.

Step	Action
4-11	**Cluster1** In the System Manager navigation pane, select **Protection** > **Relationships**, and then find the reversed relationship that is listed on the page. 
4-12	In the Volume Relationships pane on cluster1, the original source is now the destination, and the original destination is now the source.

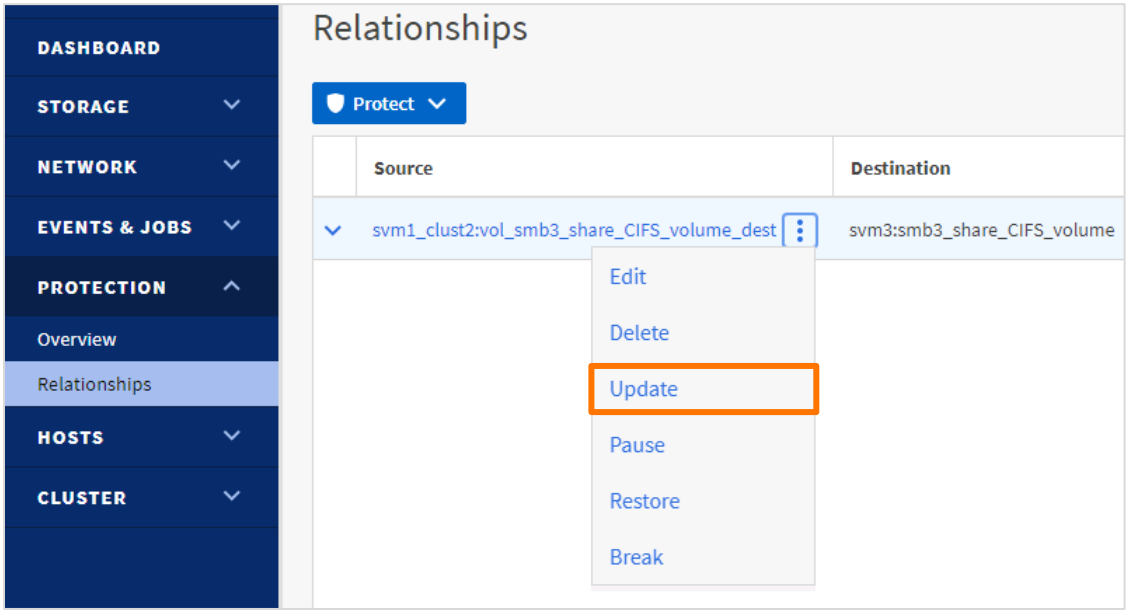
Task 5: Review the Exercise Environment

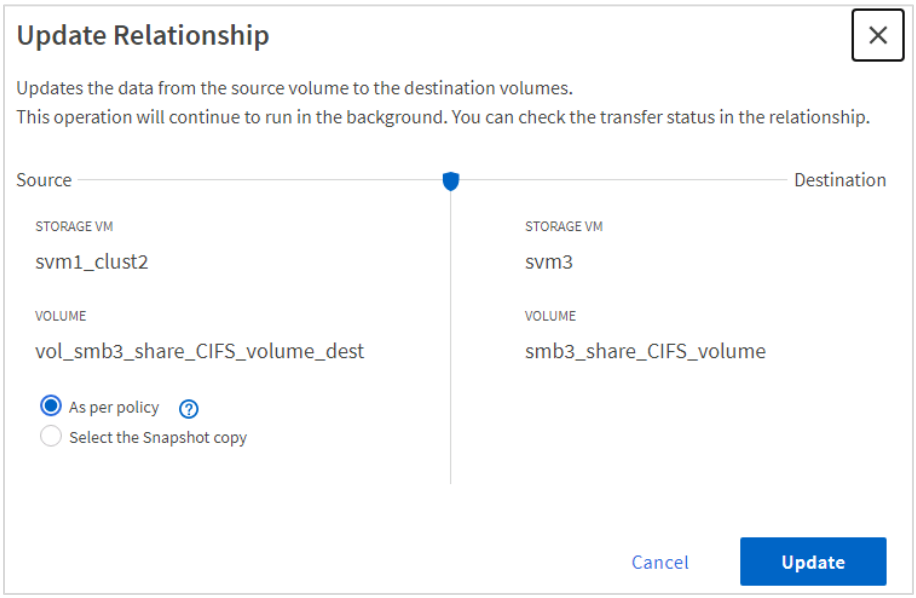
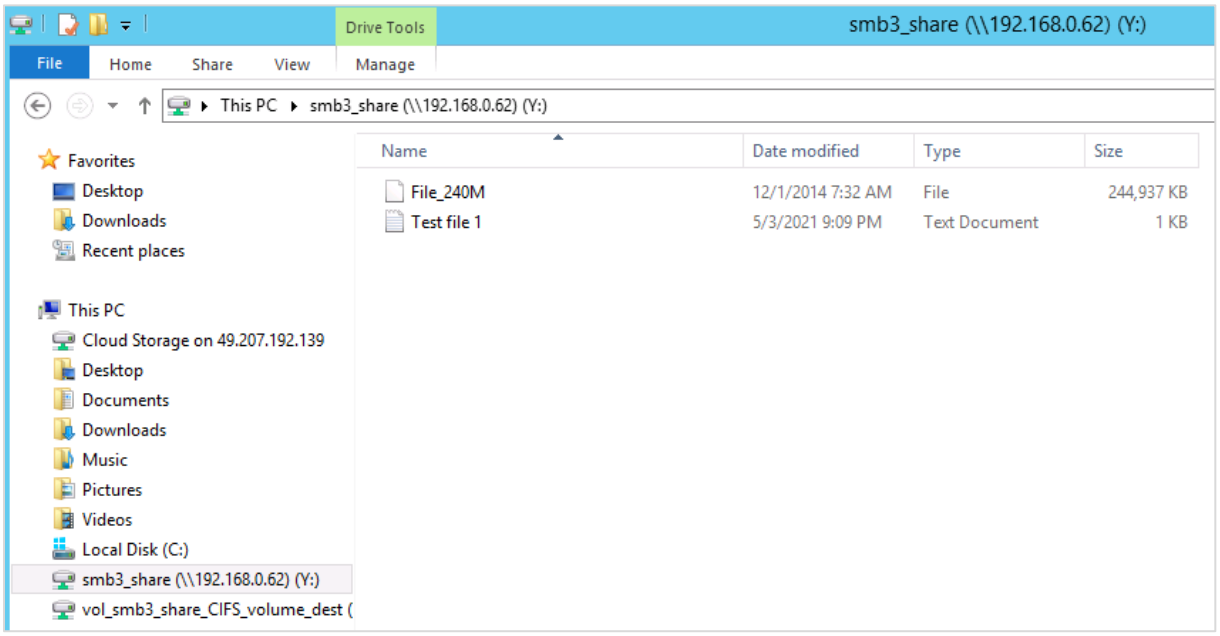
In this task, you review the exercise environment that you created in Task 4.

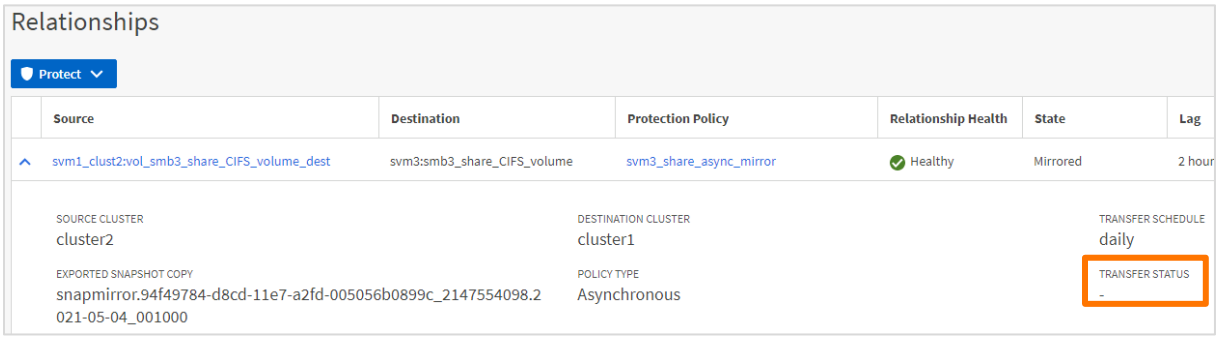
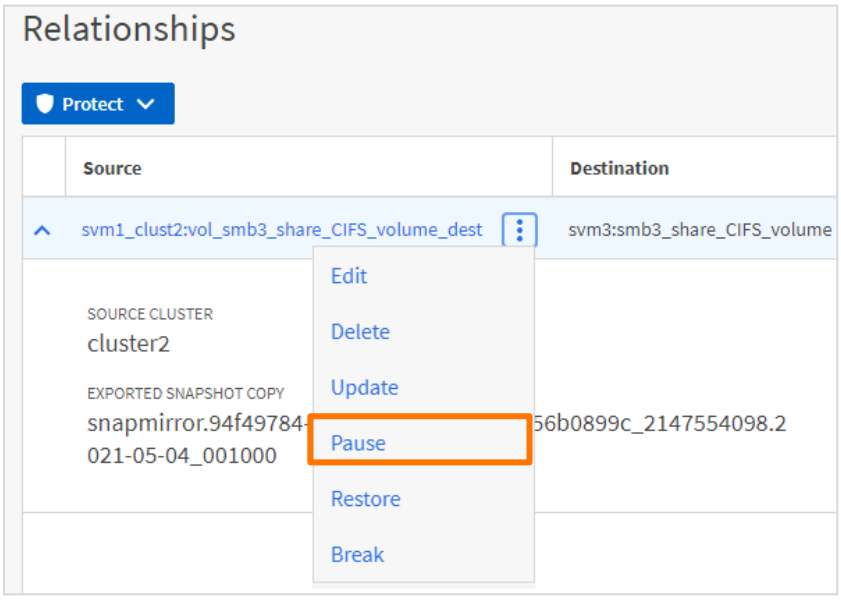
Step	Action
5-1	Verify that the original source volume is now configured as the SnapMirror destination and that the original destination is now the SnapMirror source volume. If the relationship stays in this configuration for a long time, you might need to reset the mirror policy and update schedule until you return the SnapMirror relationship to its original configuration. 

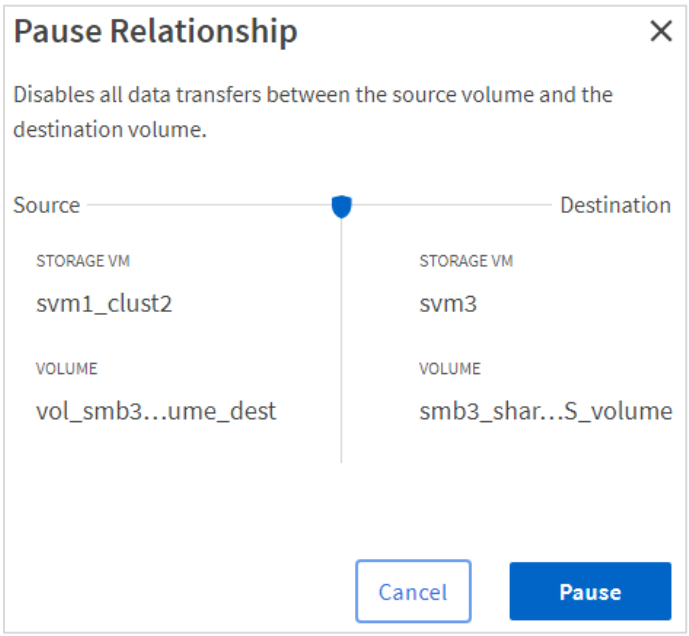
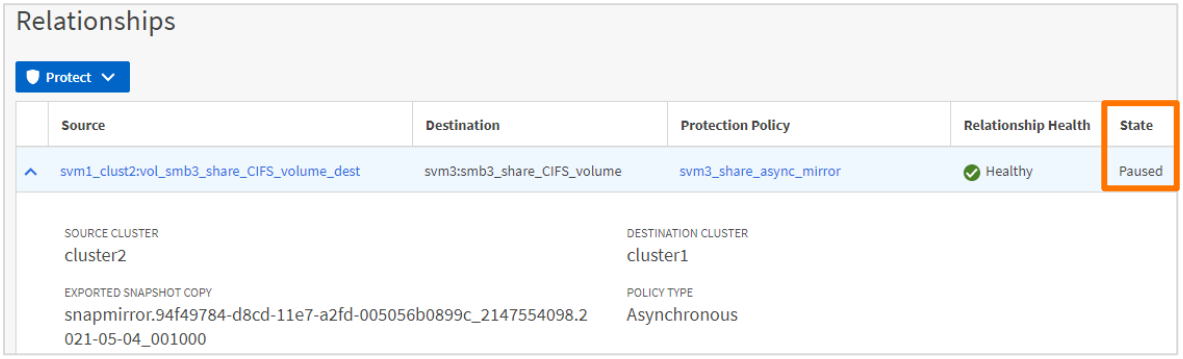
Task 6: Restore the Original SnapMirror Relationship

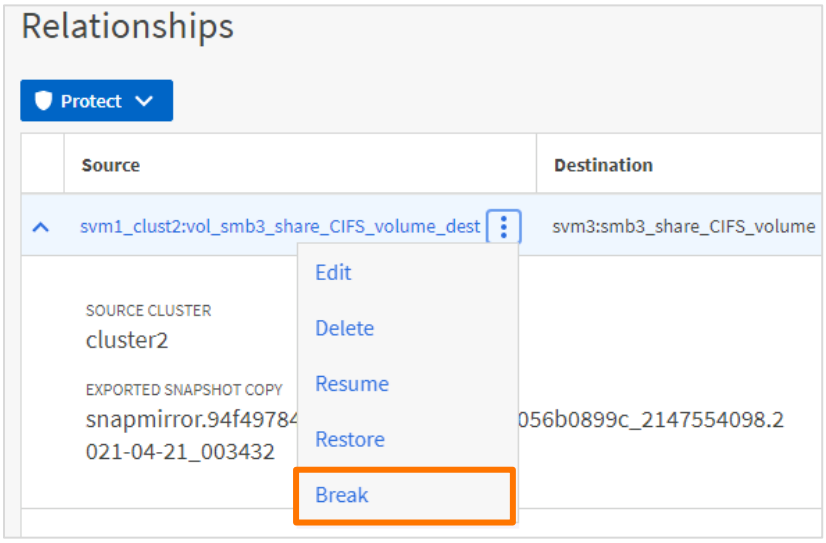
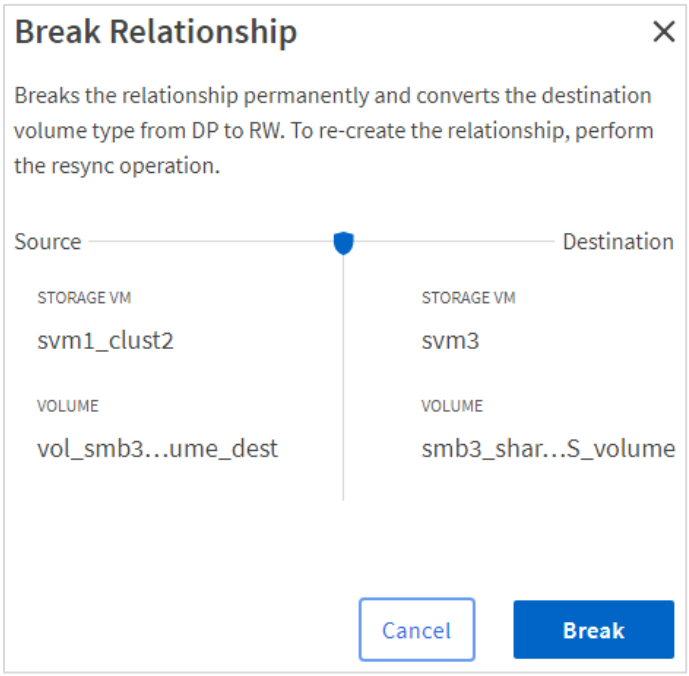
The data that was written to the SnapMirror secondary volume has been updated to the primary volume. In this task, you restore the original relationship between the two SnapMirror volumes.

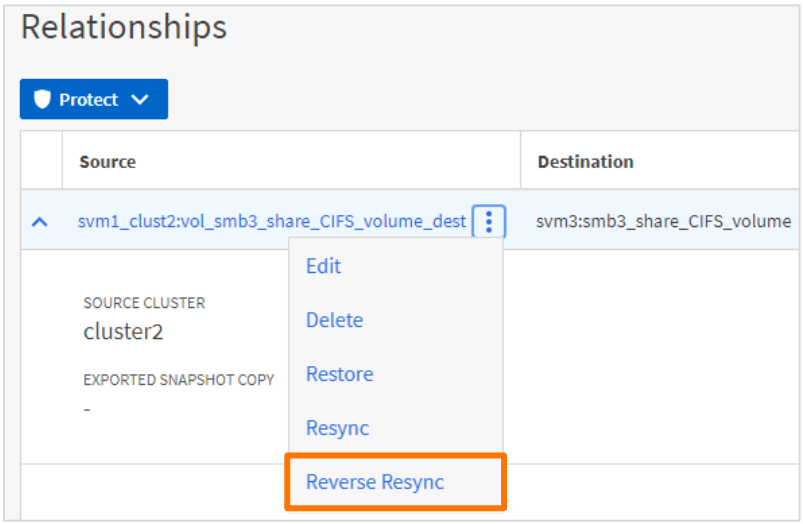
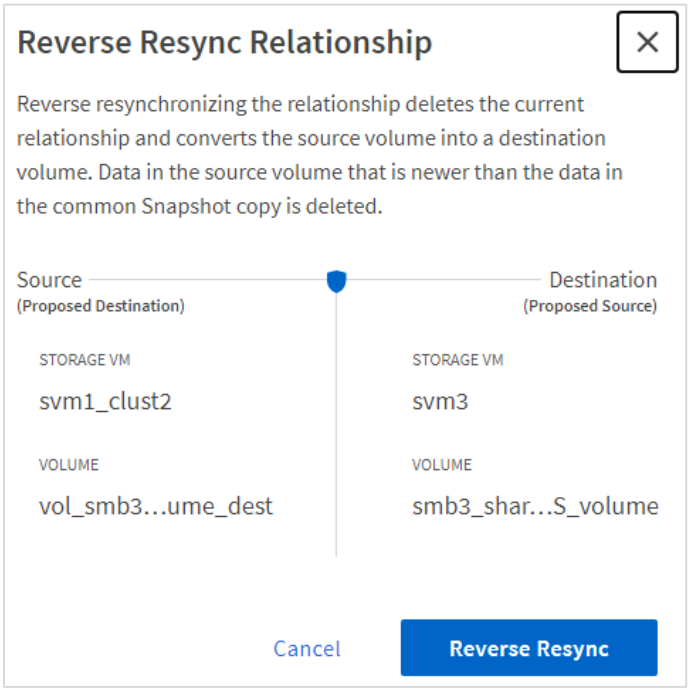
Step	Action
6-1	You start to restore the original relationship by updating the reversed SnapMirror relationship, because clients might have written to the SnapMirror reversed secondary volume. After you update the reversed relationship, you break the relationship. You must verify that the transfer status is idle before you break the reversed mirroring relationship.
6-2	**Cluster1** In the System Manager navigation pane, select **Protection** > **Relationships**.
6-3	In the Relationships pane, click the three vertical dots to the right of the source volume, and then select **Update**. 

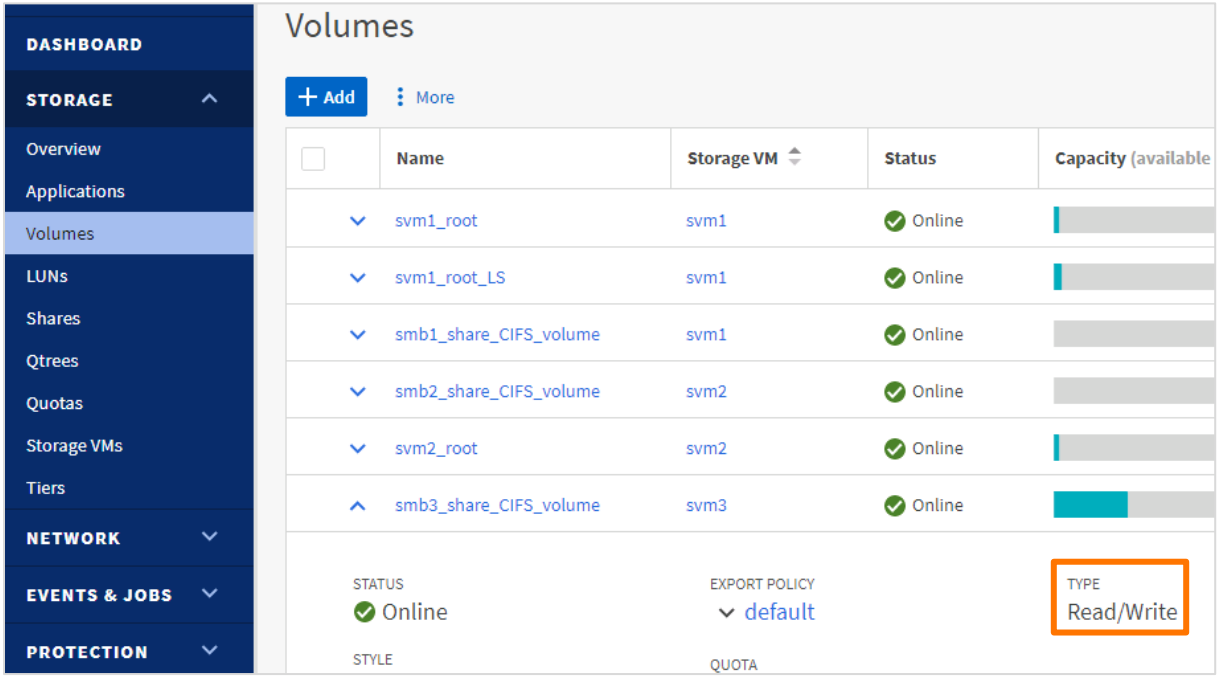
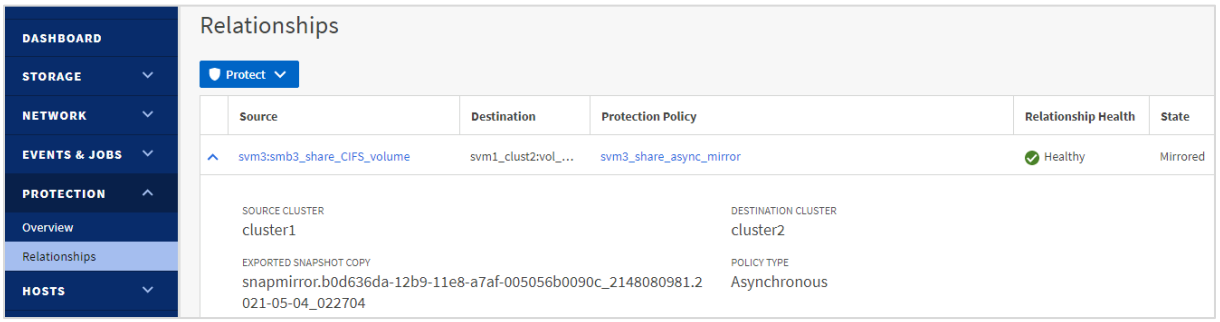
Step	Action
6-4	In the Update Relationship dialog box, accept the default configuration setting, and then click **Update**. 
6-5	The update operation is necessary to write any new data that was written to the reversed secondary volume to the primary volume after the reverse resync operation. The on-demand configuration setting transfers data according to the newest shared Snapshot copy on the source and destination volumes.
6-6	On your Windows desktop, access the mapped drive smb3_share (\\192.168.0.62), and then verify that the new file you created on the destination is now available on the source. 
6-7	After you update the reversed relationship, you pause and break the relationship. You must verify that the transfer status is idle before you break the reversed mirroring relationship.

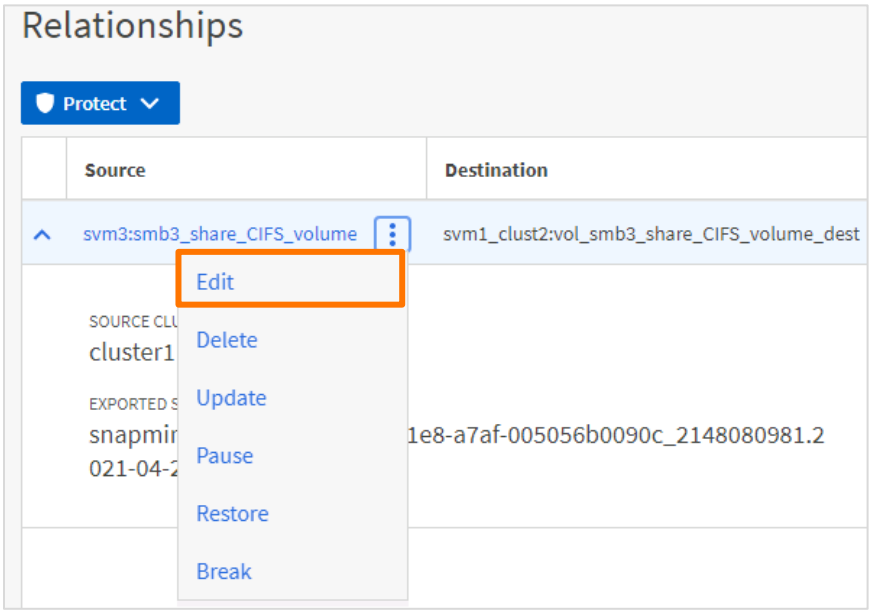
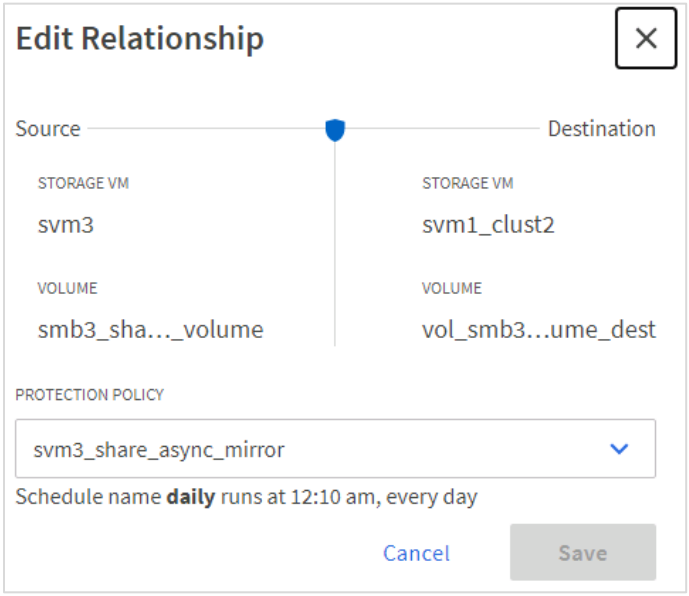
Step	Action
6-8	Verify that the Transfer Status of the relationship is idle. If the Transfer Status is Transferring, then wait until it becomes idle. 
6-9	On the Relationships pane, click the three vertical dots to the right of the source volume, and then select **Pause**. 

Step	Action
6-10	In the Pause Relationship dialog box, review the provided information, and then click **Pause**. 
6-11	Verify that the relationship state is Paused. 

Step	Action
6-12	On the Relationships pane, click the three vertical dots to the right of the source volume, and then select **Break**. 
6-13	In the Break Relationship dialog box, review the provided information, and then click **Break**. 
6-14	Verify that the relationship state is Broken Off.
6-15	In the next step, you re-establish the original SnapMirror relationship by using the reverse resync operation.

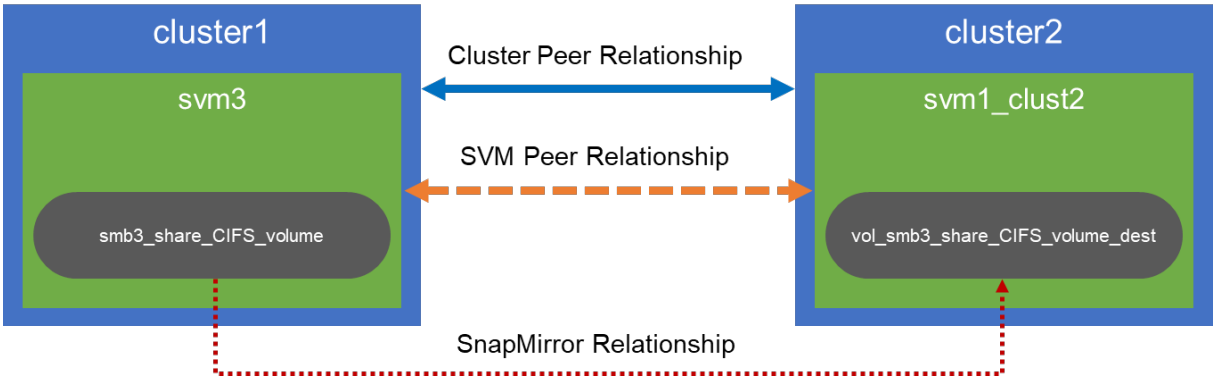
Step	Action
6-16	In the Relationships pane, click the three vertical dots to the right of the source volume, and then select **Reverse Resync**. 
6-17	In the Reverse Resync Relationship dialog box, review the provided information, and then click **Reverse Resync**. 
6-18	The SnapMirror relationship is removed from the relationships list.
6-19	In the System Manager navigation pane, select **Storage** > **Volumes**.

Step	Action
6-20	Expand the source volume **smb3_share_CIFS_volume**, and then verify that the value in the Type field is Read Write. 
6-21	SnapMirror technology is always managed from the SnapMirror destination. Now that the SnapMirror relationship is reversed, you must log in to cluster2 to verify and manage the SnapMirror relationship. You also verify that the SnapMirror policy and update schedule are retained.
6-22	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.
6-23	In the Relationships pane, verify that the original SnapMirror relationship is restored and healthy and that the relationship state is Mirrored. 

Step	Action
6-24	To verify that the original SnapMirror policy and schedule are retained, click the three vertical dots to the right of the source volume, and then select **Edit**. 
6-25	In the Edit Relationship dialog box, verify that the original policy and schedule are retained, and then click **Cancel**. 
6-26	To manually update the SnapMirror relationship, you can click the three vertical dots to the right of the source volume and then select Update.

Task 7: Review the Exercise Environment

In this task, you review the exercise environment that you created in Task 6.

Step	Action
7-1	Verify that you successfully returned the SnapMirror relationship to its original configuration. 

End of exercise

Exercise 3: Configuring SnapMirror Unified Replication for Vaulting

In this exercise, you configure and initialize a unified replication relationship between two volumes. This relationship meets the following requirements:

- Daily scheduled backups with a retention policy of seven Snapshot copies
- Weekly scheduled backups with a retention policy of 52 Snapshot copies

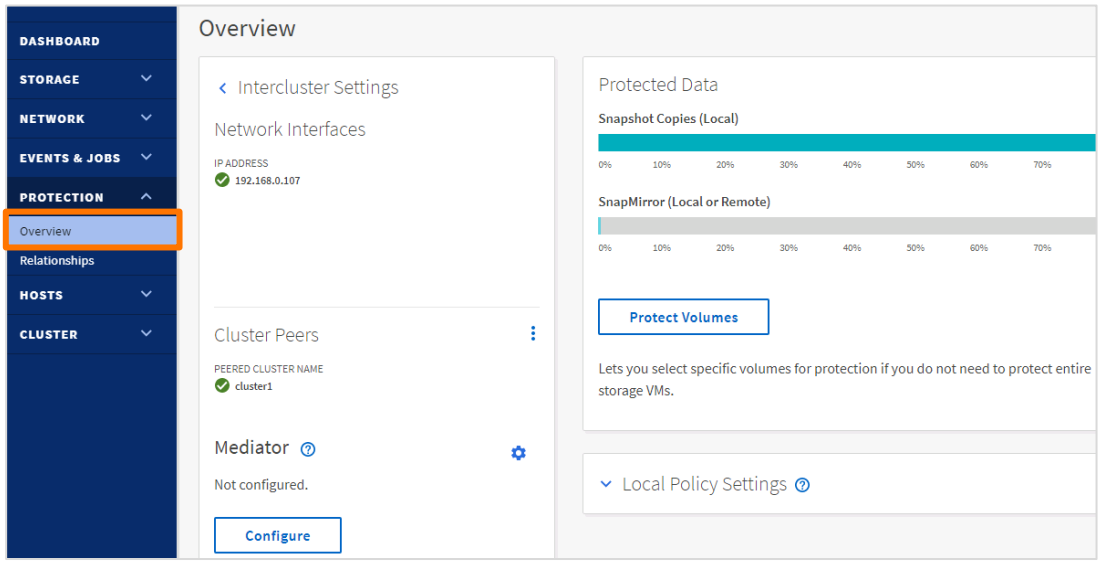
Objectives

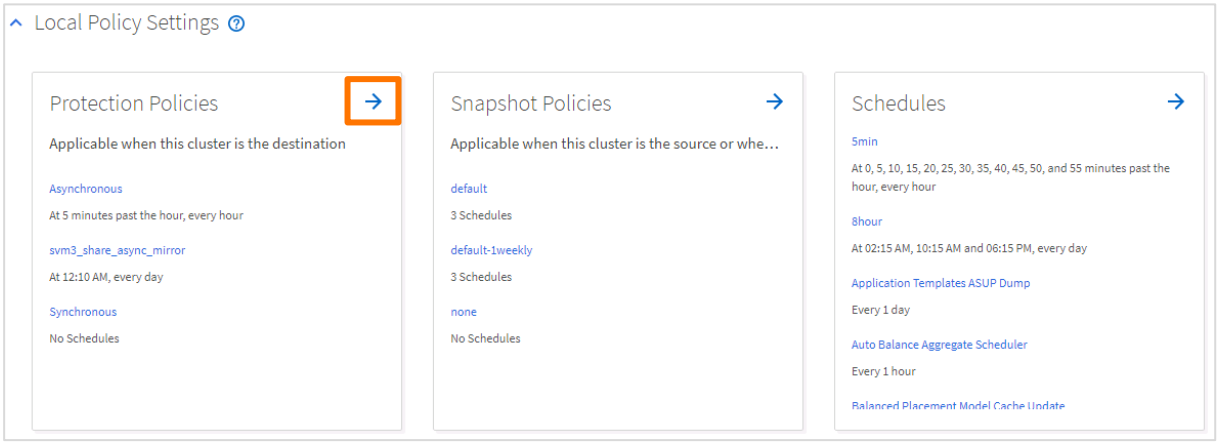
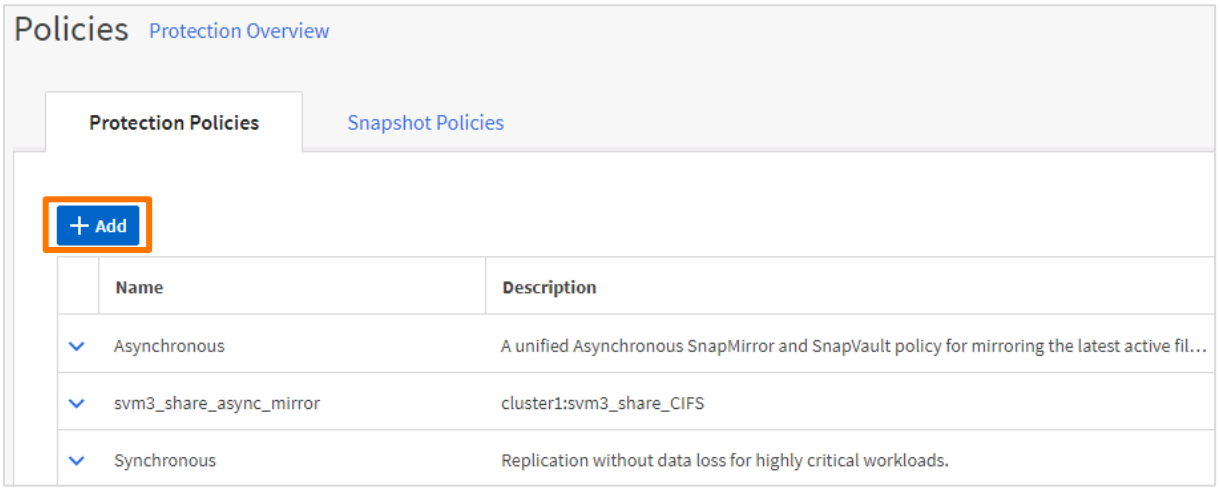
This exercise focuses on enabling you to do the following:

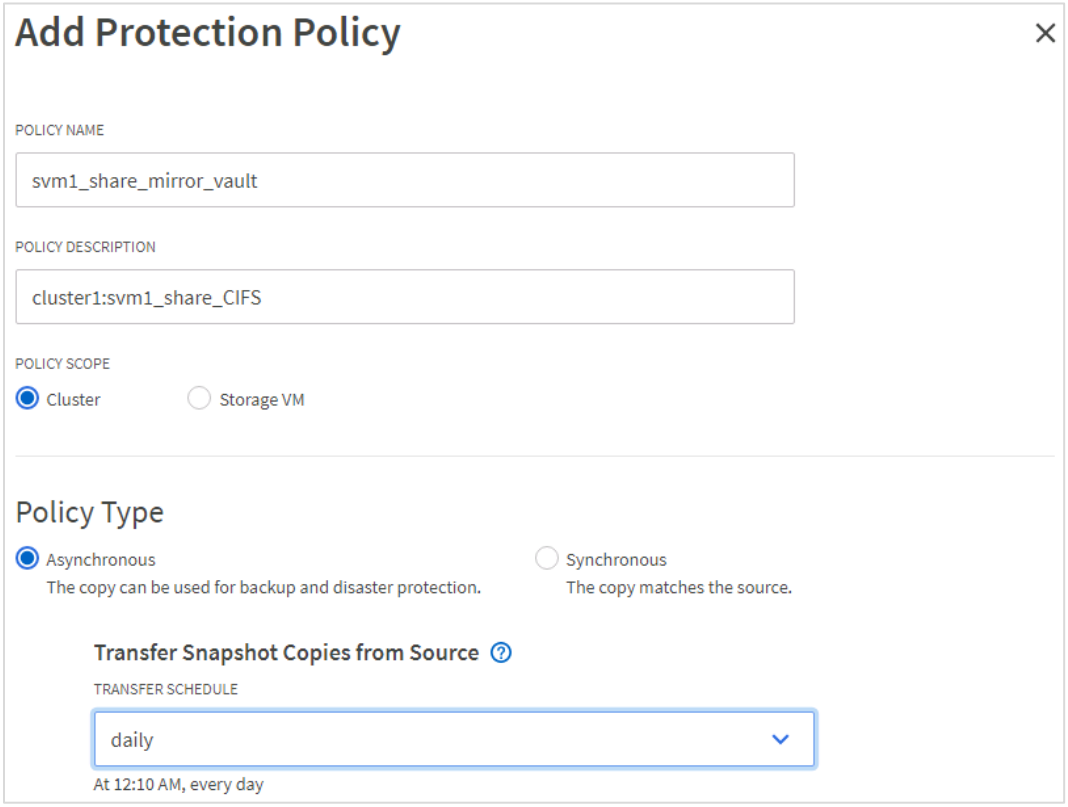
- Create a custom protection policy
- Create a SnapMirror unified replication relationship
- Perform a manual SnapMirror update
- Verify data transfer

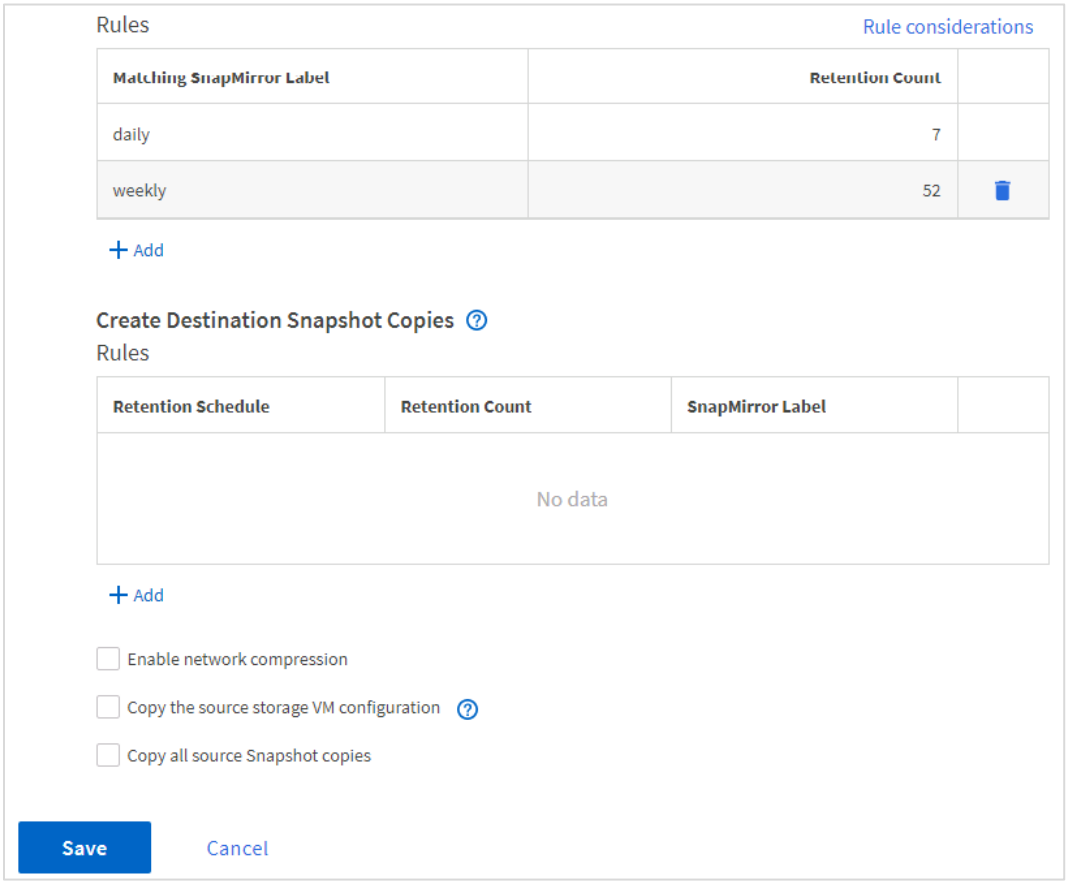
Task 1: Create a Custom Protection Policy and a SnapMirror Relationship

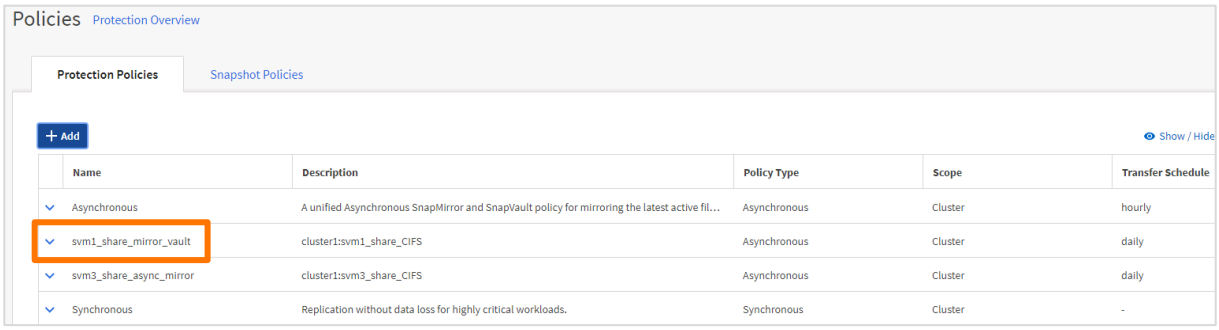
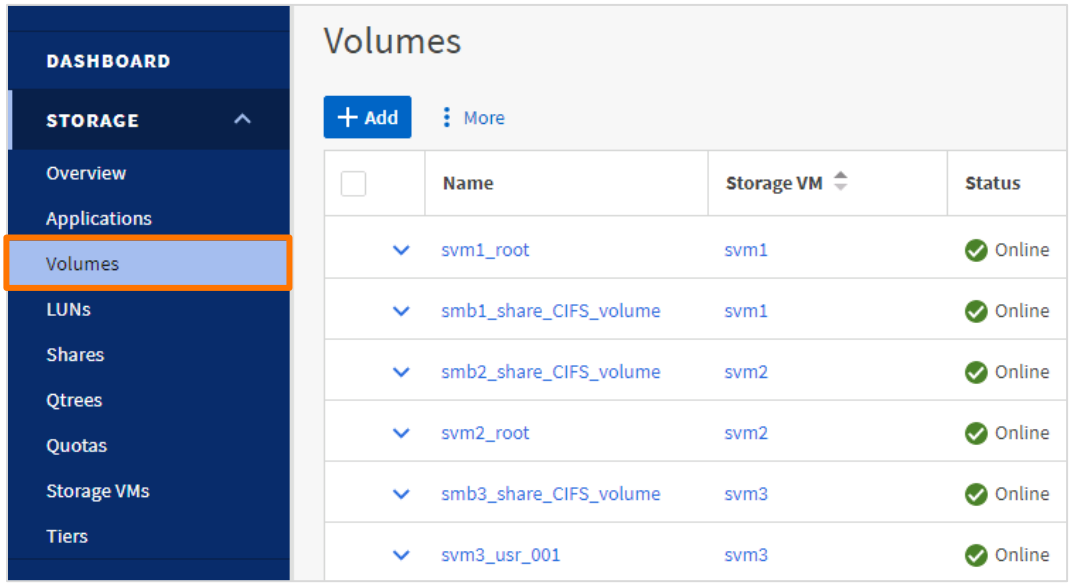
In this task, you create a custom unified replication policy and then create the SnapMirror relationship.

Step	Action
1-1	Cluster2 is the destination cluster for the protection relationship. You create the custom policy on the destination cluster.
1-2	**Cluster2** In the System Manager navigation pane, select **Protection** > **Overview**. 

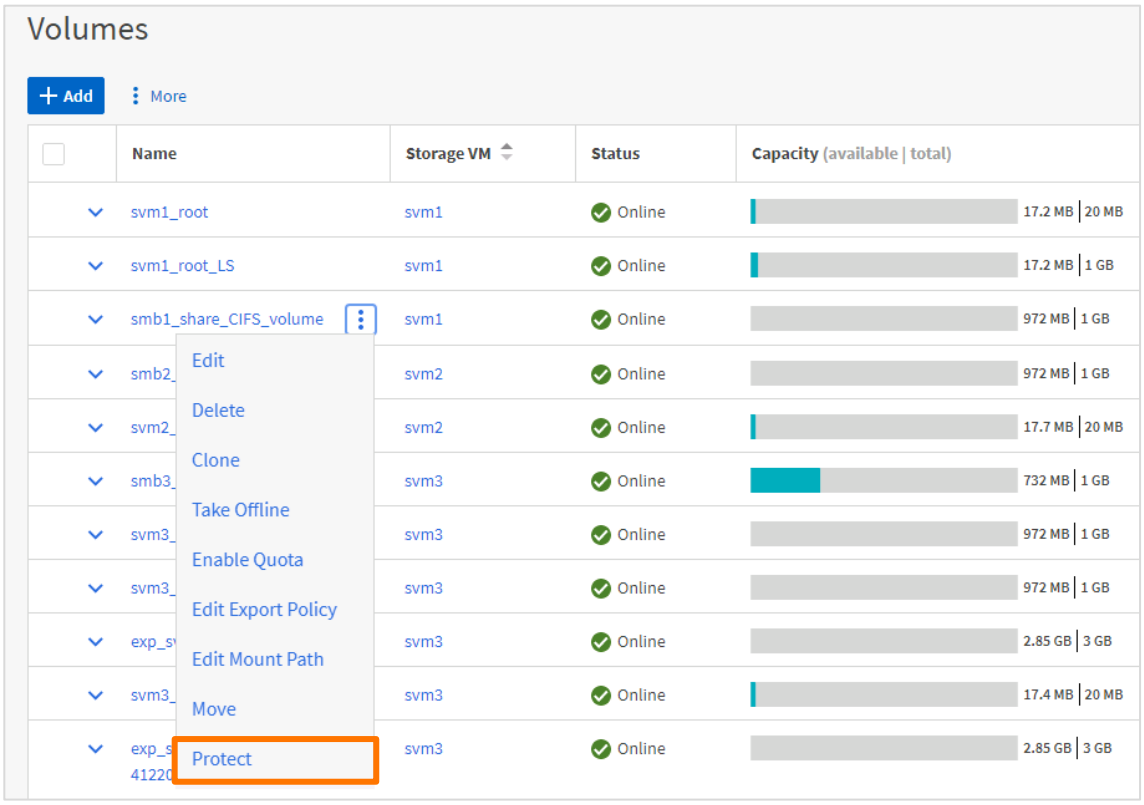
Step	Action
1-3	In the Overview pane, expand **Local Policy Settings**, and then click the arrow in the upper-right corner of the Protection Policies pane. 
1-4	In the Protection Policies pane, click **+Add** to create a policy. 

Step	Action
1-5	In the Add Protection Policy dialog box, specify the following values: ▪ Policy Name: **`svm1_share_mirror_vault`** ▪ Policy Description: **`cluster1:svm1_share_CIFS`** ▪ Policy Scope: **Cluster** ▪ Policy Type: **Asynchronous** ▪ Transfer Schedule: **daily** 

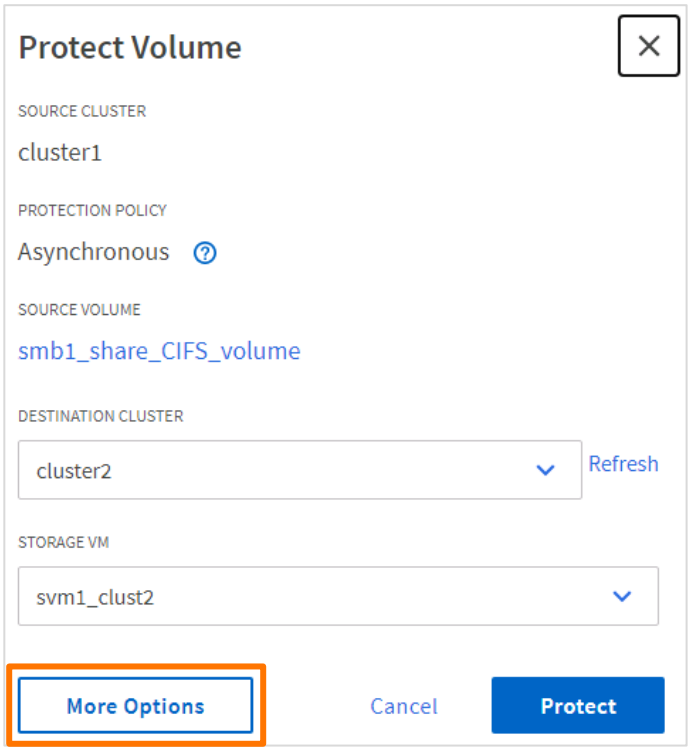
Step	Action
1-6	In the Add Protection Policy dialog box, scroll down and specify the following values: ▪ In the Rules section, click **Add**, and then specify the following values: • Matching SnapMirror Label: **`daily`** • Retention Count: **`7`** ▪ Click **Add** again, and then specify the following values: • Matching SnapMirror Label: **`weekly`** • Retention Count: **`52`** ▪ Enable network compression checkbox: *clear* ▪ Copy the source storage VM configuration checkbox: *clear* ▪ Copy all source Snapshot copies checkbox: *clear* 
1-7	Click **Save**.

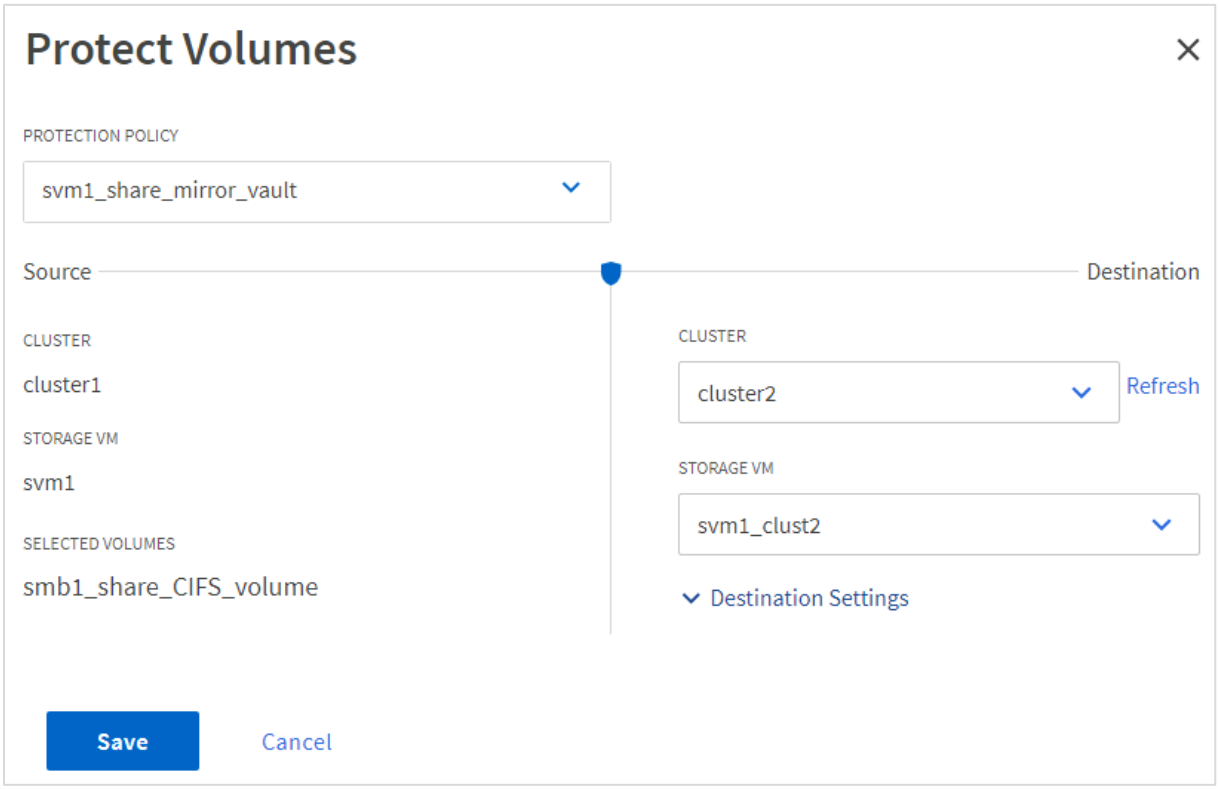
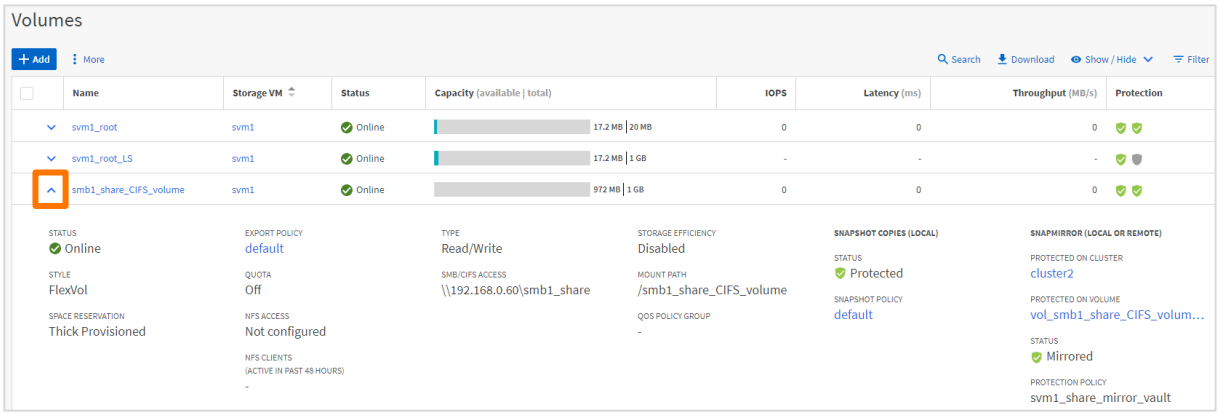
Step	Action
1-8	Verify that the policy was created successfully. 
1-9	Cluster1 is the source cluster in the protection relationship. Next, you protect the volume smb1_share_CIFS_volume on svm1 with the SnapMirror policy that you created.
1-10	**Cluster1** In the System Manager navigation pane, select **Storage** > **Volumes**. 

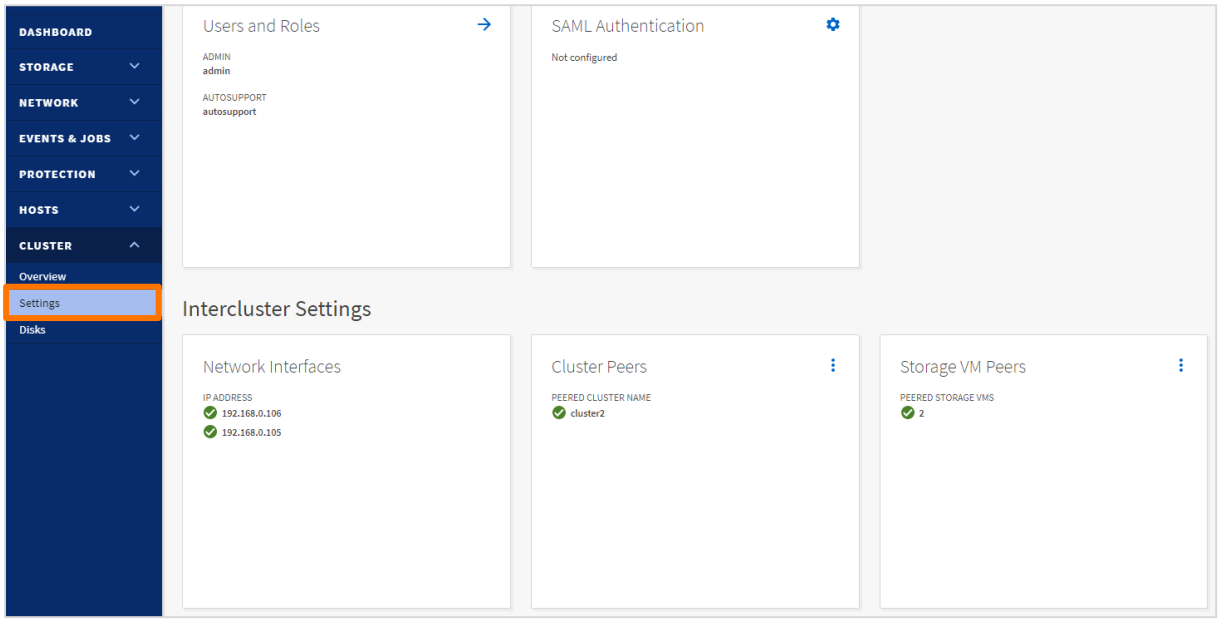
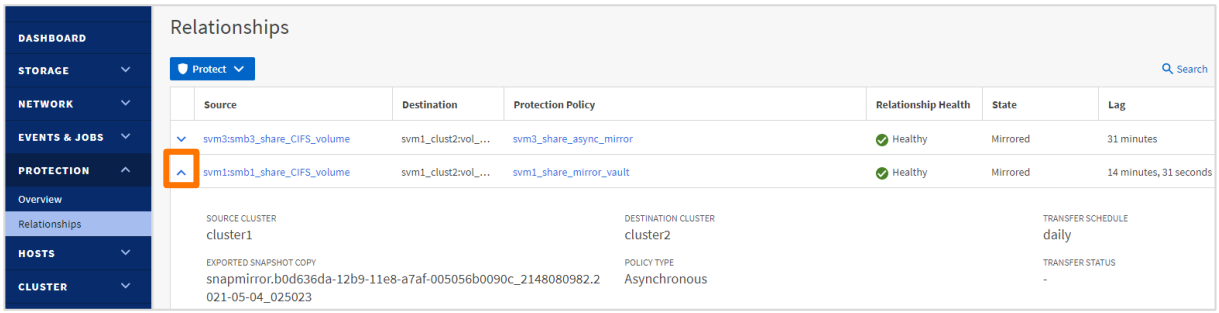
Step	Action
1-11	Click the three vertical dots to the right of smb1_share_CIFS_volume, and then select **Protect**.



1-12	In the Protect Volume dialog box, click **More Options**.

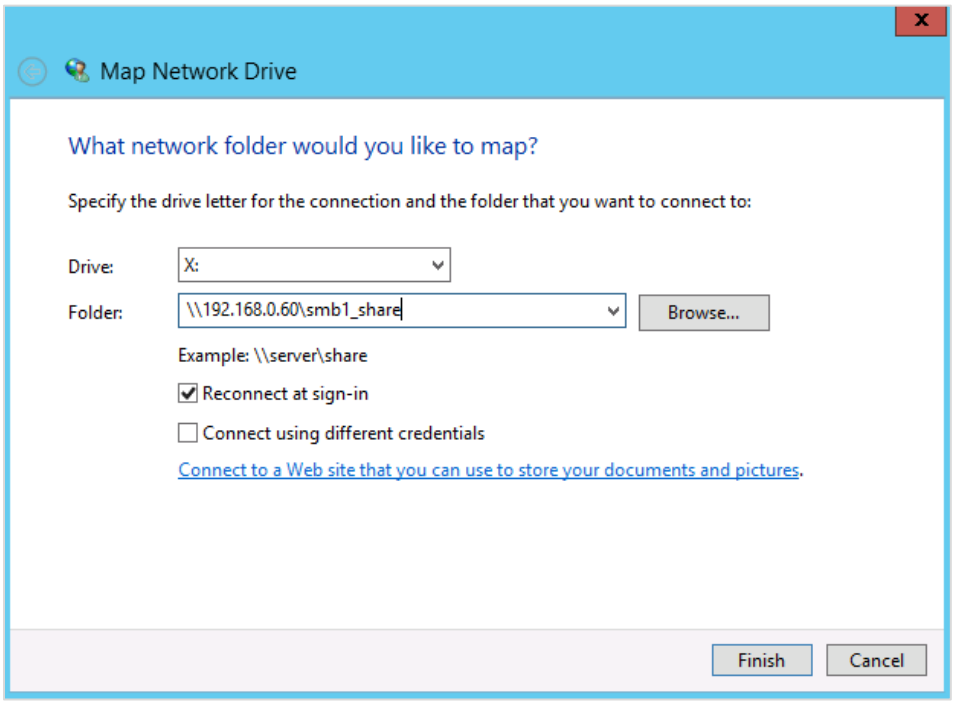


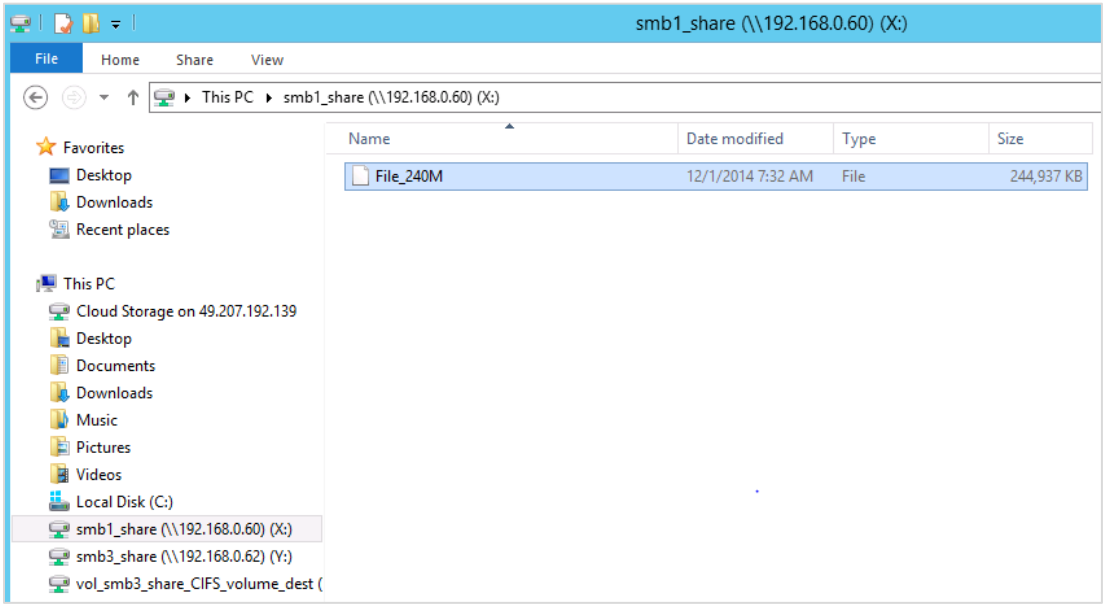
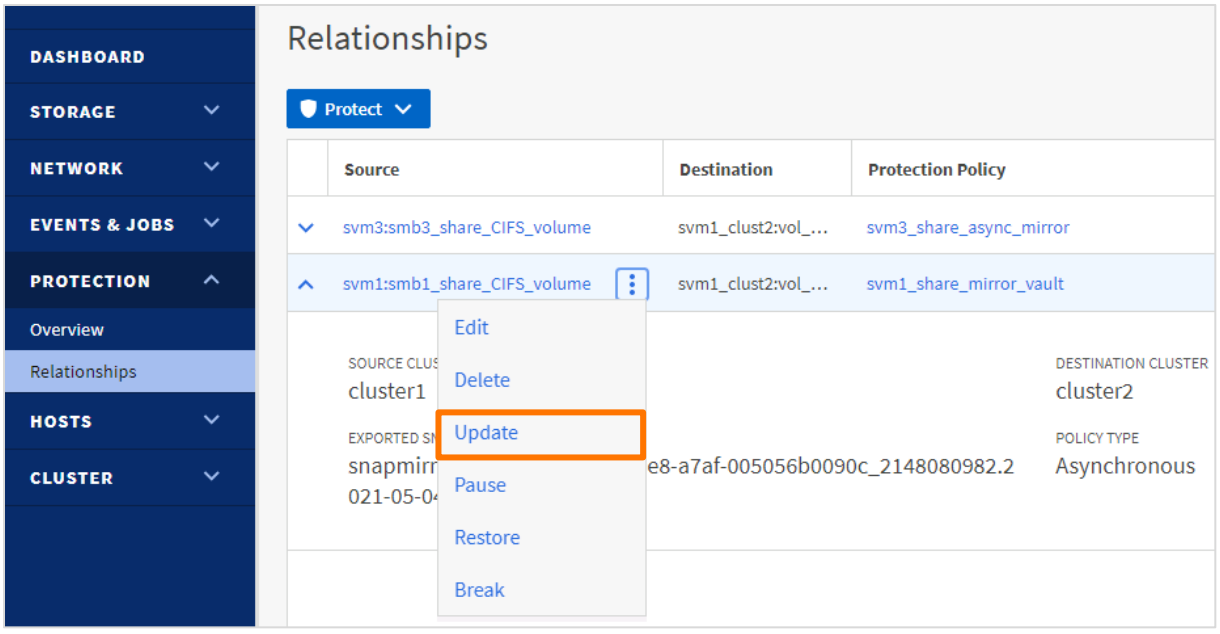
Step	Action
1-13	In the Protect Volumes pane, specify the following values: ▪ Protection Policy: **svm1_share_mirror_vault** ▪ Destination > Cluster: **cluster2** ▪ Destination > Storage VM: **svm1_clust2** 
1-14	Click **Save**.
1-15	Cluster1 and cluster2 are currently in a peer relationship. On cluster1, svm1 is not in a peer relationship with svm1_clust2 on cluster2. However, after you click Save in the previous step, System Manager automatically peers the two SVMs and then creates the SnapMirror relationship.
1-16	In the Volumes pane, click the down arrow to the left of the volume smb1_share_CIFS_volume to view details and verify that the volume is now protected on cluster2. 

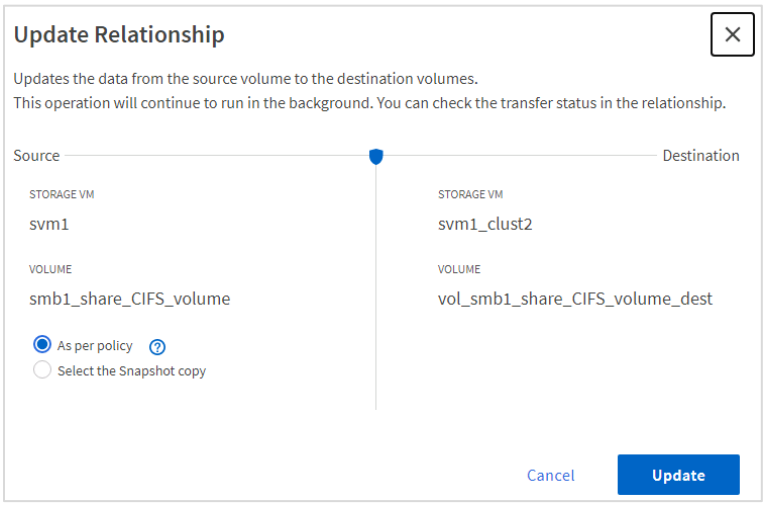
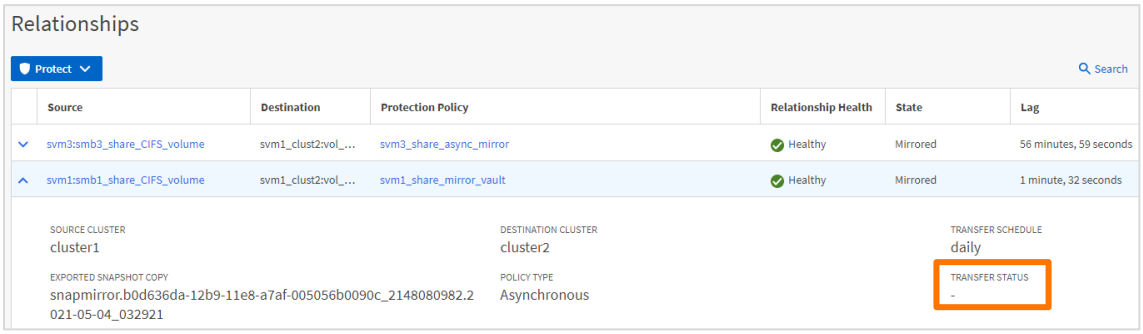
Step	Action
1-17	In the System Manager navigation pane, select **Cluster** > **Settings**.
1-18	In the Settings pane, scroll down to the Intercluster Settings section. 
1-19	In the Storage VM Peers pane, note that two SVMs are now peered with svm1_clust2 on cluster2.
1-20	To view the details of the peered SVMs, in Storage VM Peers, click the three vertical dots in the upper-right corner, and then select **Manage Storage VM Peers**.
1-21	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.
1-22	Verify that the protection relationship was created successfully. To confirm the SnapMirror status, expand the listed relationship. 

Task 2: Verify Data Transfer

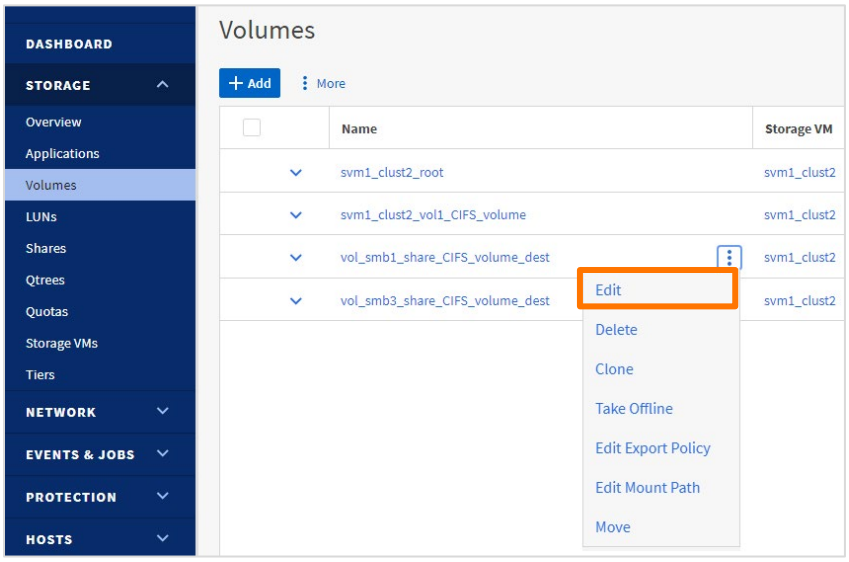
In this task, you verify that the SnapMirror relationship can successfully transfer data from the primary volume to the secondary volume. To test the replication, open File Explorer and map a drive letter to the share on svm1.

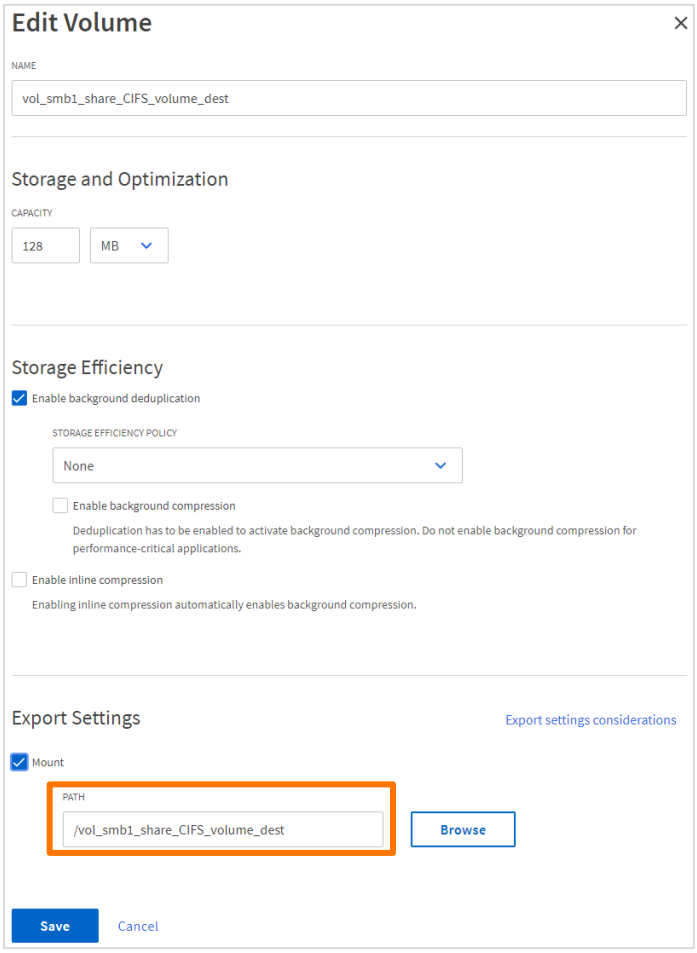
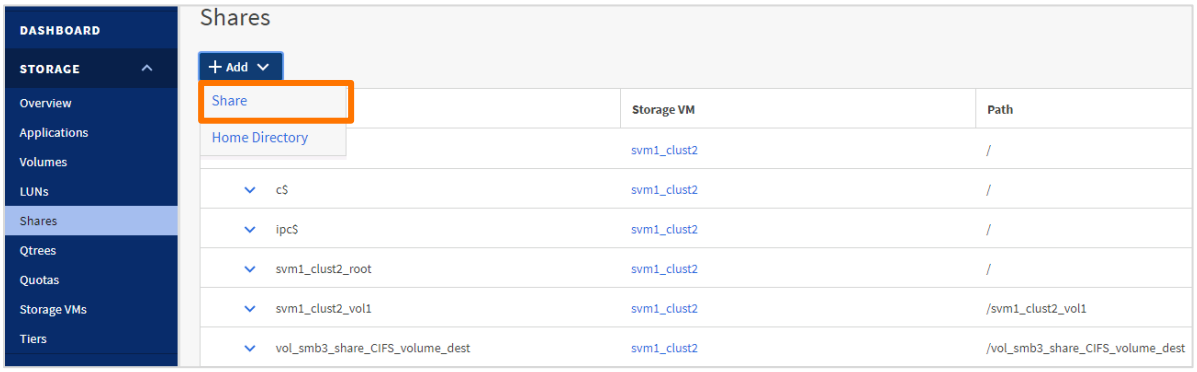
Step	Action
2-1	In File Explorer, open **This PC**, click the **Computer** tab, and then select **Map network drive**.
2-2	An SMB share is set up for the source volume smb1_share_CIFS_volume.
2-3	On the jump host, use File Explorer to map a drive to the source volume on cluster1\svm3. Use the folder path **\\192.168.0.60\smb1_share**. 
2-4	Open the mapped drive **smb1_share (\\192.168.0.60)** and verify that the folder is empty.

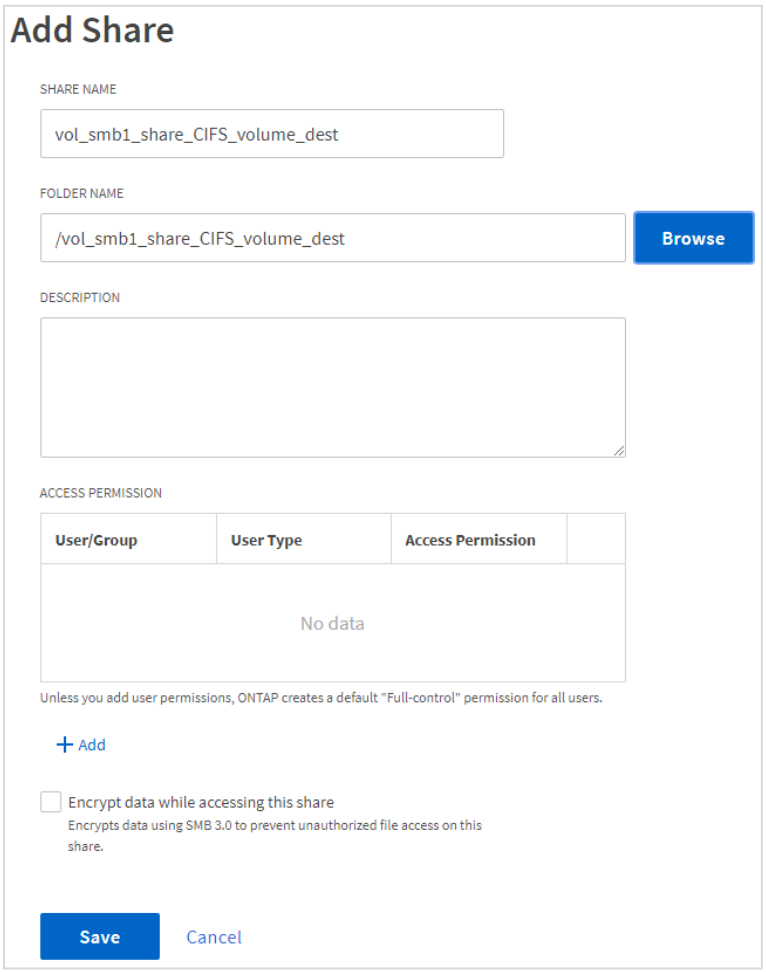
Step	Action
2-5	Copy **File_240M** from C:\CourseFiles to the folder smb1_share. 
2-6	Instead of waiting for the SnapMirror update schedule, initiate a manual update.
2-7	**Cluster2** In the System manager navigation pane, select **Protection** > **Relationships**.
2-8	In the mirror-vault Relationships pane, click the three dots to the right of the source, and then select **Update**. 

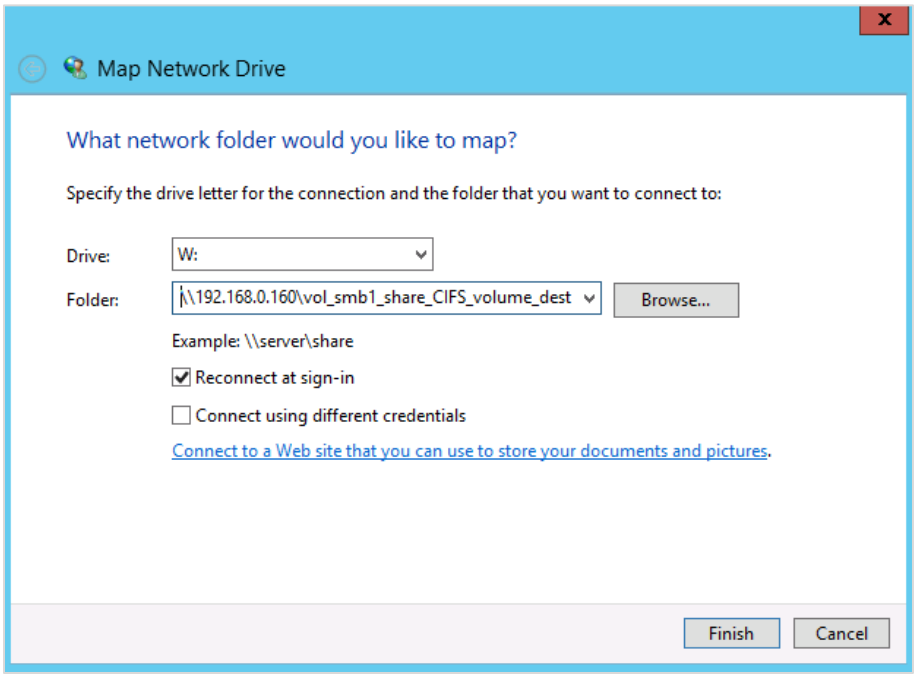
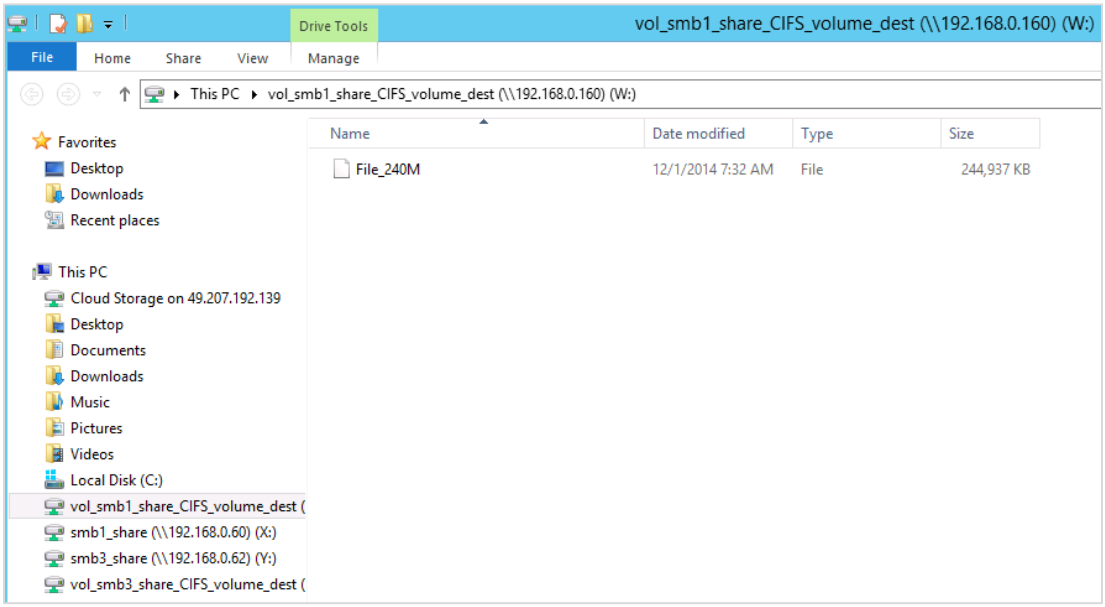
Step	Action
2-9	In the Update Relationship dialog box, click **Update**. 
2-10	Wait for the Transfer Status to change from Transferring to idle. 
2-11	Next, you mount the destination volume created on svm1_clust2 in cluster2.
2-12	In the System Manager navigation pane, select **Storage** > **Volumes**.

Step	Action
2-13	In the Volumes pane, click the three vertical dots to the right of vol_smb1_share_CIFS_volume_dest, and then select **Edit**.



Step	Action
2-14	In the Edit Volume pane, perform the following steps: a. Retain the default values for all the fields. b. Scroll down to the Export Settings section. c. Note the volume mount path (/vol_smb1_share_CIFS_volume_dest). 
2-15	Select the **Mount** checkbox, and then click **Save**.
2-16	In the System Manager navigation pane, select **Storage** > **Shares**.
2-17	In the Shares pane, click **+Add**, and then select **Share**. 

Step	Action
2-18	In the Add Share pane, specify the following values: ▪ Share Name: **`vol_smb1_share_CIFS_volume_dest`** ▪ Folder Name: **`/vol_smb1_share_CIFS_volume_dest`** (Alternatively, you can click **Browse**, and then select the folder.) ▪ Description: *clear* 
2-19	Click **Save**.
2-20	Next, on the jump host, you map a drive to the destination volume.

Step	Action
2-21	To map a drive to the destination volume, use the following folder path: **\\192.168.0.160\vol_smb1_share_CIFS_volume_dest**. 
2-22	In File Explorer, open the mapped drive **vol_smb1_share_CIFS_volume_dest** and verify that the SnapMirror relationship transferred the file from the source. 

End of exercise

Exercise 4: Restoring Data From a Snapshot Copy

In this exercise, you simulate data loss or corruption on the source volume. You then restore an entire volume to the most recent Snapshot copy.

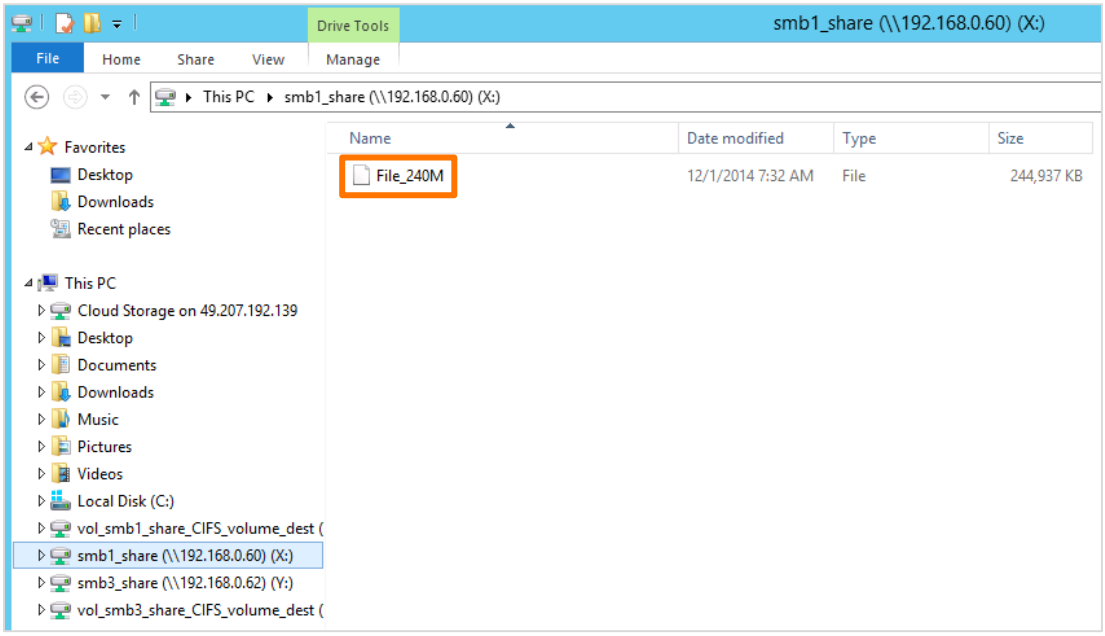
Objectives

This exercise focuses on enabling you to do the following:

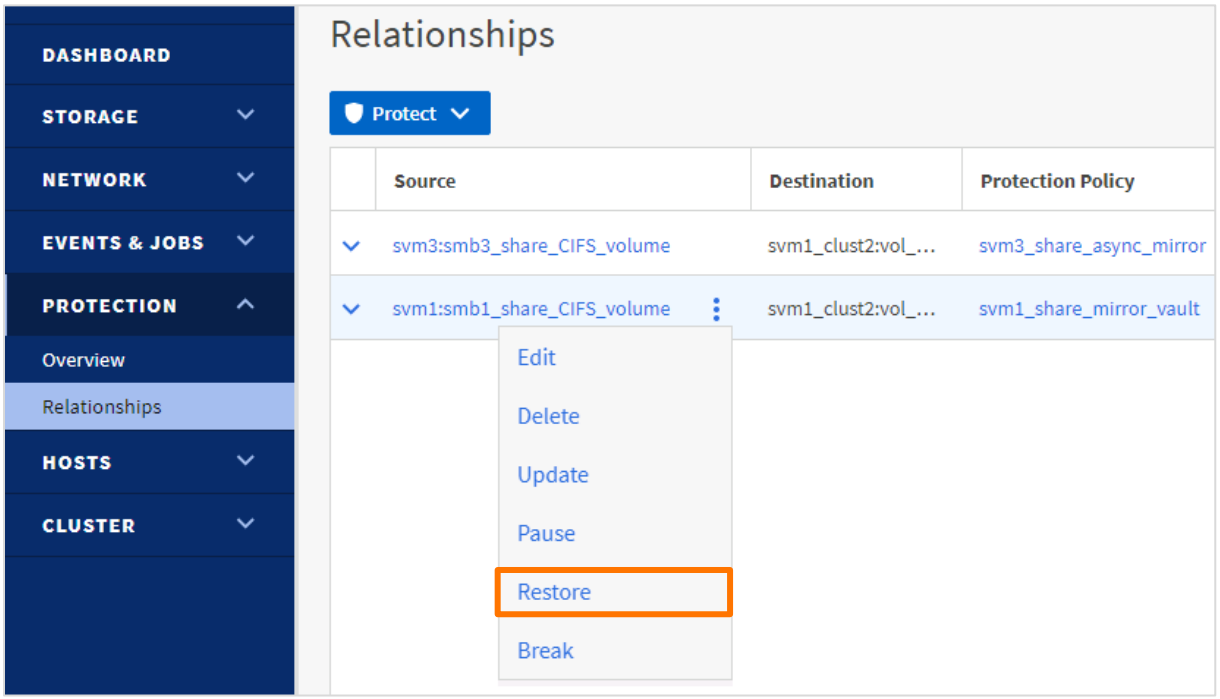
- Simulate a disaster
- Use SnapMirror to recover your data

Task 1: Simulate a Disaster and Recover Data

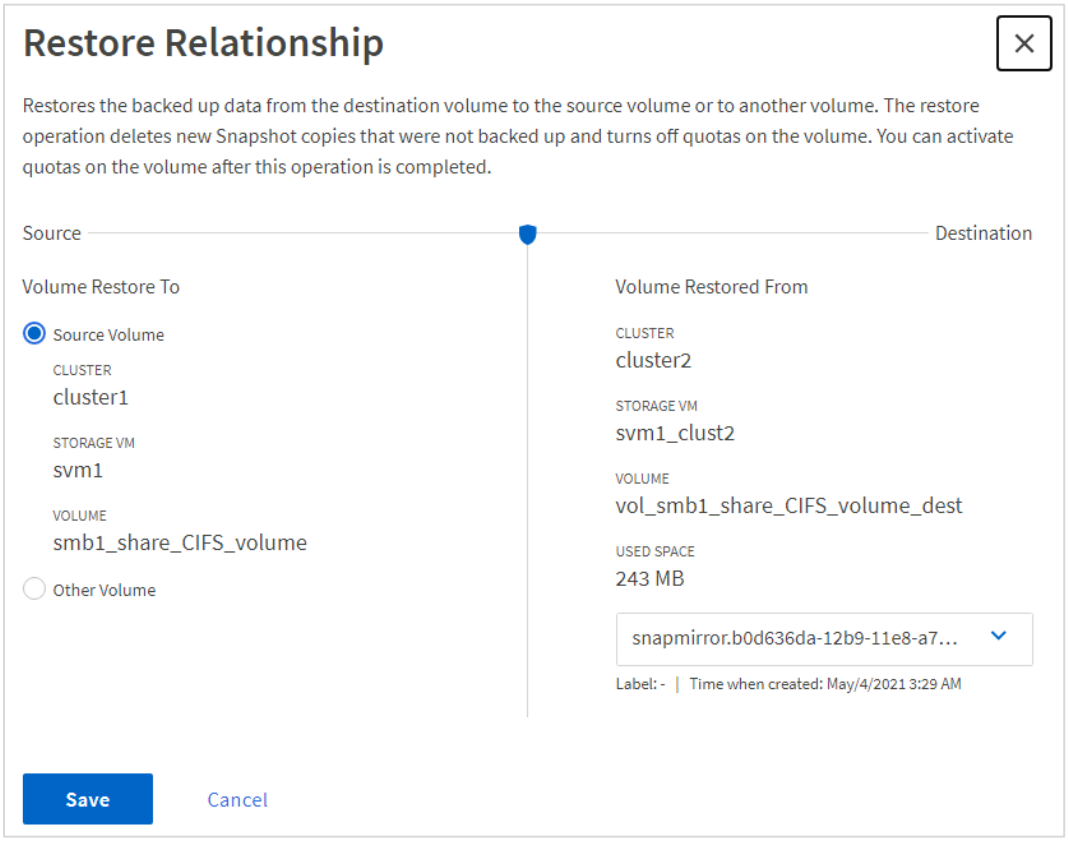
In this task, you delete a file on the source volume to simulate data loss or corruption. From the destination cluster, you then roll back your data by restoring from an earlier Snapshot copy.

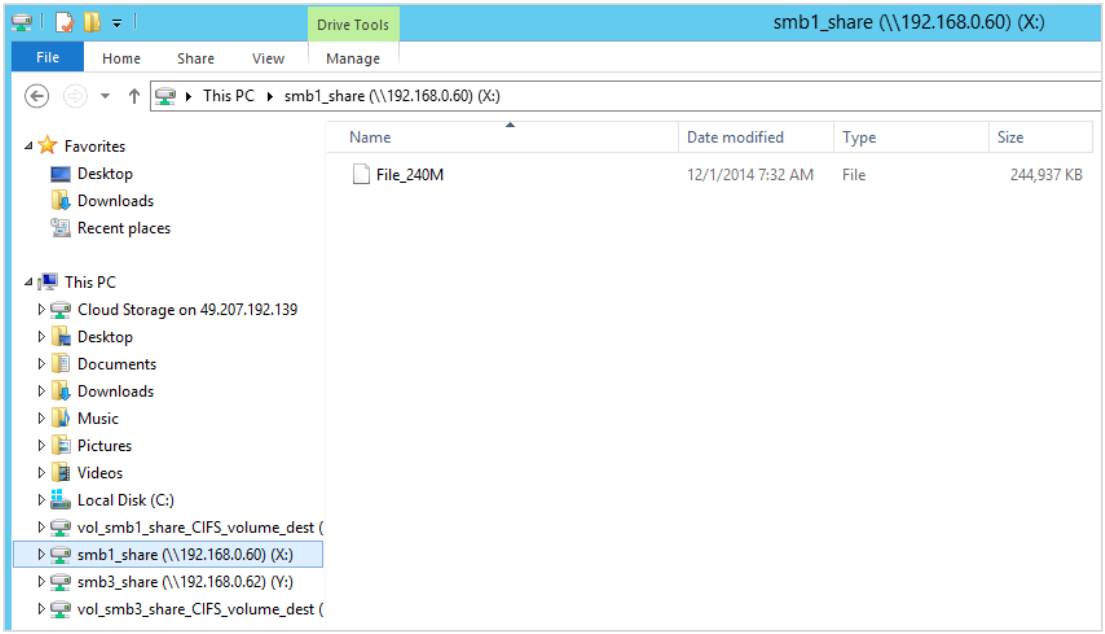
Step	Action
1-1	In File Explorer, open the mapped drive **smb1_share** and simulate data loss by deleting **File_240M**. 
1-2	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.

Step	Action
1-3	On the Relationships pane, in the mirror-vault relationship, click the three vertical dots to the right of the source, and then select **Restore**.



1-4	On the Restore Relationship pane, retain the default settings and verify that the latest Snapshot copy is selected.



Step	Action
1-5	The policy that is assigned to the SnapMirror relationship has a job schedule that is configured for daily and weekly updates, so you need to restore from the most recent Snapshot copy.
1-6	Click **Save**, and then wait for the restore operation to complete.
1-7	In File Explorer, return to **smb1_share (\\192.168.0.60)** and verify that file File_240M is restored. If required, refresh your screen. 

End of exercise

Exercise 5: Configuring a SnapMirror Synchronous Relationship

In this exercise, you configure a SnapMirror Synchronous (SM-S) relationship between two volumes.

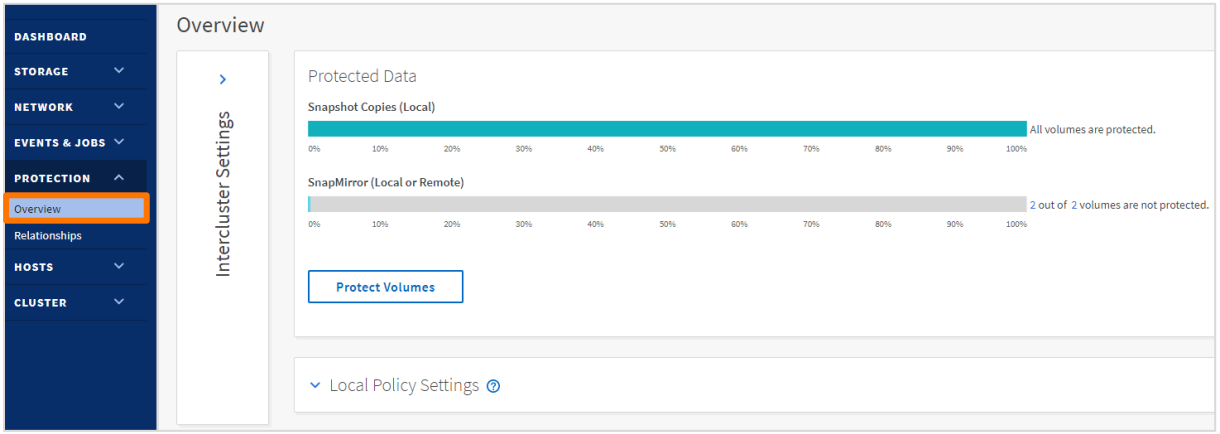
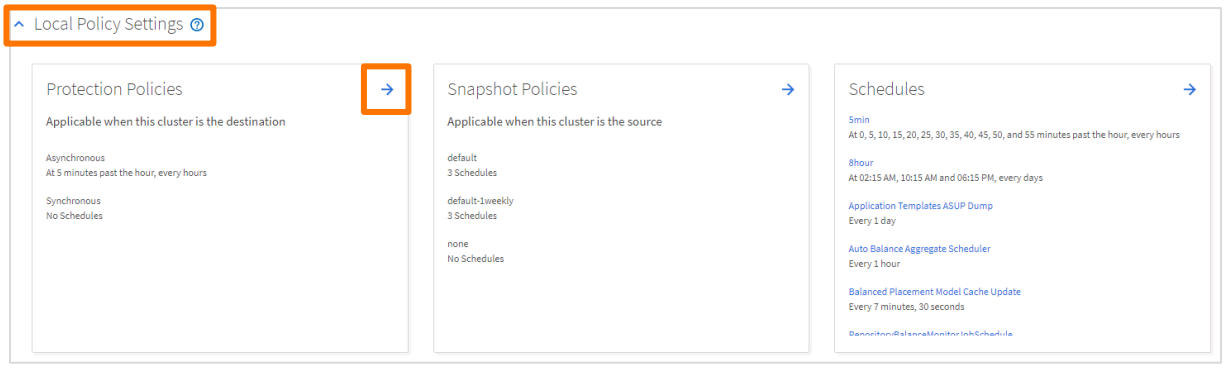
Objectives

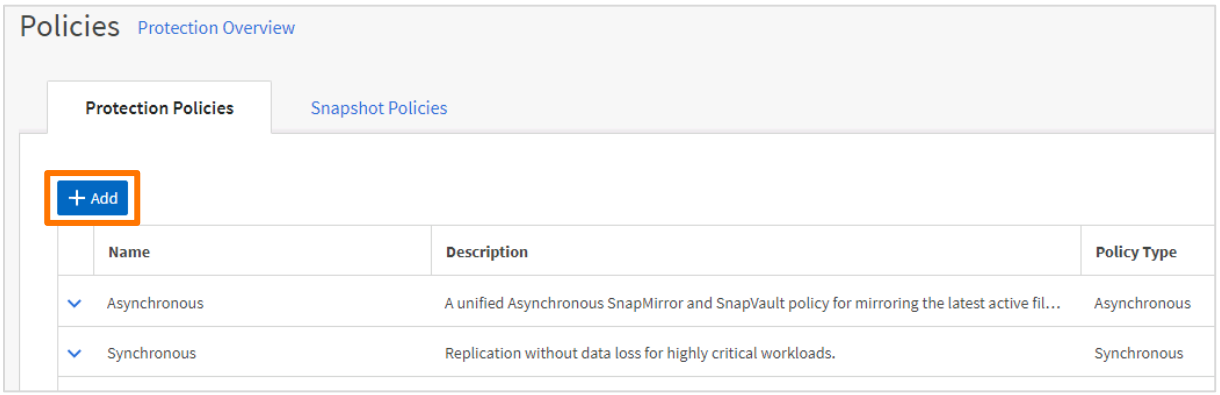
This exercise focuses on enabling you to do the following:

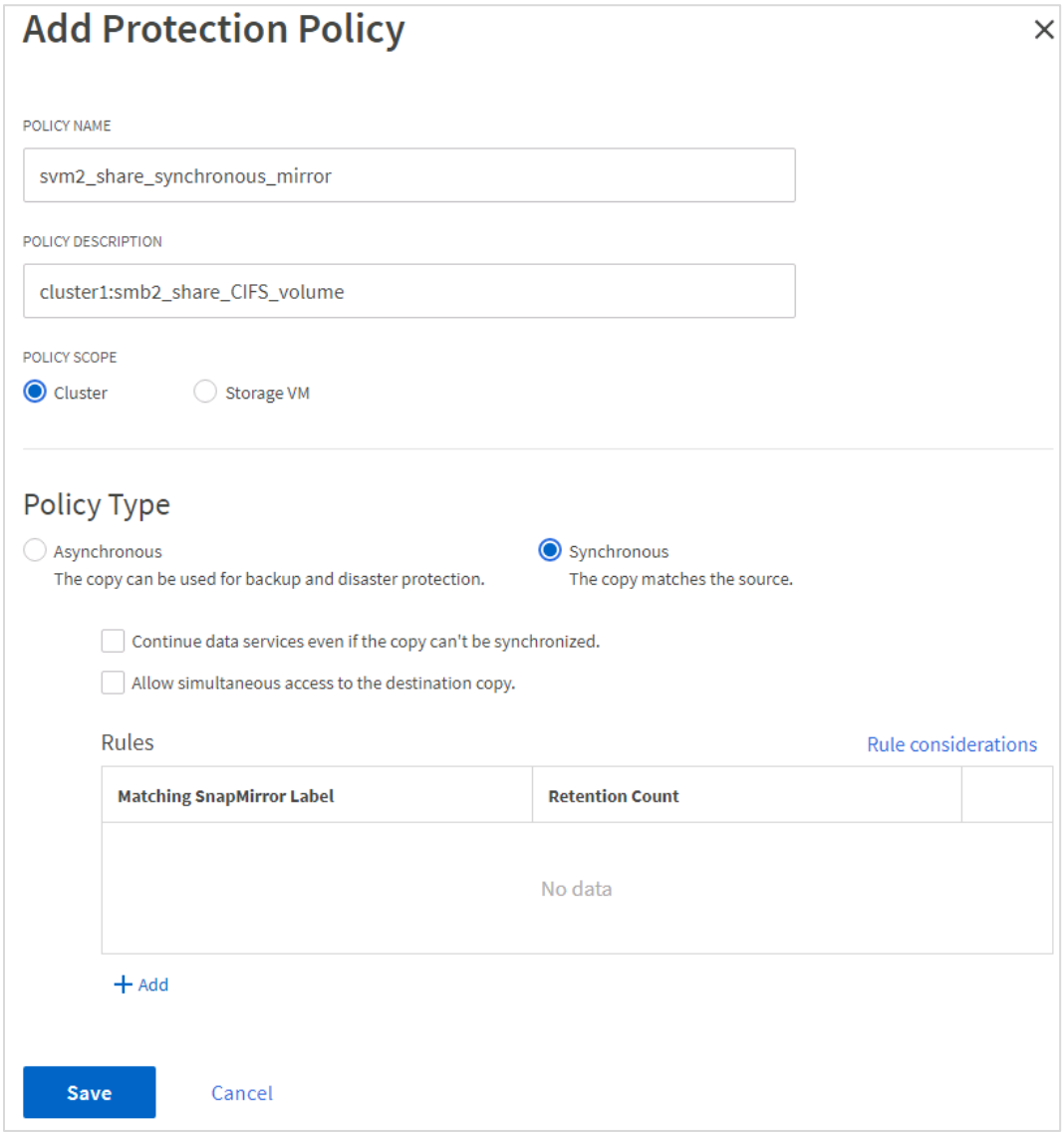
- Create an SM-S replication policy
- Create an SM-S relationship

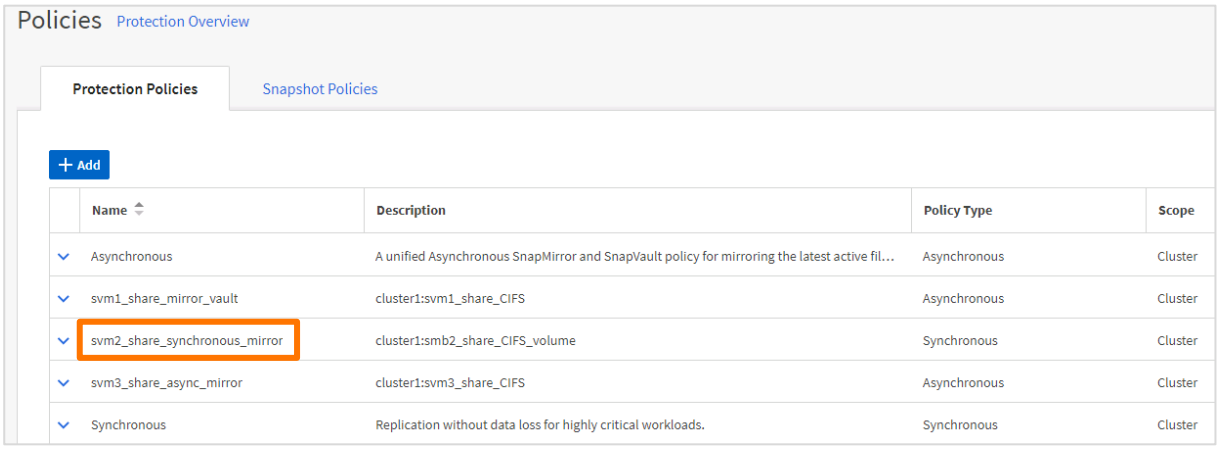
Task 1: Create an SM-S Policy

In this task, you create an SM-S policy and relationship.

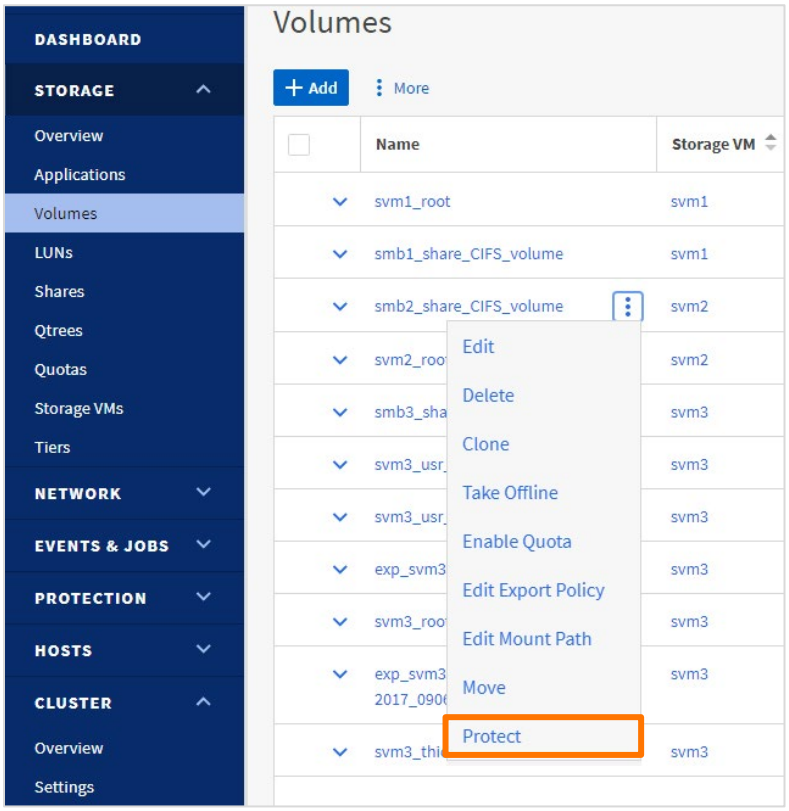
Step	Action
1-1	**Cluster2** In the System Manager navigation pane, select **Protection** > **Overview**. 
1-2	In the Overview pane, expand **Local Policy Settings**, and then click the arrow in the upper-right corner of **Local Policy Settings** > **Protection Policies**. 

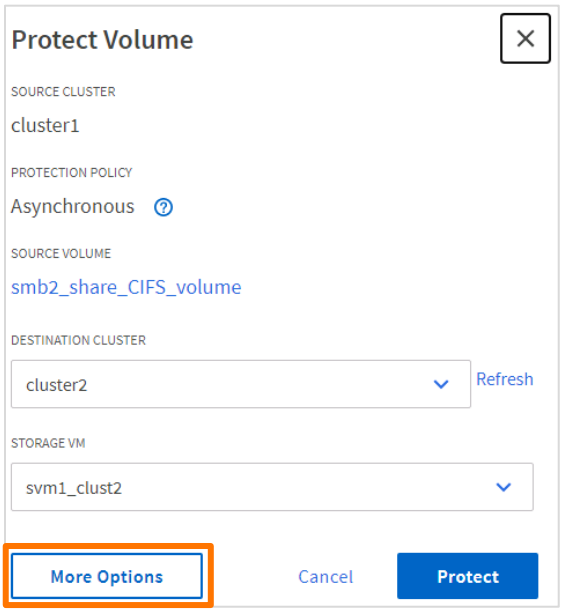
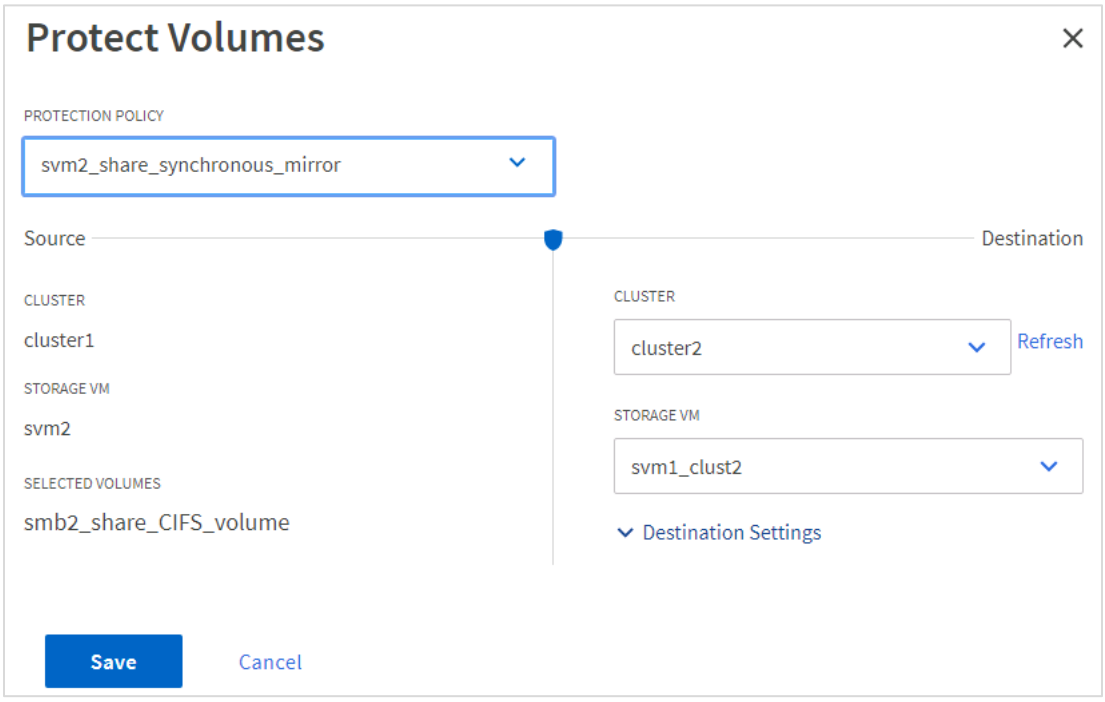
Step	Action
1-3	In the Protection Policies pane, click **+Add** to create a policy. 
1-4	In the next step, select the Synchronous policy type before entering the policy name. If you select the Synchronous policy type after entering the policy name, then the policy name changes to a default value. You will then need to reenter the policy name.

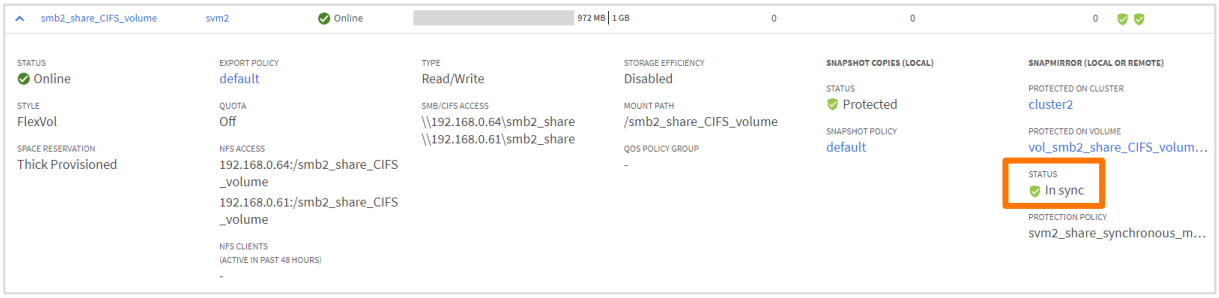
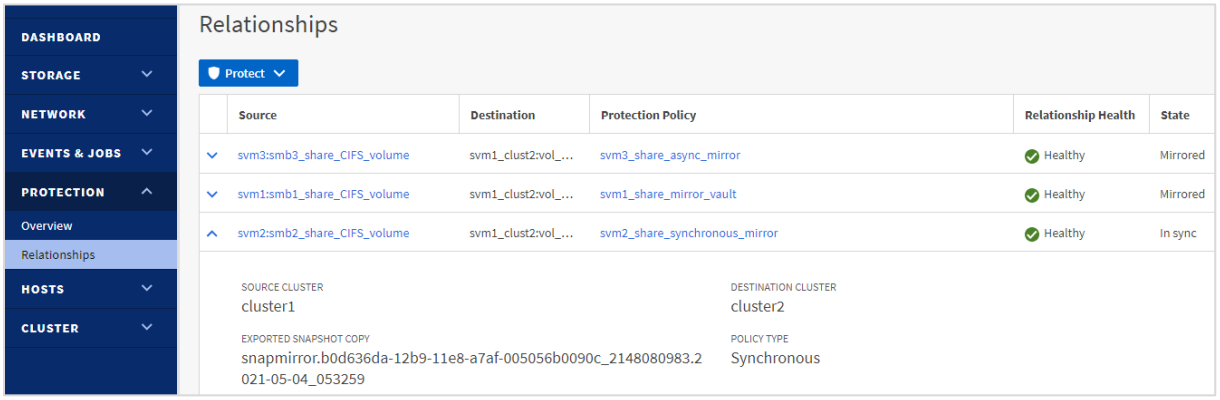
Step	Action
1-5	In the Adding Protection Policy dialog box, specify the following values: ▪ Policy Name: **`svm2_share_synchronous_mirror`** ▪ Policy Description: **`cluster1:smb2_share_CIFS_volume`** ▪ Policy Scope: **Cluster** ▪ Policy Type: **Synchronous** ▪ Continue data services even if the copy can't be synchronized checkbox: *clear* ▪ Allow simultaneous access to the destination copy checkbox: *clear* 
1-6	Click **Save**.

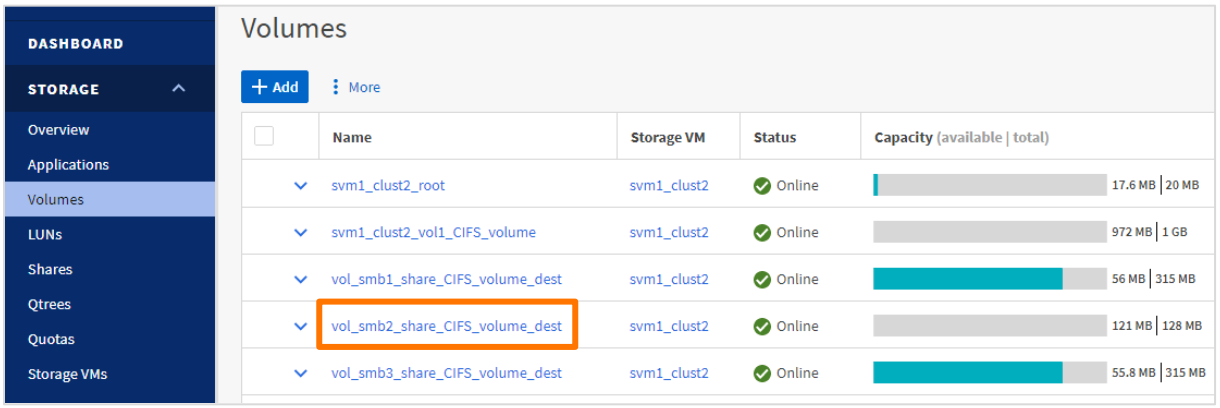
Step	Action
1-7	In the Protection Policies section, verify that the policy was created successfully. 

Task 2: Create an SM-S Relationship

Step	Action
2-1	**Cluster1** In the System Manager navigation pane, select **Storage** > **Volumes**.
2-2	Click the three vertical dots to the right of smb2_share_CIFS_volume, and then select **Protect**. 

Step	Action
2-3	In the Protect Volume dialog box, click **More Options**. 
2-4	In the Protect Volumes pane, specify the following values: ▪ Protection Policy: **svm2_share_synchronous_mirror** ▪ Destination > Cluster: **cluster2** ▪ Destination > Storage VM: **svm1_clust2** 
2-5	Expand **Destination Settings**, and then review the listed values without making any changes.
2-6	Click **Save**.

Step	Action
2-7	Cluster1 and cluster2 are currently in a peer relationship. On cluster1, svm2 is not in a peer relationship with svm1_clust2 on cluster2. However, after you click Save in the previous step, System Manager automatically peers the two SVMs and then creates the SnapMirror relationship.
2-8	The Adding the relationship status bar appears for a few seconds. Optionally, you may click **Run in Background**.
2-9	In the Volumes pane, click the down arrow next to **smb2_share_CIFS_volume** to view details and verify that the protection relationship was created successfully and that the status is In sync. 
2-10	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.
2-11	In the Relationships pane, verify that the SM-S relationship is listed and healthy. 
2-12	In the navigation pane, select **Storage** > **Volumes**.

Step	Action
2-13	In the Volumes pane, verify that the destination volume for the SM-S relationship is listed. 

End of exercise

Exercise 6: Using FlexClone Technology to Clone a SnapMirror Volume

In this exercise, you use FlexClone technology to clone the SnapMirror destination volume for disaster-recovery testing.

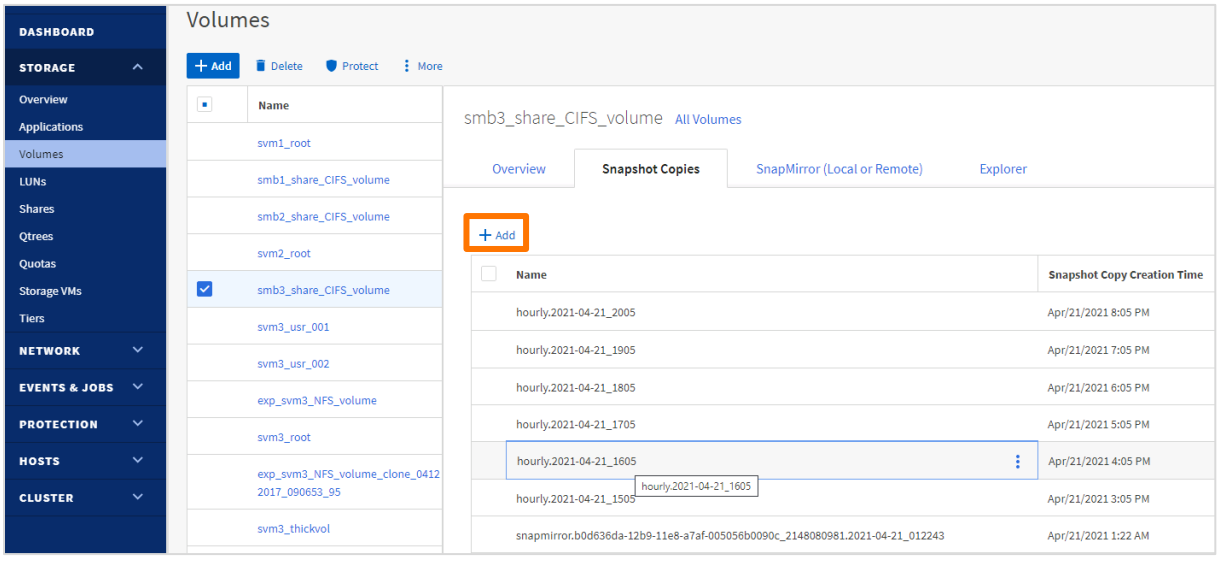
Objectives

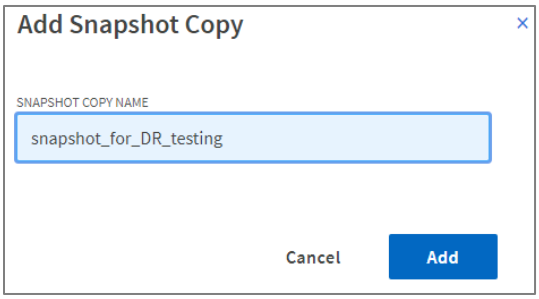
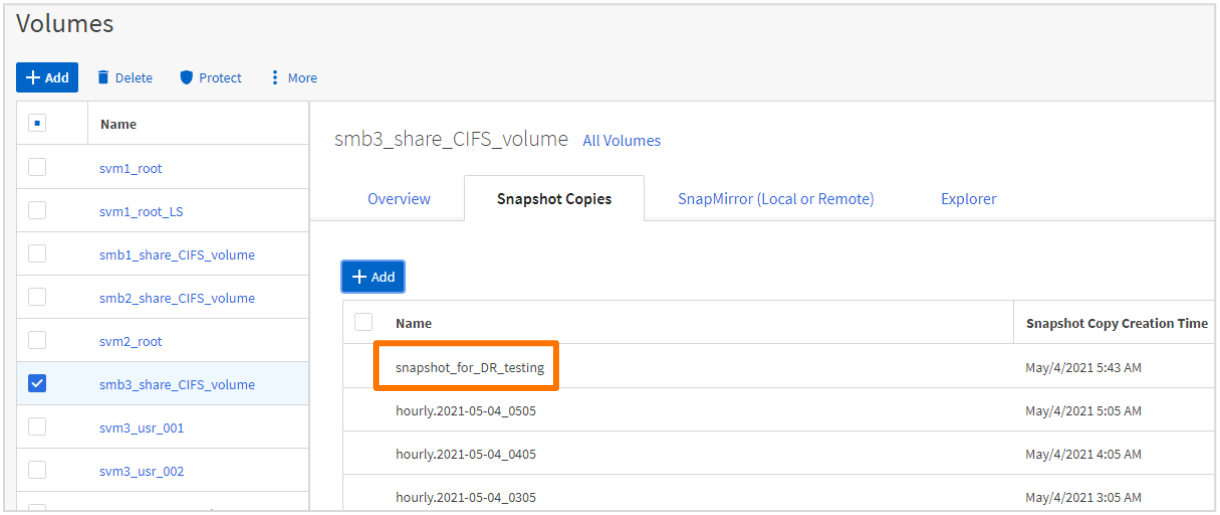
This exercise focuses on enabling you to do the following:

- Create an unscheduled Snapshot copy on the SnapMirror source volume
- Perform a SnapMirror update to replicate the unscheduled Snapshot copy to the destination volume
- Use the unscheduled Snapshot copy as a base for the FlexClone volume
- Take the cloned volume offline and delete the cloned volume

Task 1: Create an Unscheduled Snapshot Copy on the SnapMirror Source Volume

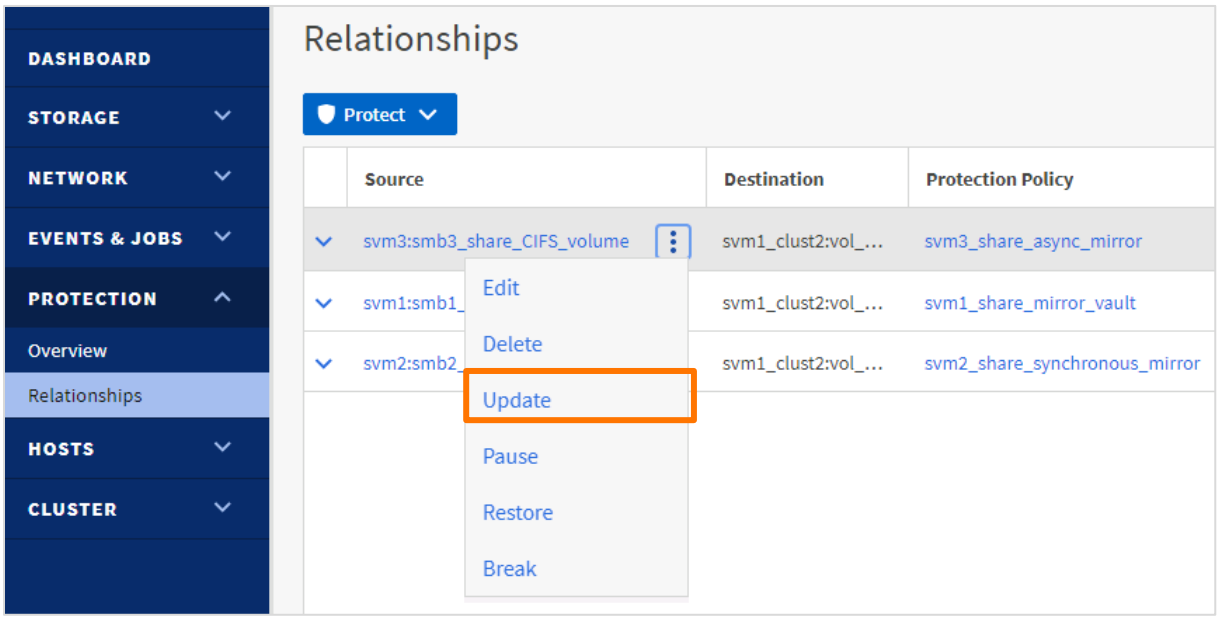
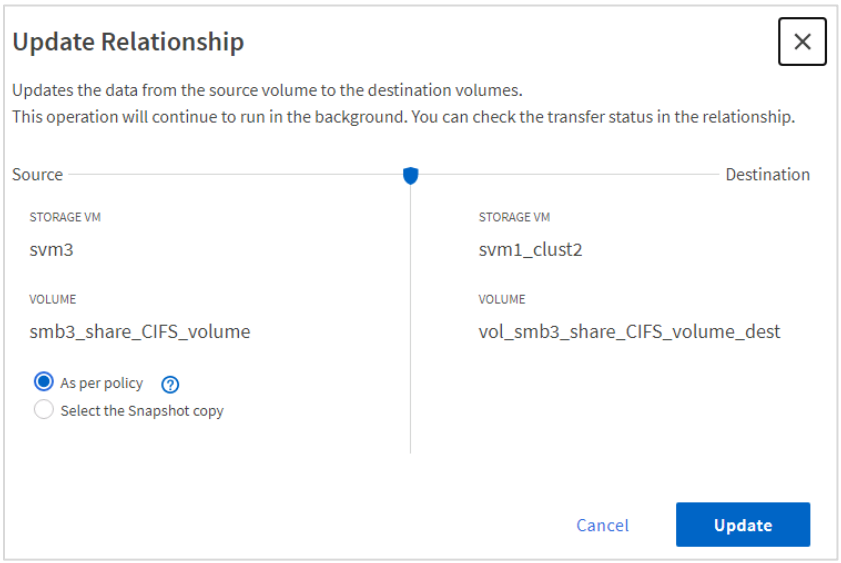
In this task, you create an unscheduled Snapshot copy of the volume smb3_share_CIFS_volume.

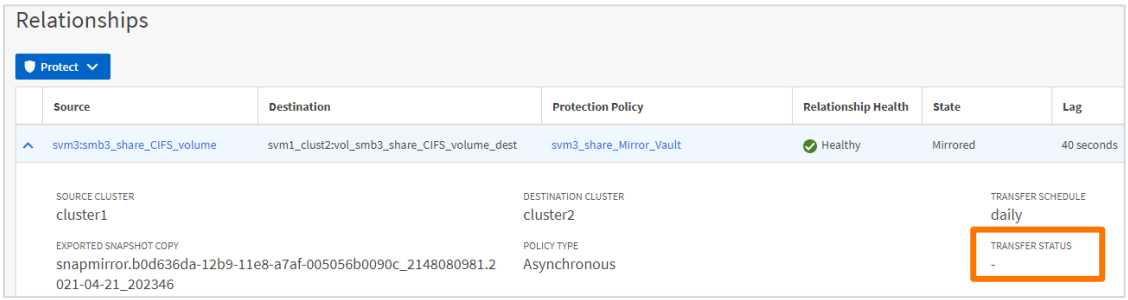
Step	Action
1-1	**Cluster1** In the System Manager navigation pane, select **Storage** > **Volumes**.
1-2	In the Volumes pane, click **smb3_share_CIFS_volume**.
1-3	Click the **Snapshot Copies** tab, and then click **+Add**. 

Step	Action
1-4	In the Add Snapshot Copy dialog box, name the Snapshot Copy **`snapshot_for_DR_testing`**, and then click **Add**. 
1-5	Verify that the snapshot copy is created and visible in the smb3_share_CIFS_volume Snapshot Copies list. 
1-6	Next, you manually update the SnapMirror relationship.

Task 2: Perform a SnapMirror Update to Replicate the Unscheduled Snapshot Copy

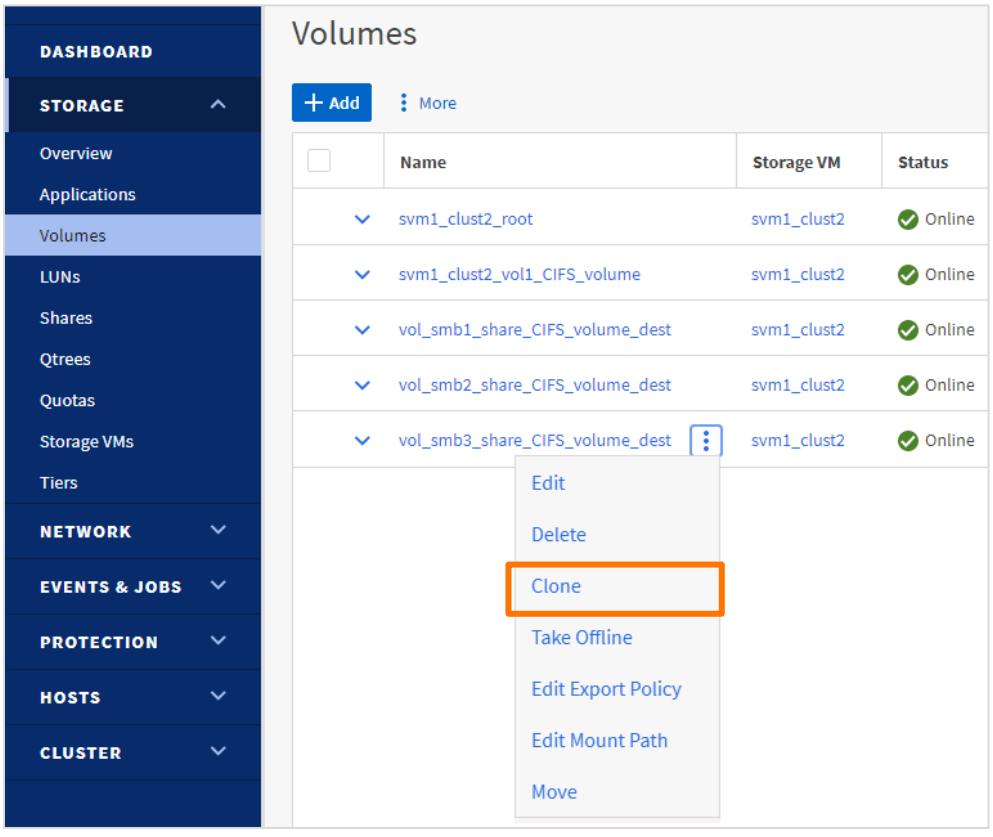
In this task, you perform a SnapMirror update to replicate the unscheduled Snapshot copy to the destination volume.

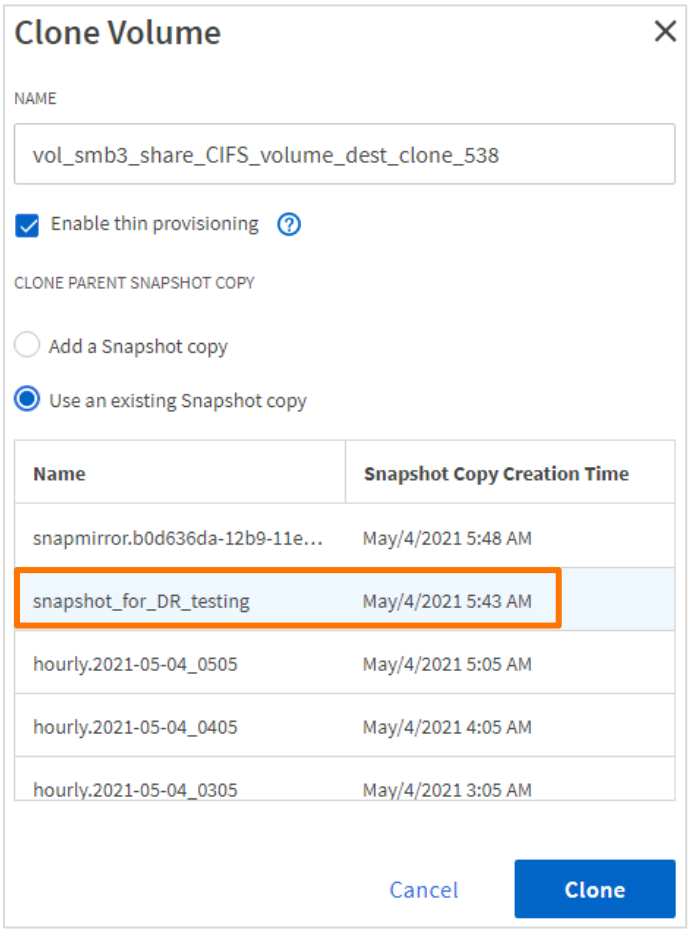
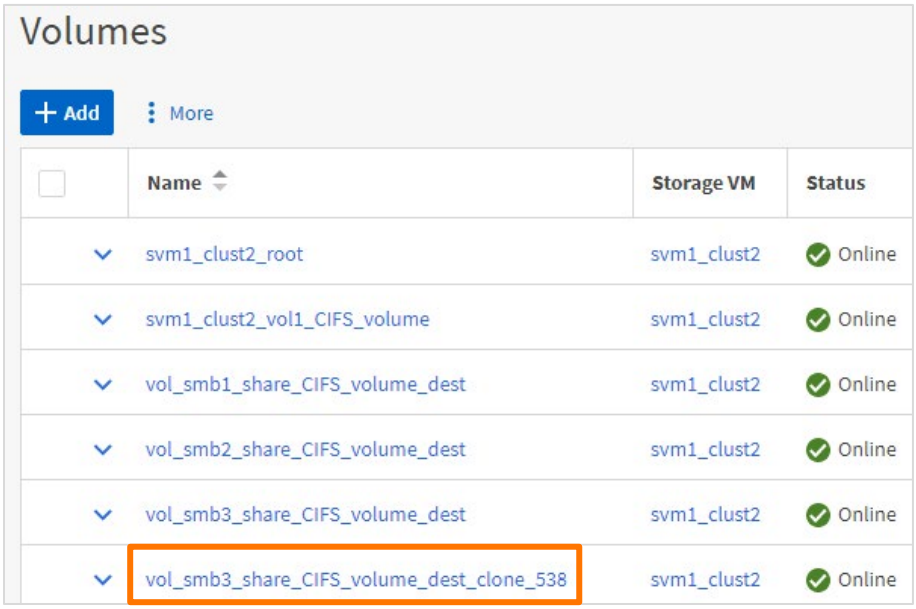
Step	Action
2-1	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.
2-2	In the Relationships pane, select the three vertical dots to the right of the relationship for smb3_share_CIFS_volume, and then select **Update**. 
2-3	In the Update Relationship dialog box, accept the default settings, and then click **Update**. 

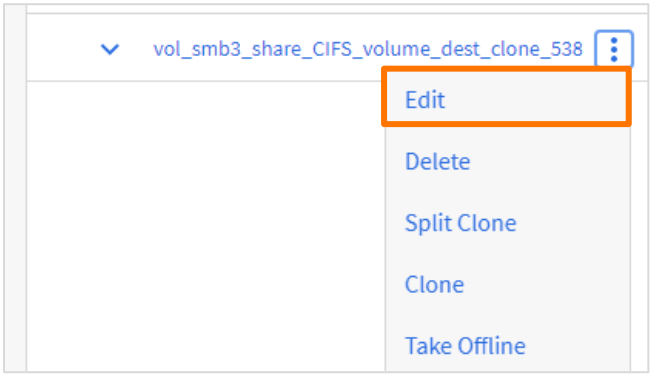
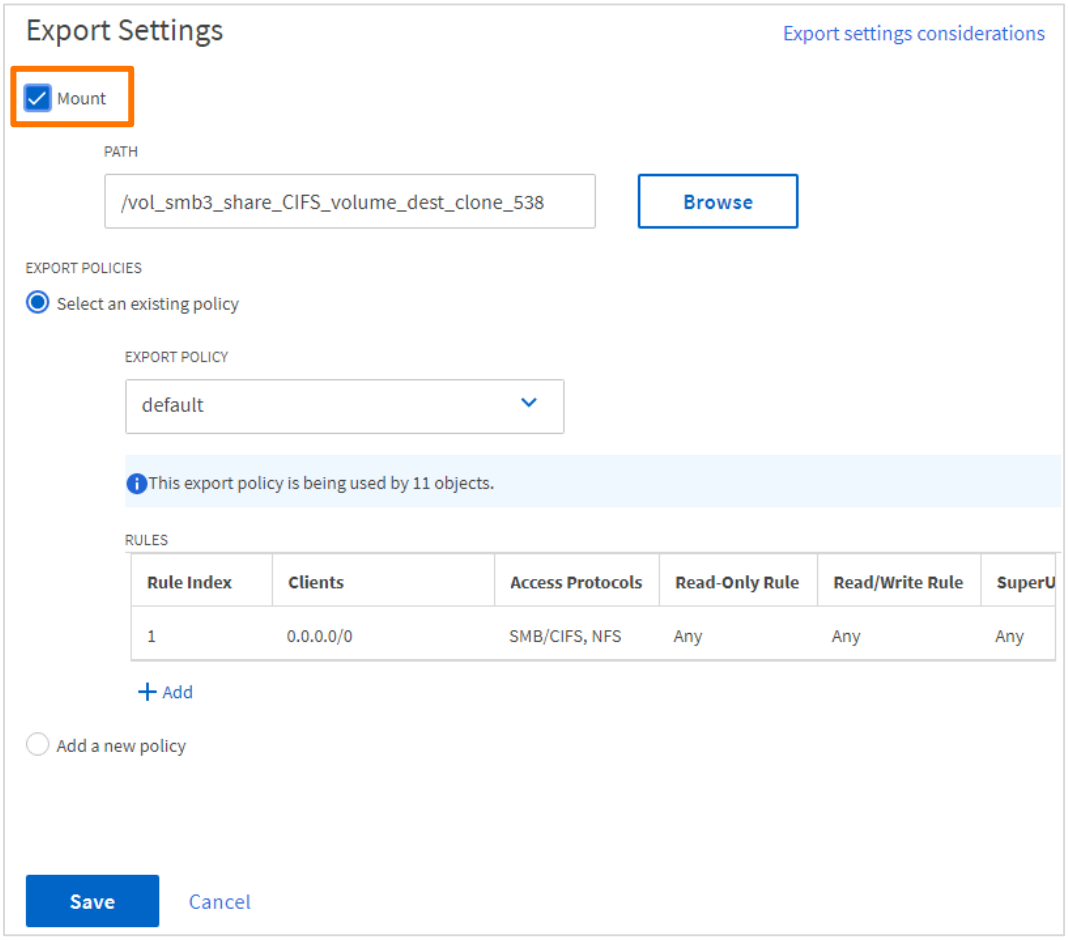
Step	Action
2-4	Expand the **smb3_share_CIFS_volume** relationship, and then wait for the Transfer Status to change from Transferring to idle. 

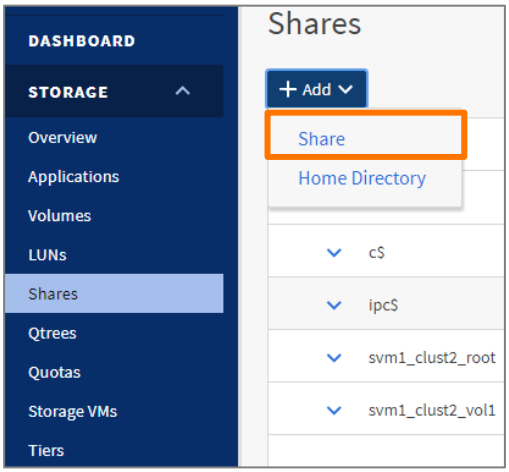
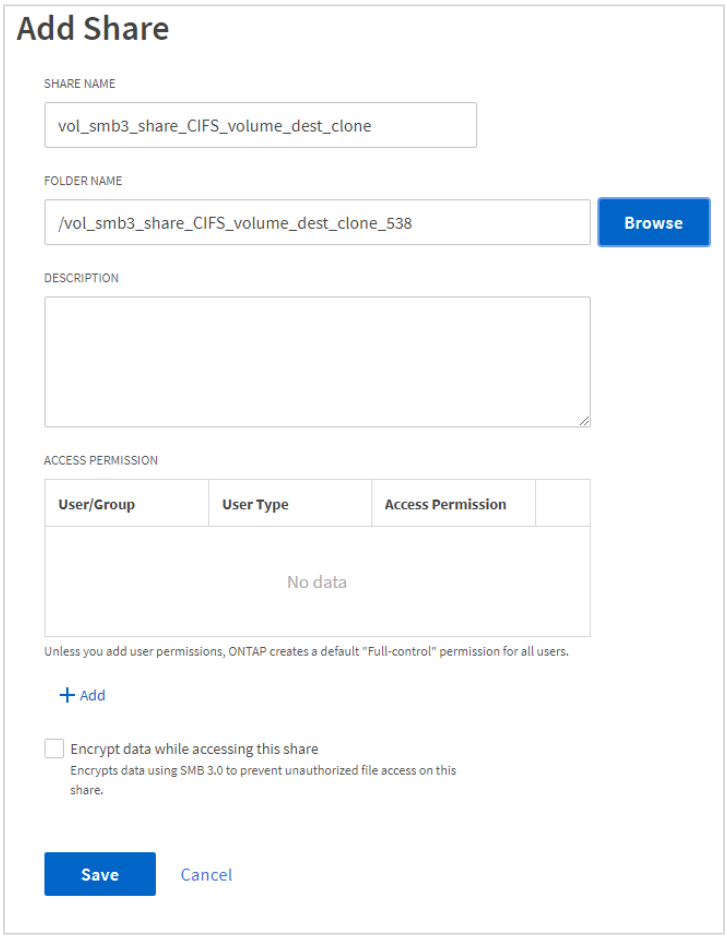
Task 3: Create the FlexClone Volume

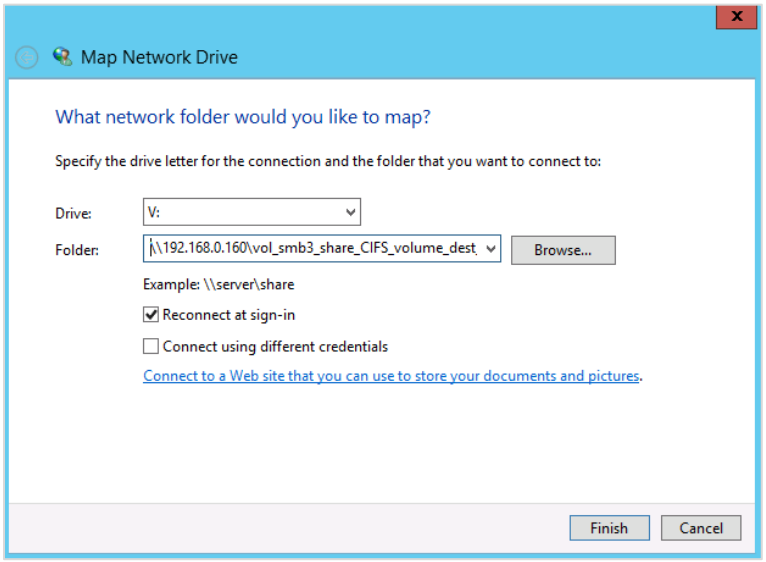
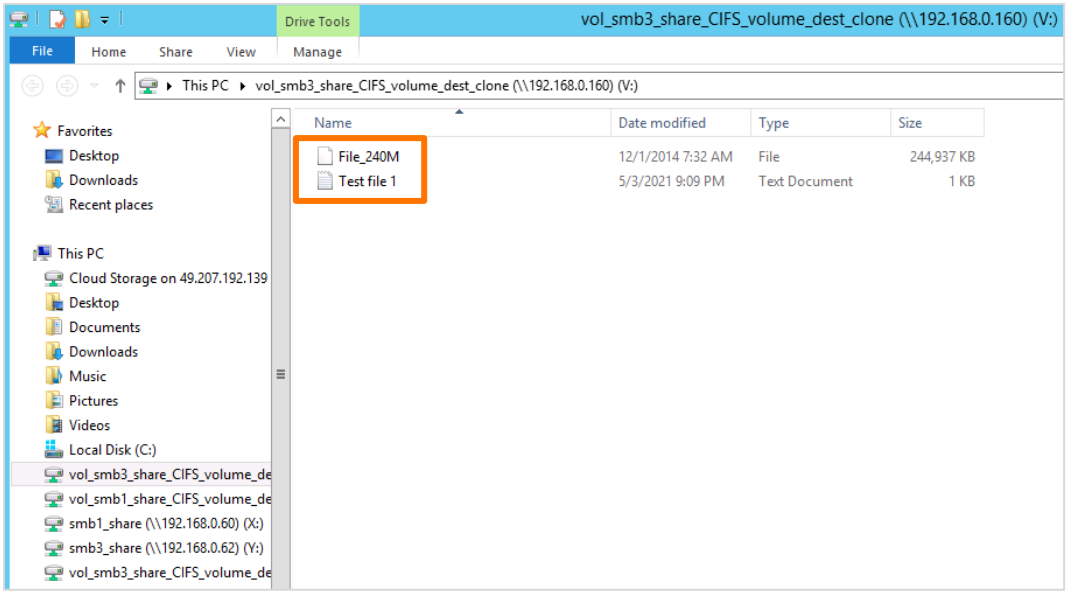
In this task, you use the unscheduled Snapshot copy as a base for the FlexClone volume.

Step	Action
3-1	**Cluster2** In the System Manager navigation pane, select **Storage** > **Volumes**.
3-2	In the Volumes pane, click the three vertical dots to the right of the SnapMirror destination volume vol_smb3_share_CIFS_volume_dest, and then select **Clone**. 

Step	Action
3-3	In the Clone Volume dialog box, select **Use an existing Snapshot copy**, select **snapshot_for_DR_testing** from the list of Snapshot copies, and then click **Clone**. 
3-4	On the Volumes pane, verify that the clone was created. 

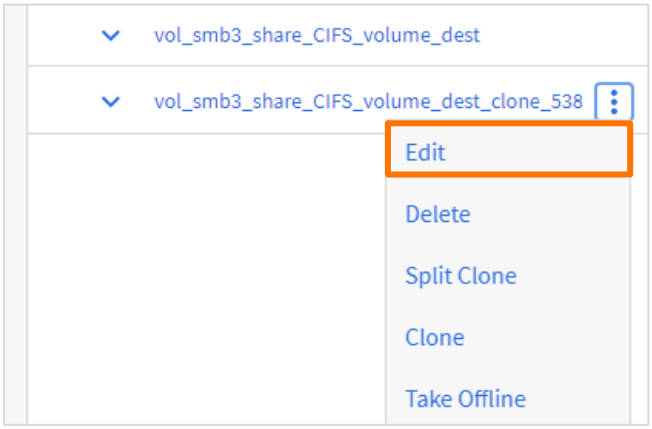
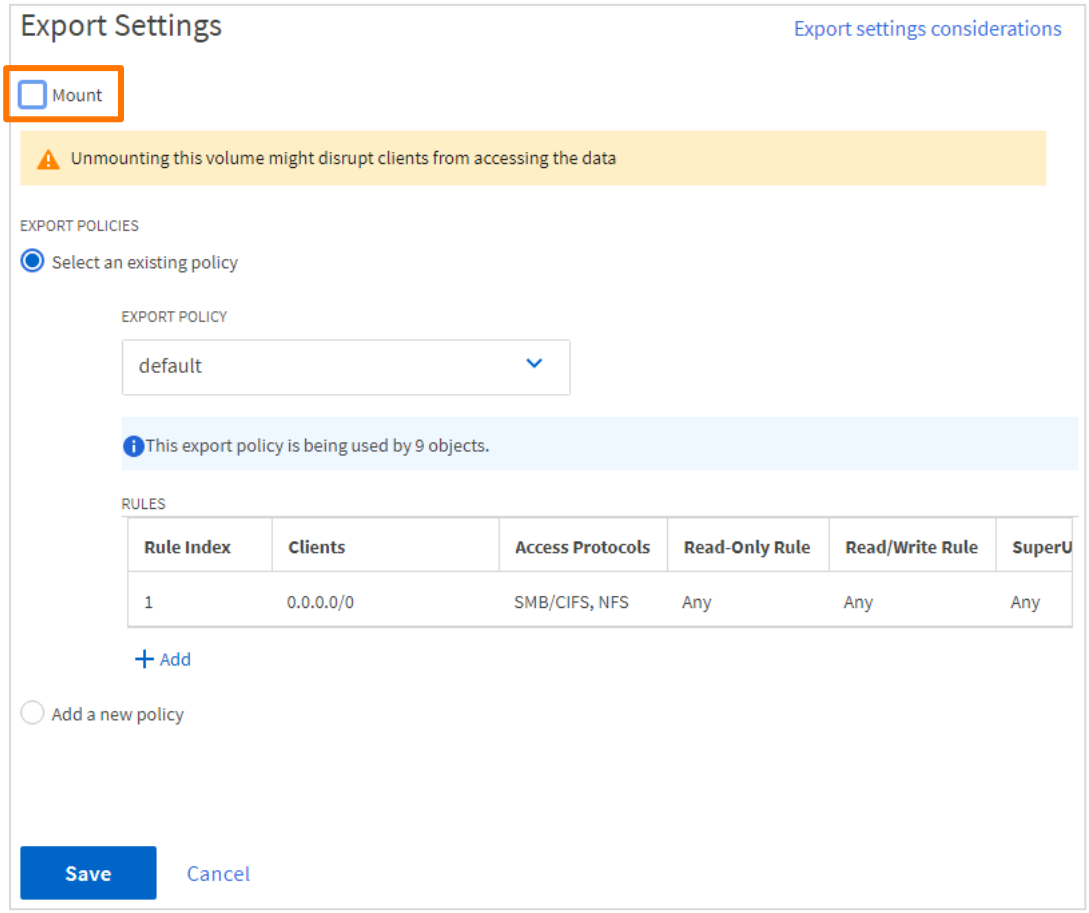
Step	Action
3-5	Next, on your Windows desktop, you map a drive to the cloned volume.
3-6	In the Volumes Pane, click the three vertical dots to the right of the clone volume, and select **Edit**. 
3-7	In the Edit Volume pane, scroll down to the Export Settings section, and then select the **Mount** checkbox. 
3-8	Click **Save**.
3-9	In the navigation pane, select **Storage** > **Shares**.

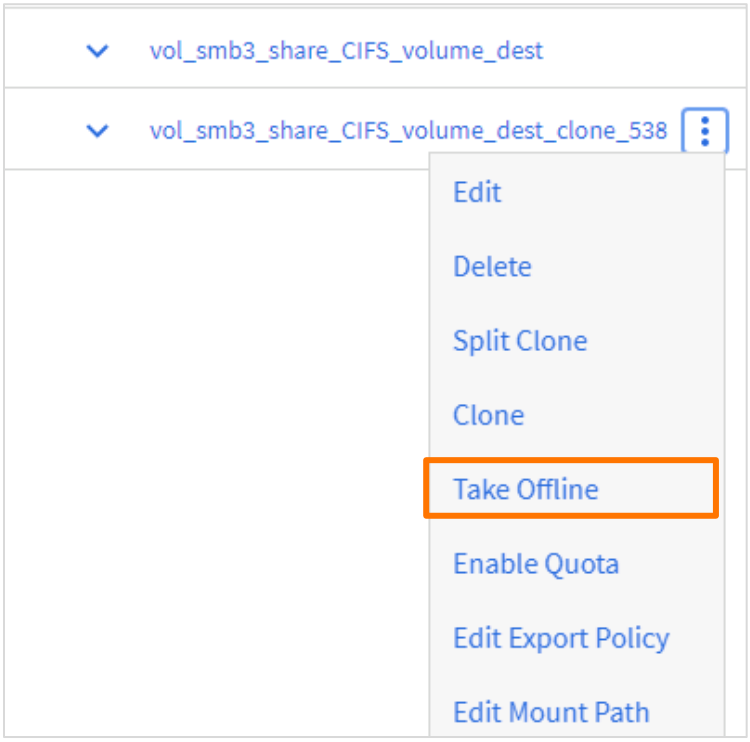
Step	Action
3-10	In the Shares pane, click **+Add**, and then select **Share**. 
3-11	In the Add Share pane, specify the following values: ▪ Share Name: **`vol_smb3_share_CIFS_volume_dest_clone`** ▪ Folder Name: **`/vol_smb3_share_CIFS_volume_dest_clone_538`** (Alternatively, click **Browse**, and then select the clone folder.) ▪ Description: *clear* 

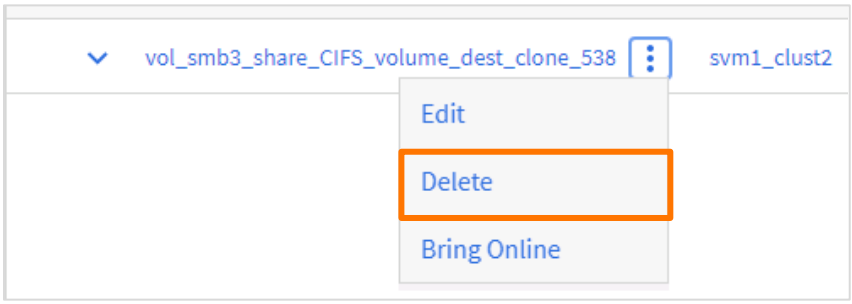
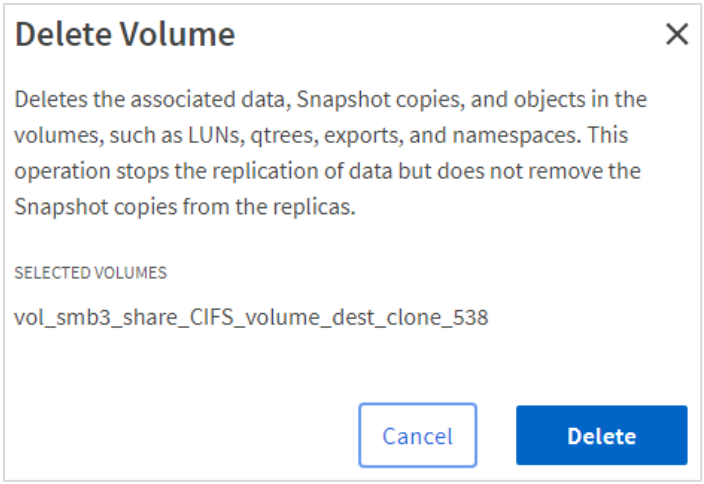
Step	Action
3-12	Click **Save** and verify that the new share is listed in the Shares pane.
3-13	On the jump host, use File Explorer to map a drive to the clone volume on cluster2\svm1_clust2. Use the folder path **\\192.168.0.160\vol_smb3_share_CIFS_volume_dest_clone**. 
3-14	Open the clone folder and verify that it contains the same two files that exist in the SnapMirror source and destination volumes. 
3-15	You can make changes to the clone. Try creating some files on the folder.

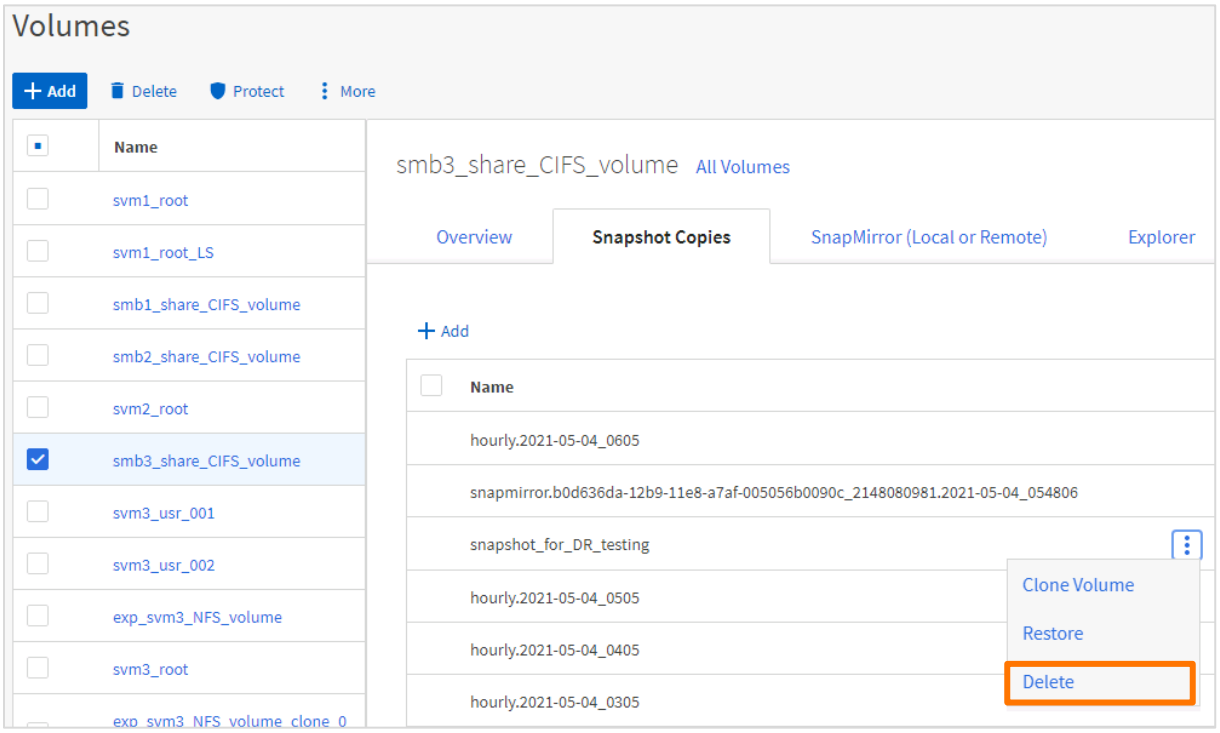
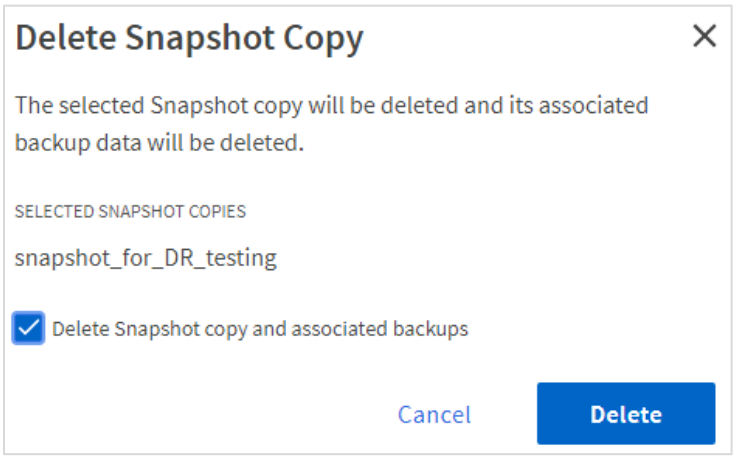
Task 4: Delete the Clone

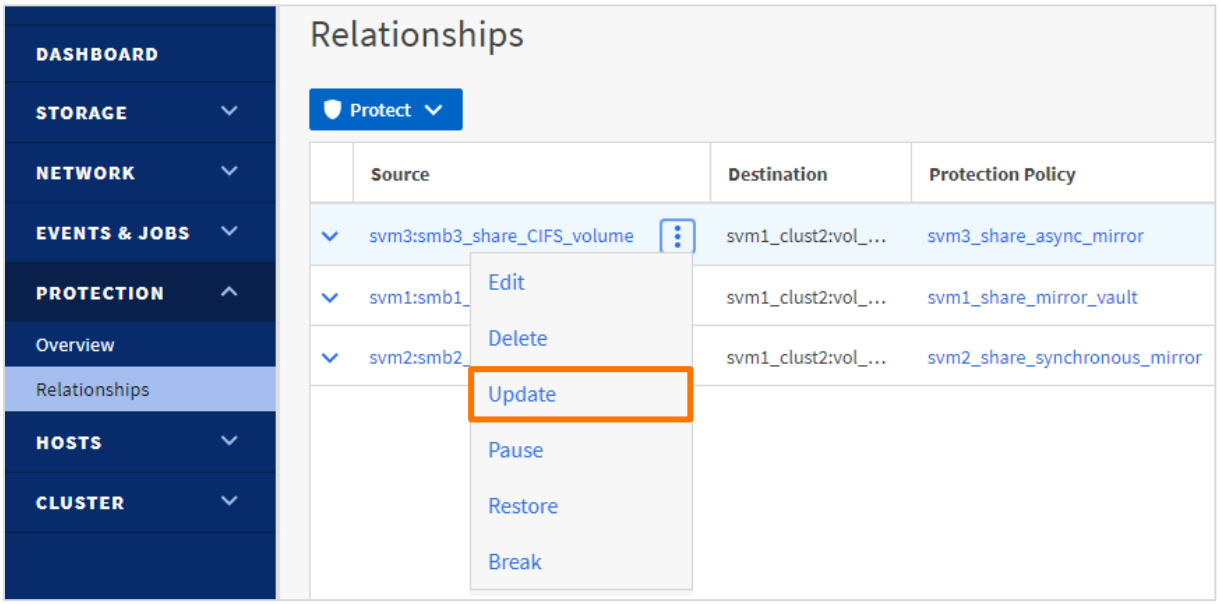
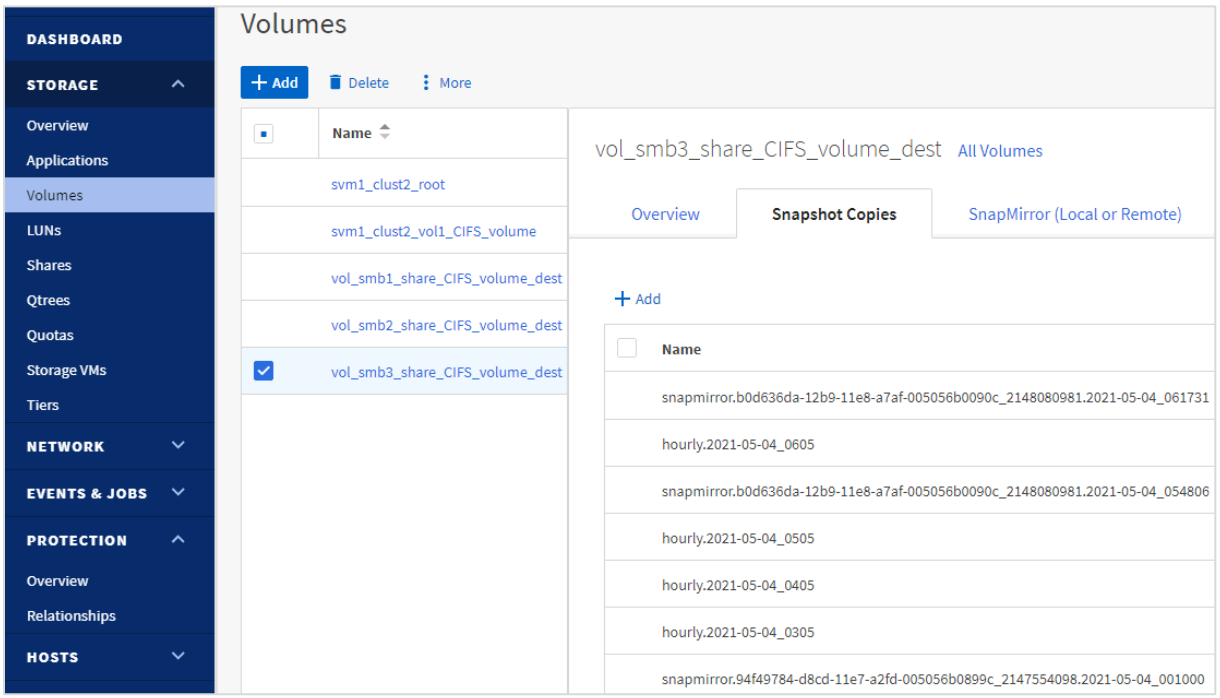
In this task, you take the FlexClone volume offline and delete the clone.

Step	Action
4-1	**Cluster2** In the System Manager navigation pane, select **Storage** > **Volumes**.
4-2	In the Volumes pane, click the three vertical dots to the right of the clone, and then select **Edit**. 
4-3	In the Edit Volume pane, scroll down to the Export Settings section, and then clear the **Mount** checkbox. 

Step	Action
4-4	Click **Save**.
4-5	To unmount the clone from the CLI, use the **`volume unmount`** command. Example: **`volume unmount -volume vol_smb3_share_CIFS_volume_dest_clone_538`**
4-6	In the Volumes pane, click the three vertical dots to the right of the clone, and then select **Take Offline**. 
4-7	Verify that the status of the clone is **Offline**, as signified by the red status icon. 
4-8	To take the clone offline from the CLI, use the **`volume offline`** command. Example: **`volume offline -volume vol_smb3_share_CIFS_volume_dest_clone_538`**
4-9	**Cluster2** In the System Manager navigation pane, select **Storage** > **Volumes**.

Step	Action
4-10	In the Volumes pane, click the three vertical dots to the right of the clone, and then select **Delete**. 
4-11	In the Delete Volume dialog box, review the provided information, and then click **Delete**. 
4-12	In this exercise, you created an unscheduled Snapshot copy on the SnapMirror source volume. SnapMirror replicated the Snapshot copy to the destination volume and used the copy for a FlexClone operation. After you delete the FlexClone volume, NetApp recommends that you delete the original Snapshot copy from the source volume.
4-13	**Cluster1** In the System Manager navigation pane, select **Storage** > **Volumes**.
4-14	Click the SnapMirror source volume **smb3_share_CIFS_volume**.

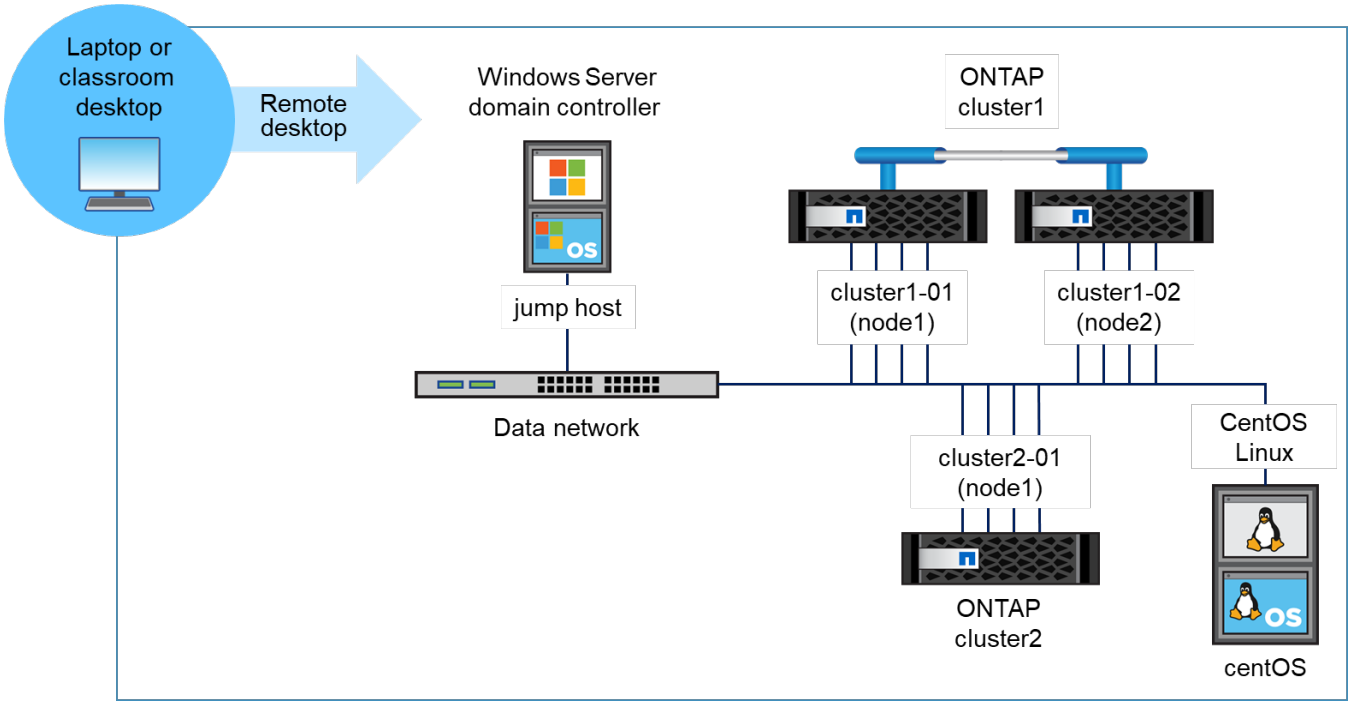
Step	Action
4-15	In the Snapshot Copies pane, click the three vertical dots to the right of the snapshot copy **snapshot_for_DR_testing**, and then select **Delete**. 
4-16	In the Delete Snapshot Copy dialog box, the **Delete Snapshot copy and associated backups** checkbox, and then click **Delete**. 
4-17	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.

Step	Action
4-18	Select the SnapMirror relationship for **smb3_share_CIFS_volume**, and then select **Update** to run a SnapMirror update as per policy. 
4-19	Review the SnapMirror destination volume vol_smb3_share_CIFS_volume_dest and determine whether the unscheduled Snapshot copy was deleted, as indicated by the absence of the snapshot_for_DR_testing Snapshot copy. 

End of exercise

Module 4: SVM DR

Exercise Equipment Diagram



System	Host Name	IP Addresses	User Name	Password
Windows Server 2012 R2	JUMPHOST	192.168.0.5	demo\Administrator	Netapp1!
ONTAP cluster-management LIF	cluster1	192.168.0.101	admin (case-sensitive)	Netapp1!
node 1	cluster1-01	192.168.0.111	admin (case-sensitive)	Netapp1!
node 2	cluster1-02	192.168.0.112	admin (case-sensitive)	Netapp1!
ONTAP cluster-management LIF	cluster2	192.168.0 102	admin (case-sensitive)	Netapp1!
node 1	cluster-01	192.168.0 113	admin (case-sensitive)	Netapp1!
Linux Server	centos65	192.168.0.21	root	Netapp1!

Exercise 1: Configuring SVM DR

In this exercise, you use NetApp ONTAP System Manager to configure a disaster-recovery relationship between two storage VMs (storage virtual machines, also known as SVMs) in different clusters. You can also use the ONTAP CLI to configure SVM DR. You use the svm3 SVM as the source SVM.

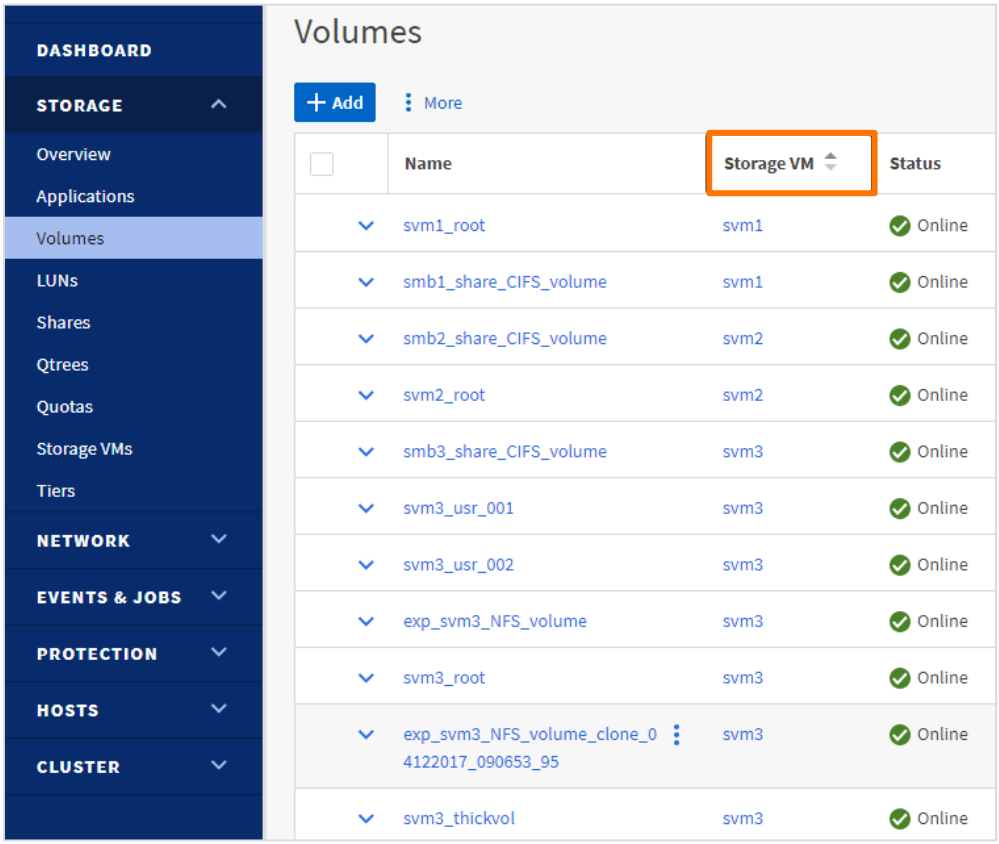
Objectives

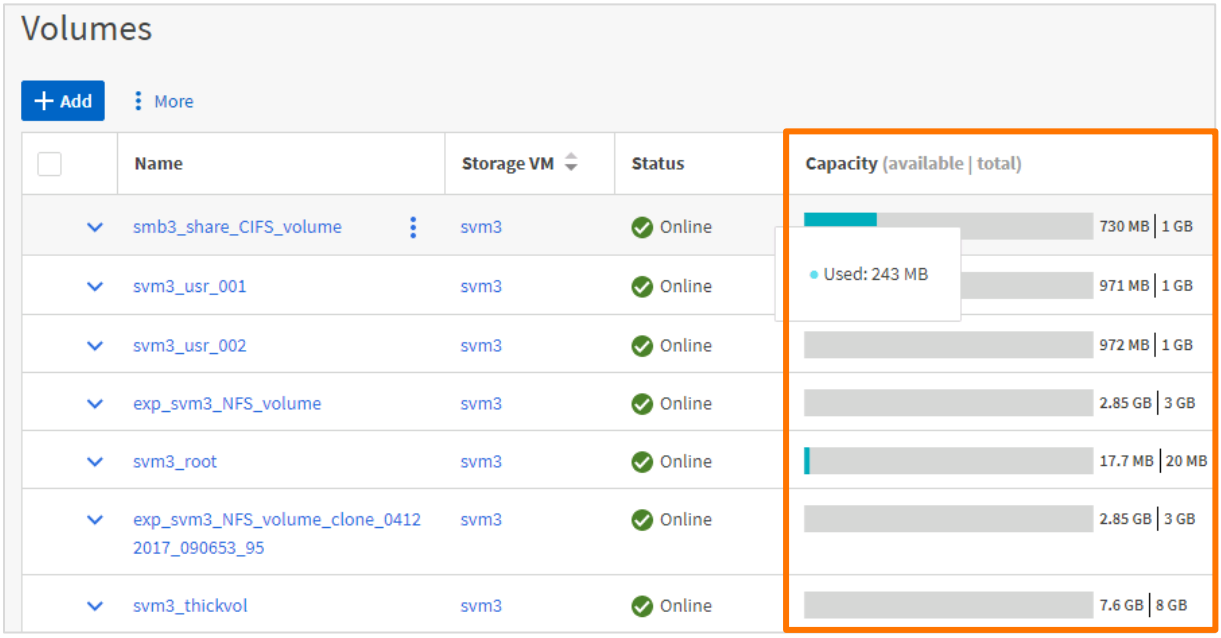
This exercise focuses on enabling you to do the following:

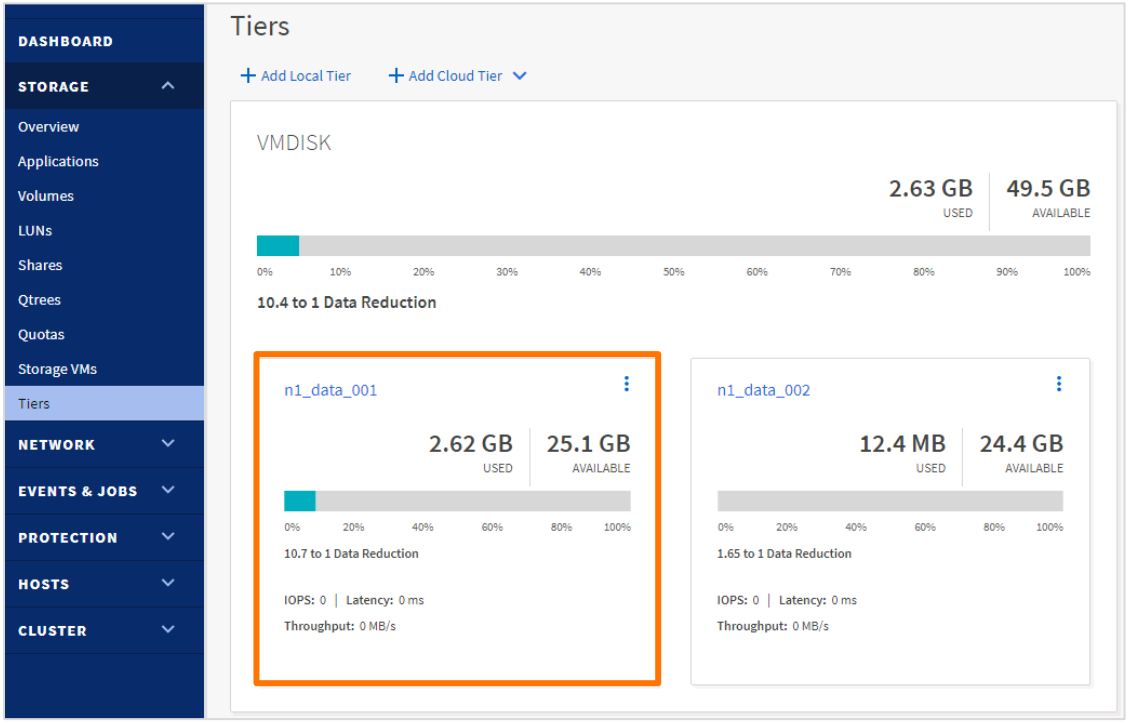
- Verify that space requirements are met
- Create an SVM DR policy
- Create an SVM DR relationship that protects SVM-scoped resources
- Fail over to the SVM on the disaster-recovery cluster and confirm data access
- Recover and resynchronize the primary source SVM

Task 1: Check Space Requirements

In this task, you examine the primary SVM svm3 for used space. You also examine the destination aggregates for free space.

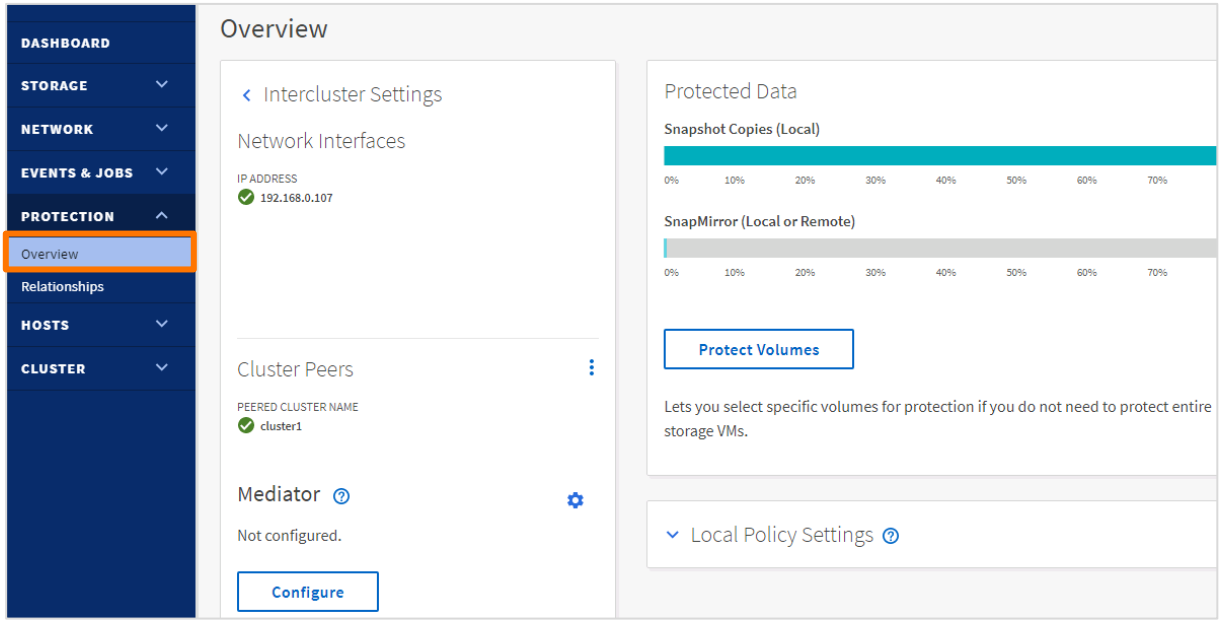
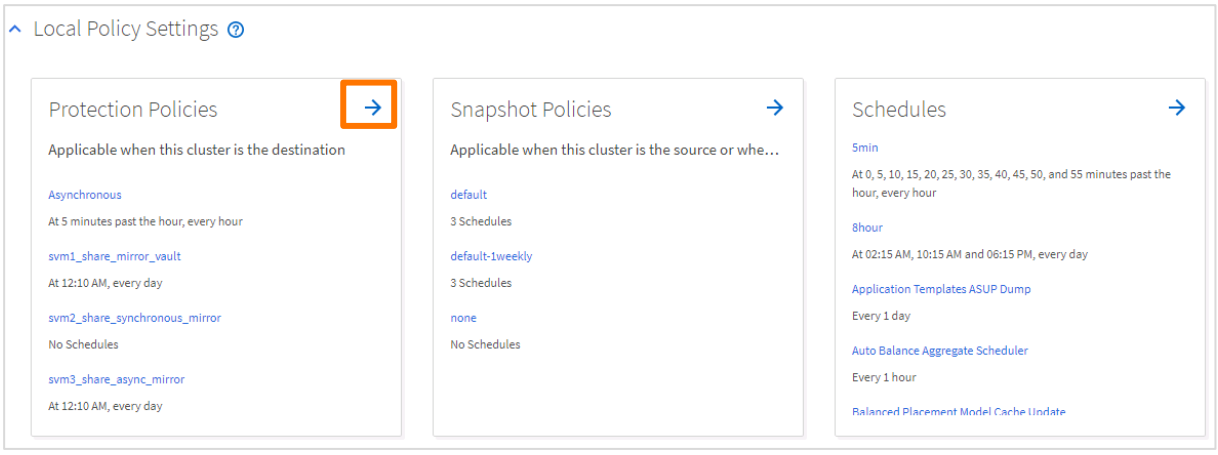
Step	Action
1-1	**Cluster1** In the System Manager navigation pane, select **Storage** > **Volumes**.
1-2	Click the **Storage VM** column to sort the SVMs by name. 

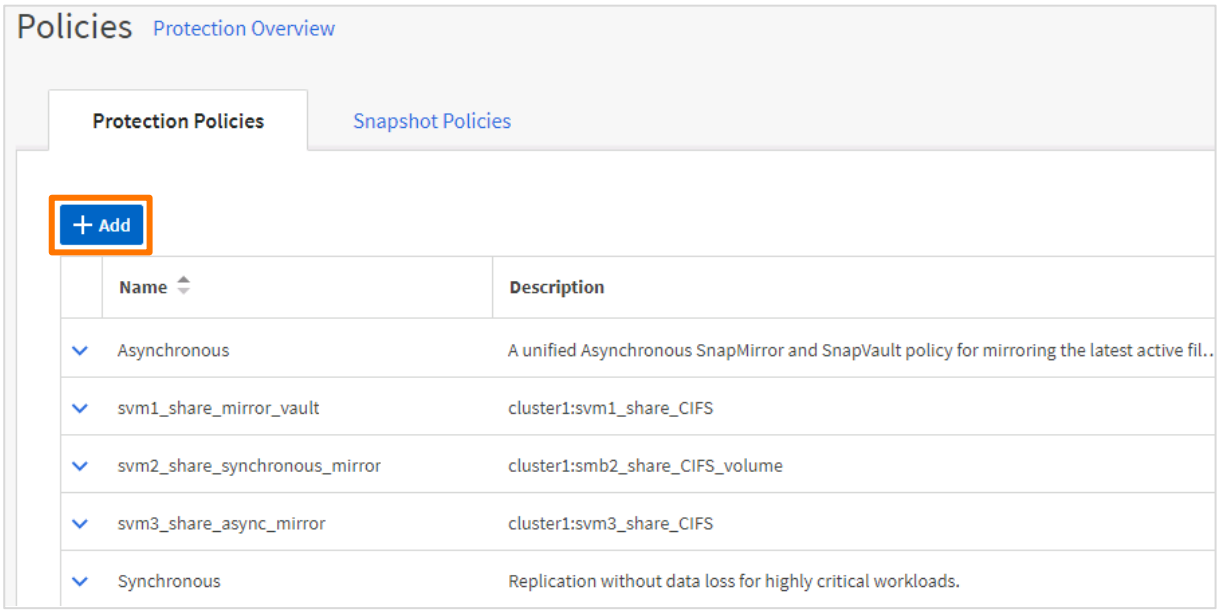
Step	Action
1-3	For each volume, you can view the total capacity, used capacity, and available capacity. To calculate the total aggregate size of the storage that is needed for the disaster-recovery cluster, review the used capacity in each volume in svm3.
1-4	For each volume in svm3, position your cursor over the capacity bar in the Capacity column and review the used capacity. 
1-5	To use the CLI to view the used capacity in all the volumes of svm3, run the **`volume show`** command: **`volume show -vserver svm3 -fields used`**
1-6	You must determine how much space is required for the disaster-recovery SVM. You must account for the space that the replicated volumes and SVM configuration data require. In a production environment, the SVM configuration data requires at least one non-root aggregate with a minimum of 10 GB of free space. The recommended practice for the SVM configuration data is to have at least two non-root aggregates, each with a minimum of 10 GB of free space.
1-7	**Cluster2** In the System Manager navigation pane, select **Storage** > **Tiers**.

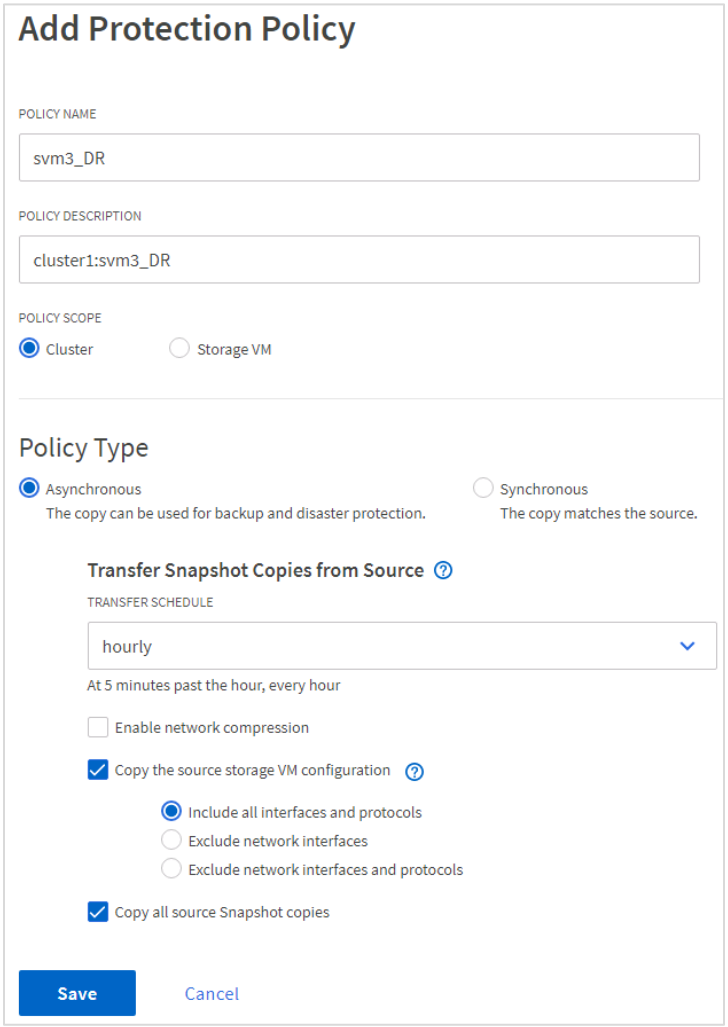
Step	Action
1-8	In the Tiers > VMDISK pane, verify that the **n1_data_001** aggregate can support the size of the volumes in svm3. 
1-9	To use the CLI to view the used and available capacity in the aggregates on cluster2, enter the **`storage aggregate show`** command: `cluster2::> storage aggregate show`

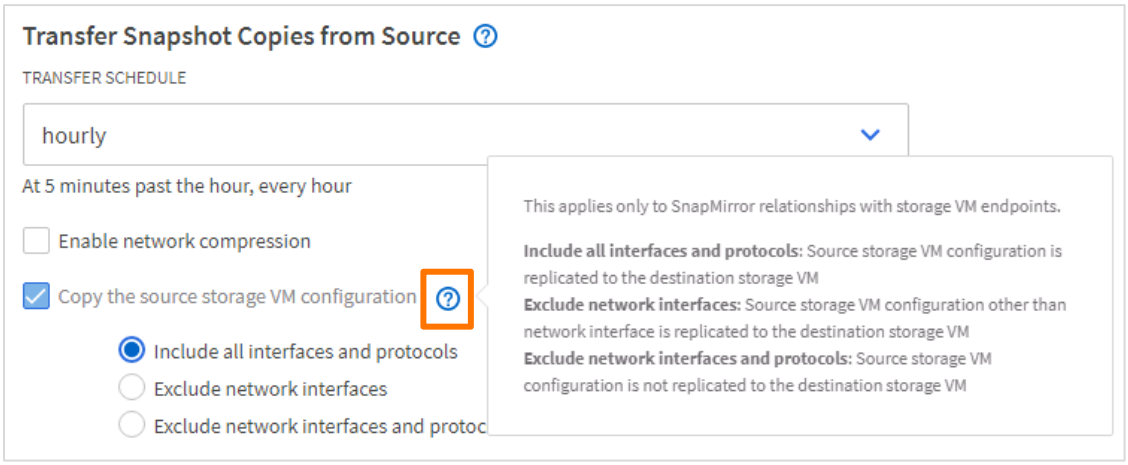
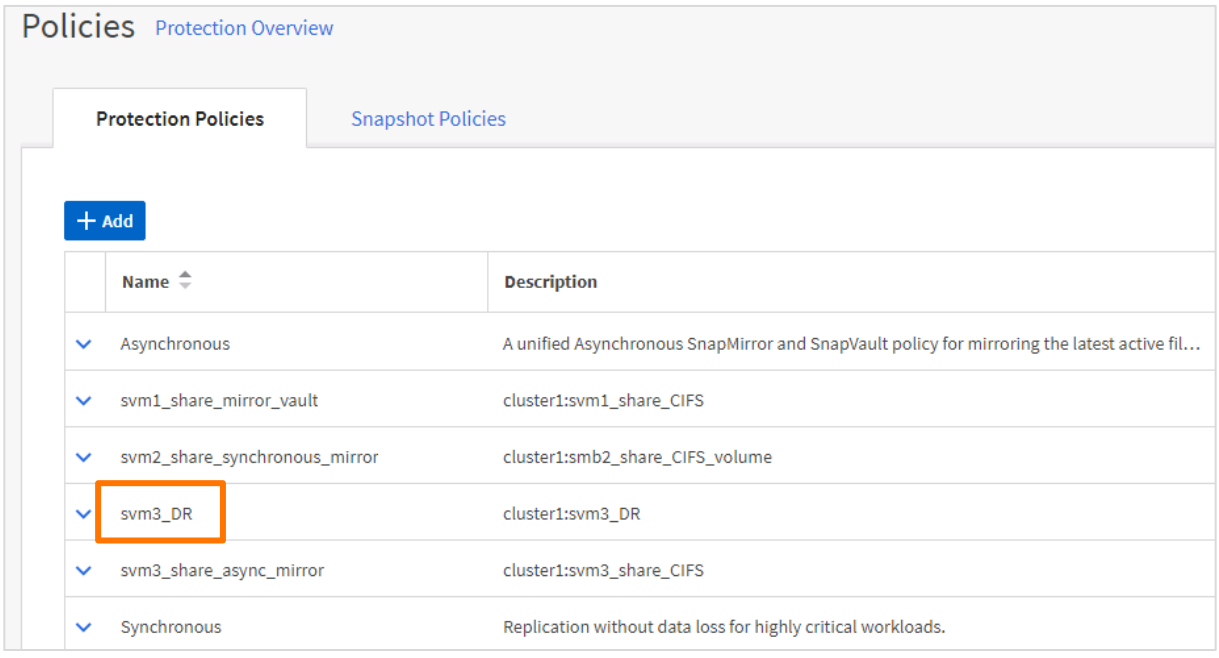
Task 2: Create an SVM DR Policy

In this task, you create a custom policy for your SVM DR relationship.

Step	Action
2-1	Cluster2 is the destination cluster for the protection relationship. You create the custom policy on the destination cluster.
2-2	**Cluster2** In the System Manager navigation pane, select **Protection** > **Overview**. 
2-3	In the Overview > Local Policy Settings pane, select **Local Policy Settings**, and then click the arrow in the upper-right corner of the **Protection Policies** box. 

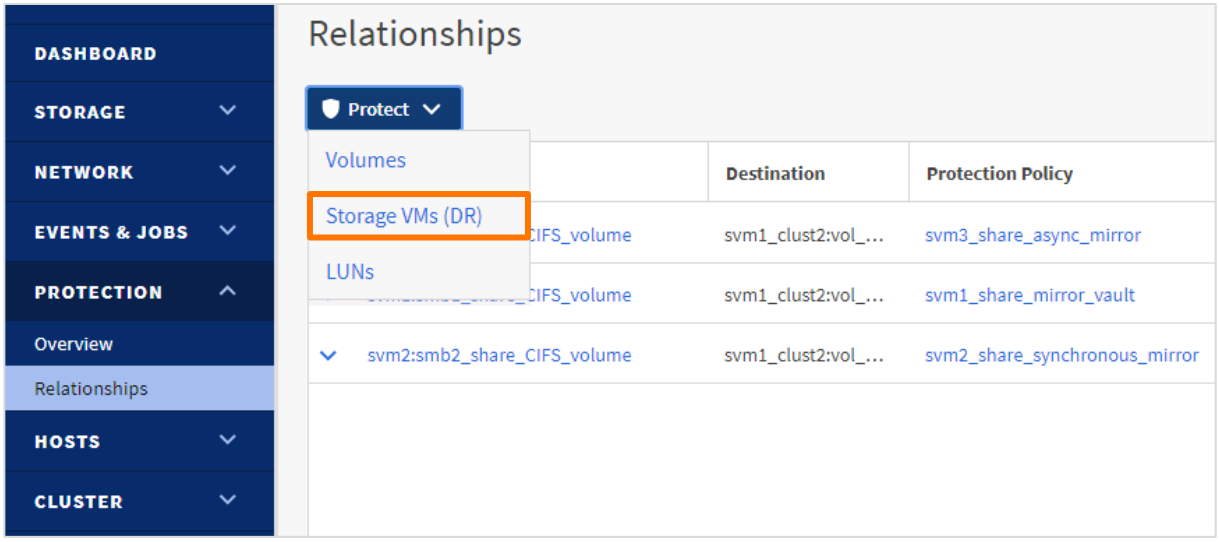
Step	Action
2-4	In the Policies > Protection Policies pane, click **+Add** to create a policy. 

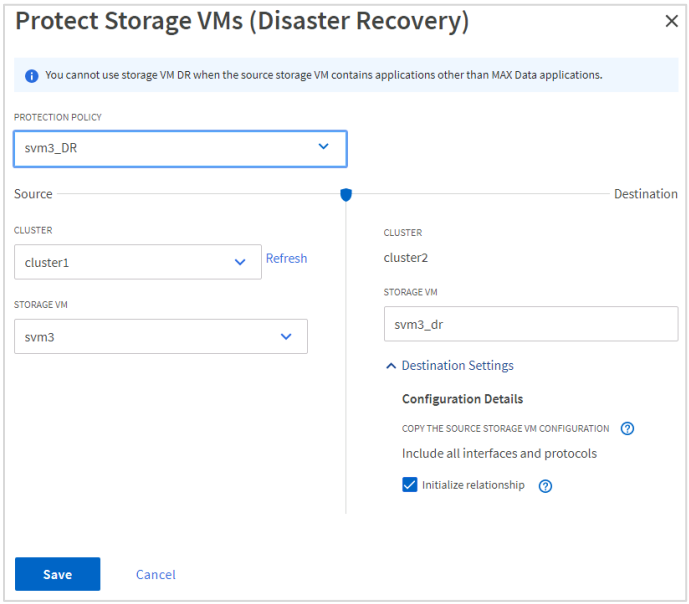
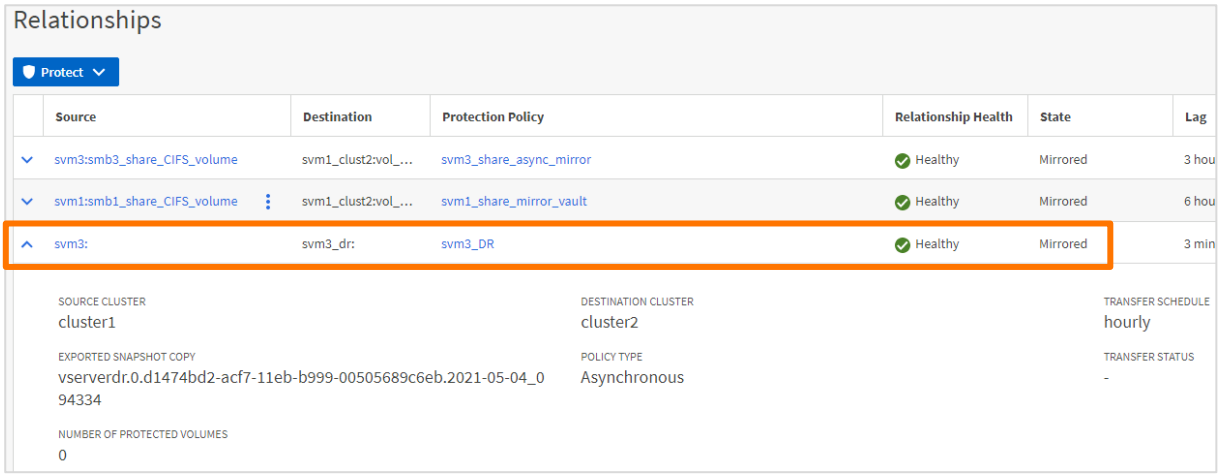
Step	Action
2-5	In the Add Protection Policy dialog box, specify the following values: ▪ Policy Name: **`svm3_DR`** ▪ Policy Description: **`cluster1:svm3_DR`** ▪ Policy Scope: **Cluster** ▪ Policy Type: **Asynchronous** ▪ Transfer Schedule: **hourly** ▪ Enable network compression checkbox: *clear* ▪ Copy the source storage VM configuration: *selected* ▪ Include all interfaces and protocols: *selected* ▪ Copy all source Snapshot copies: *selected* 

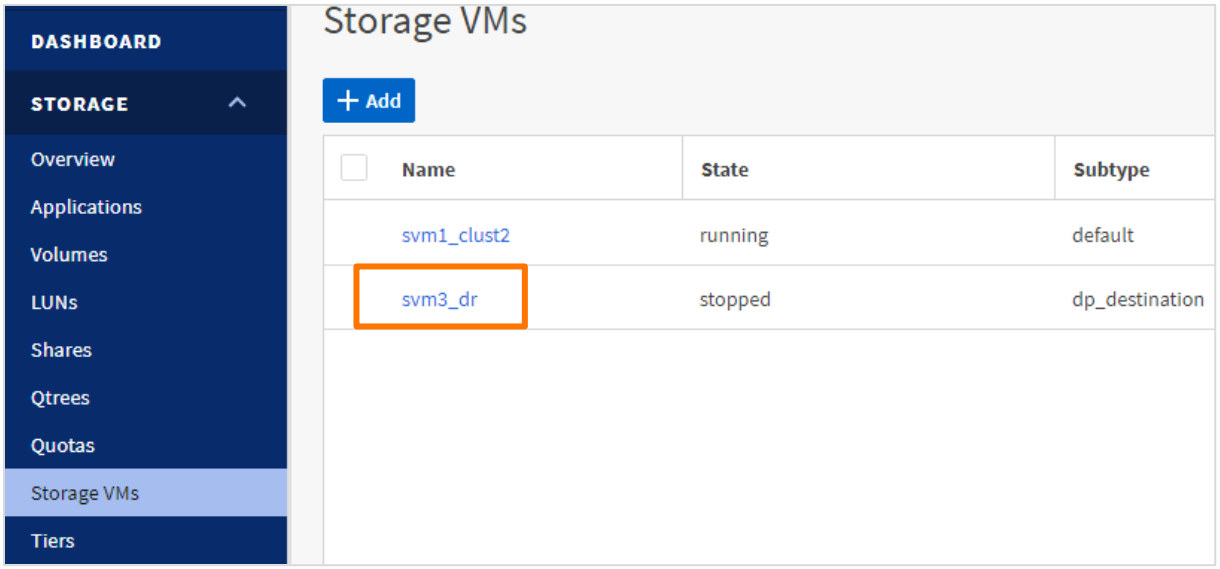
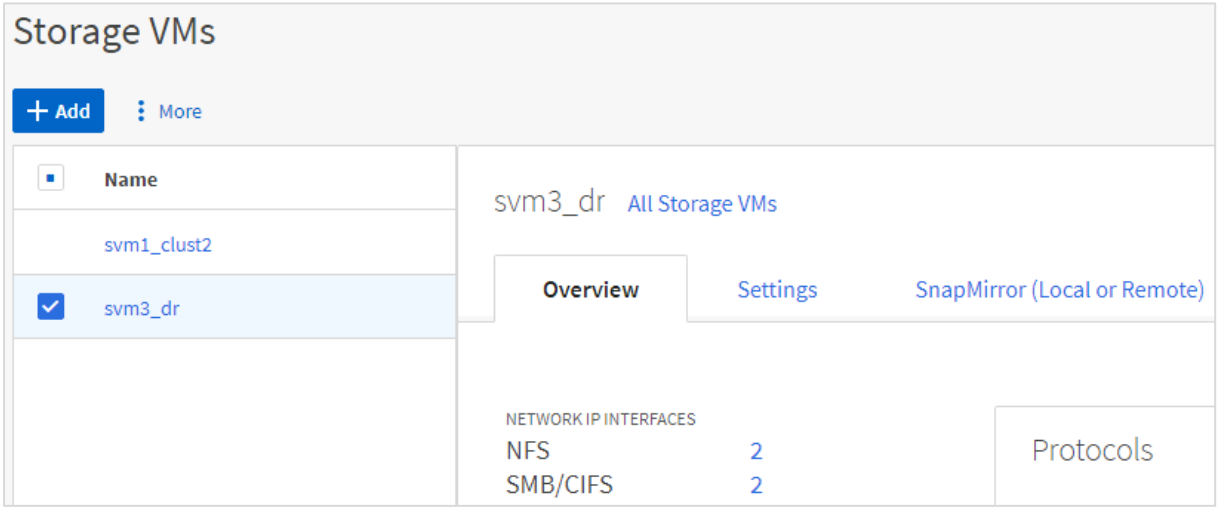
Step	Action
2-6	In the Add Protection Policy dialog box, position your cursor over the question mark to the right of the **Copy the source storage VM configuration** checkbox, and then review the information about data that is replicated when each sub-option is selected. 
2-7	The source and disaster-recovery clusters share a Layer 2 network. To preserve the network configuration that each client uses during a failover event, use identity-preserve mode. In some use cases for identity-preserve mode, the administrator might want to modify some network configuration settings after cutover.
2-8	Click **Save**.
2-9	Verify that the policy was created successfully. 

Task 3: Create an SVM DR Relationship

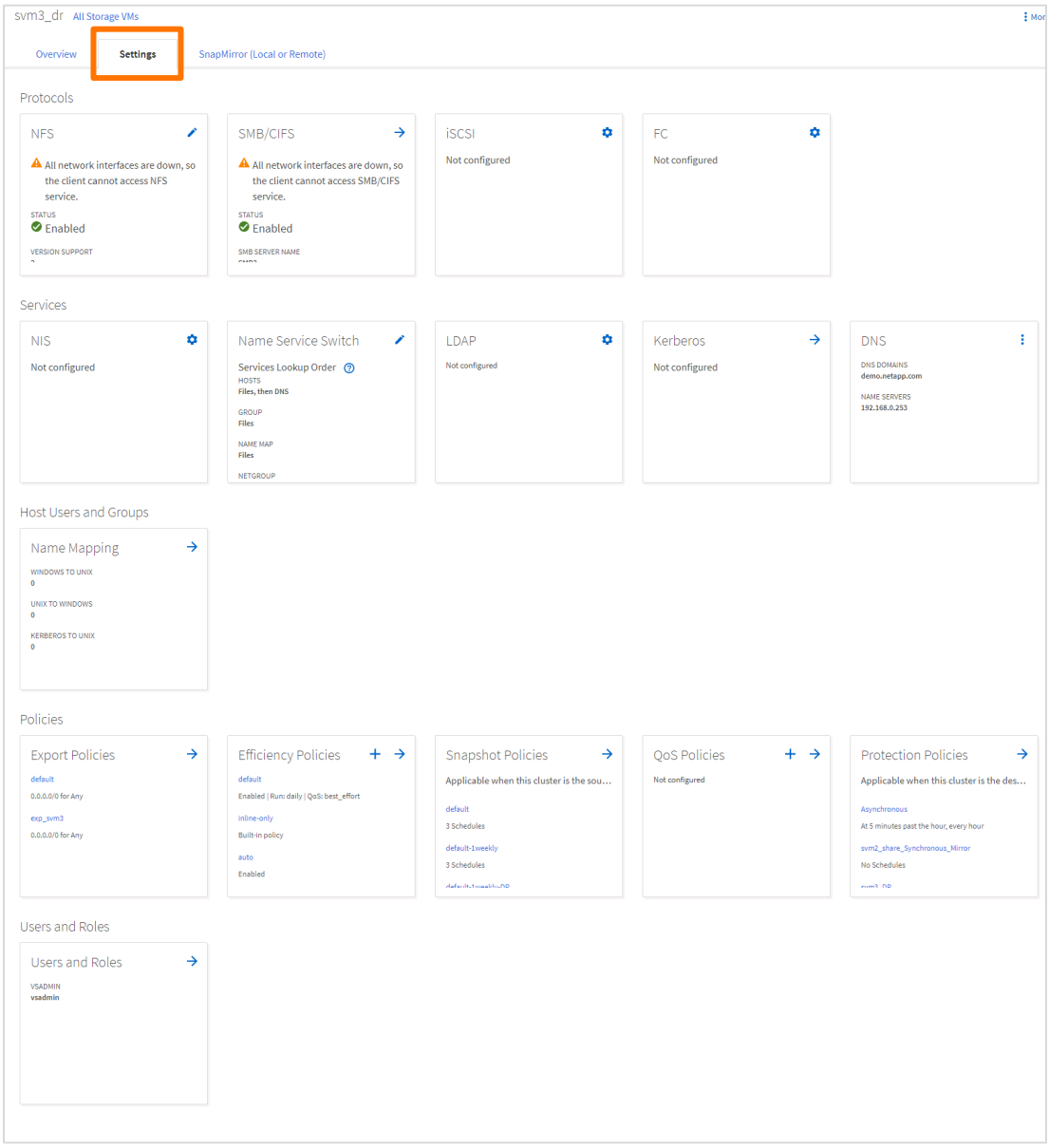
In this task, you create an SVM DR relationship between the primary SVM on cluster1 and a disaster-recovery SVM on cluster2.

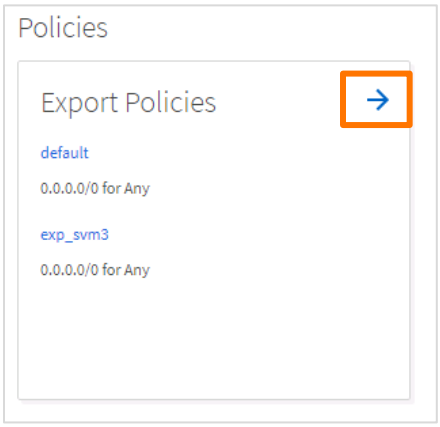
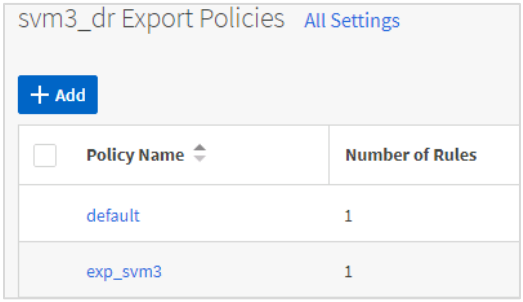
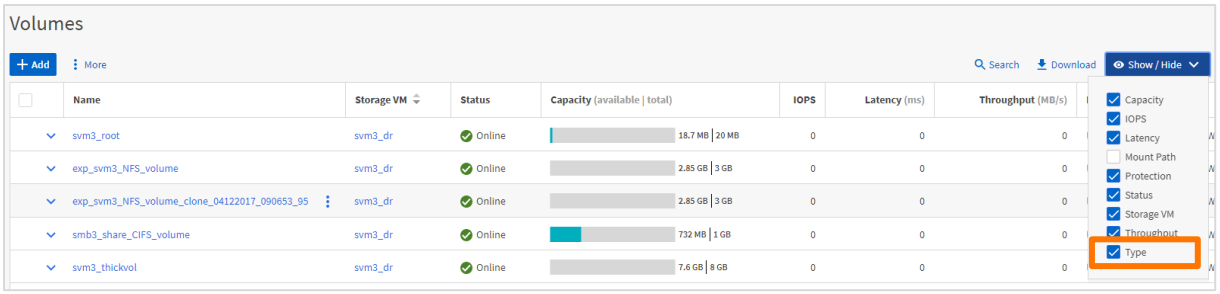
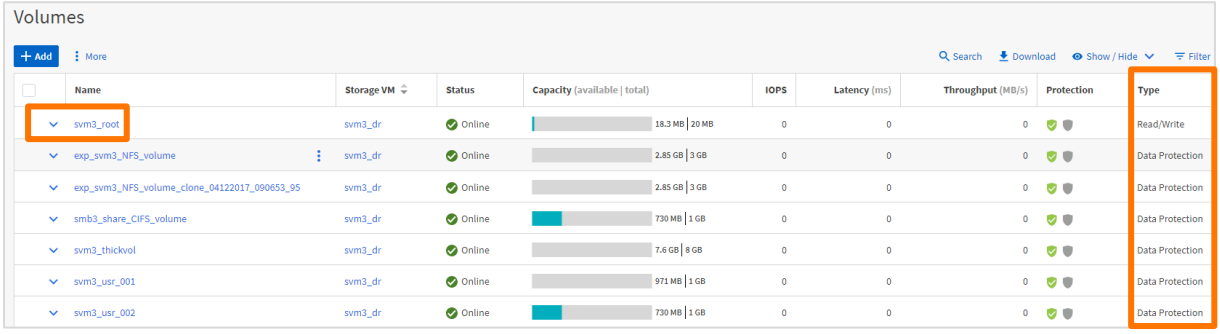
Step	Action
3-1	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.
3-2	Click **Protect**, and then select **Storage VMs (DR)**. 
3-3	In the next step, select the source SVM before you select the protection policy. Whenever you change the source SVM, the policy name changes to the default value.

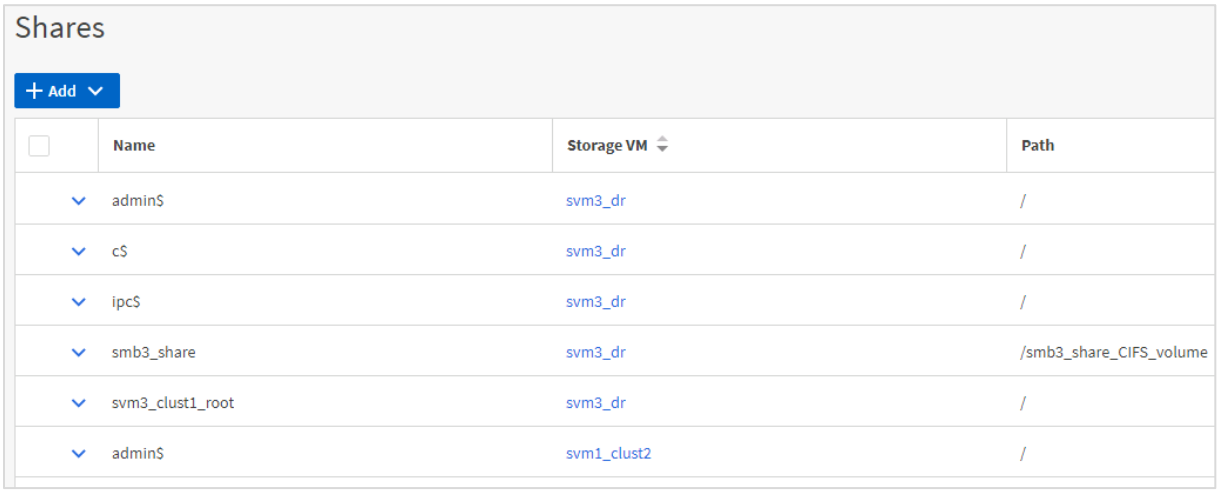
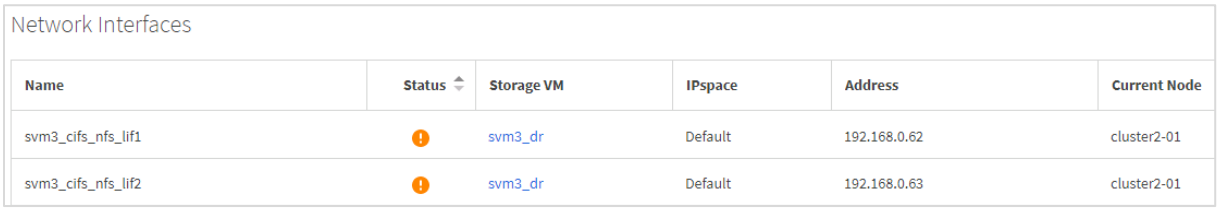
Step	Action
3-4	In the Protect Storage VMs (Disaster Recovery) pane, specify the following values: ▪ Protection Policy: **`svm3_DR`** ▪ Source > Cluster: **cluster1** ▪ Source > Storage VM: **svm3** ▪ Destination > Storage VM: **`svm3_dr`** 
3-5	Expand Destination Settings, and then review the information without changing anything.
3-6	Click **Save**.
3-7	In the Relationships pane, perform the following steps: a. Verify that the new SVM DR relationship is listed. b. Note how the source and destination are denoted. c. Verify that the state is Mirrored. d. Expand the relationship and note the listed details. 

Step	Action
3-8	In the System Manager navigation pane, select **Storage** > **Storage VMs**.
3-9	In the list, note that the newly created disaster-recovery SVM **svm3_dr** is in a stopped state and of Subtype **dp_destination**. 
3-10	Click **svm3_dr** to view the details and settings. 

Step	Action
3-11	Click **Settings** and examine all the settings listed for the SVM.



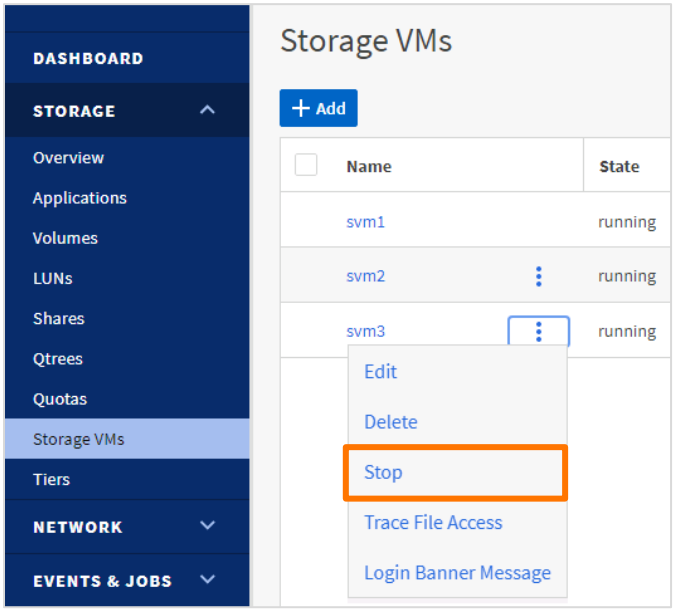
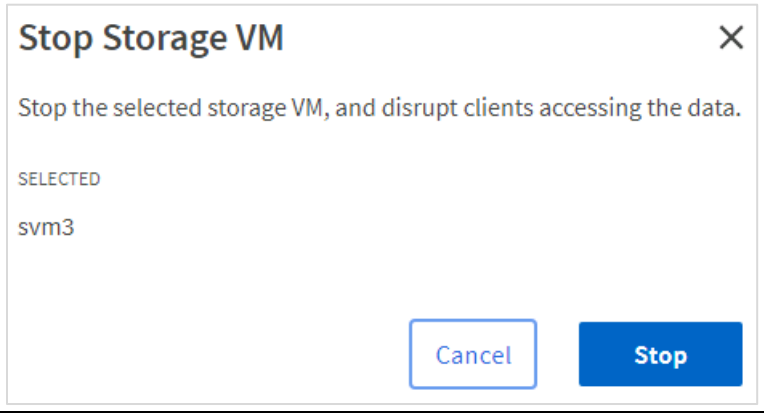
Step	Action
3-12	Scroll down to the **Policies** pane, and then in the **Export Policies** box, click the arrow in the upper-right corner. 
3-13	Examine the export-policy rules of the svm3_dr SVM. 
3-14	In the System Manager navigation pain, select **Storage** > **Volumes**.
3-15	At the top of the Volumes list, click **Show/Hide**, and then select **Type** to view the Type column. 
3-16	Verify that all the source volumes are copied and are of type **Data Protection** and that a new root volume is created automatically for the SVM. 

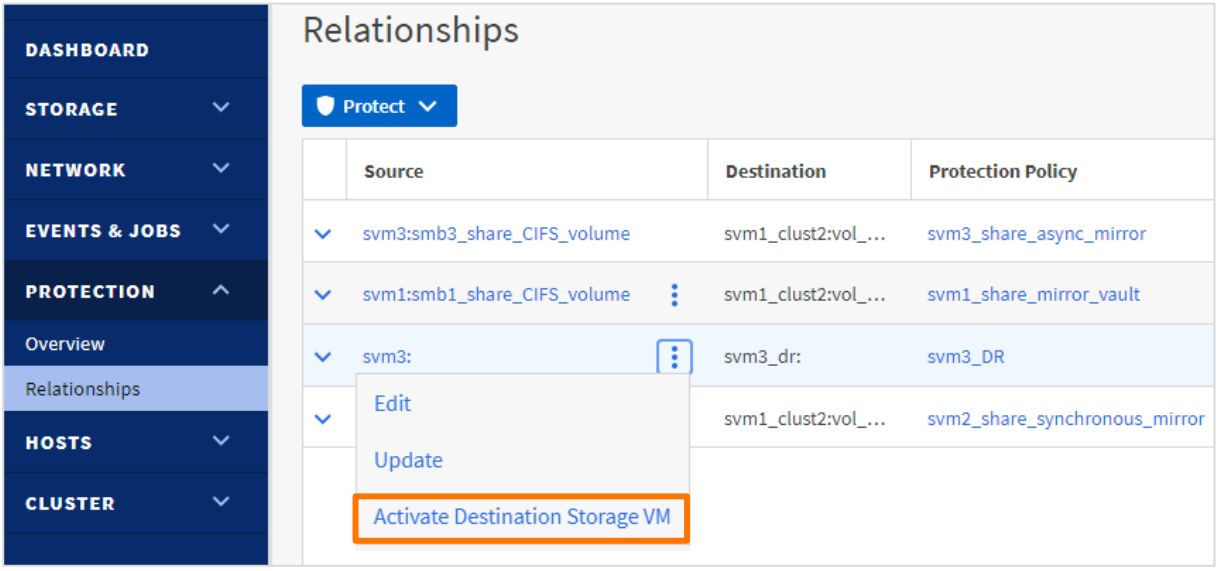
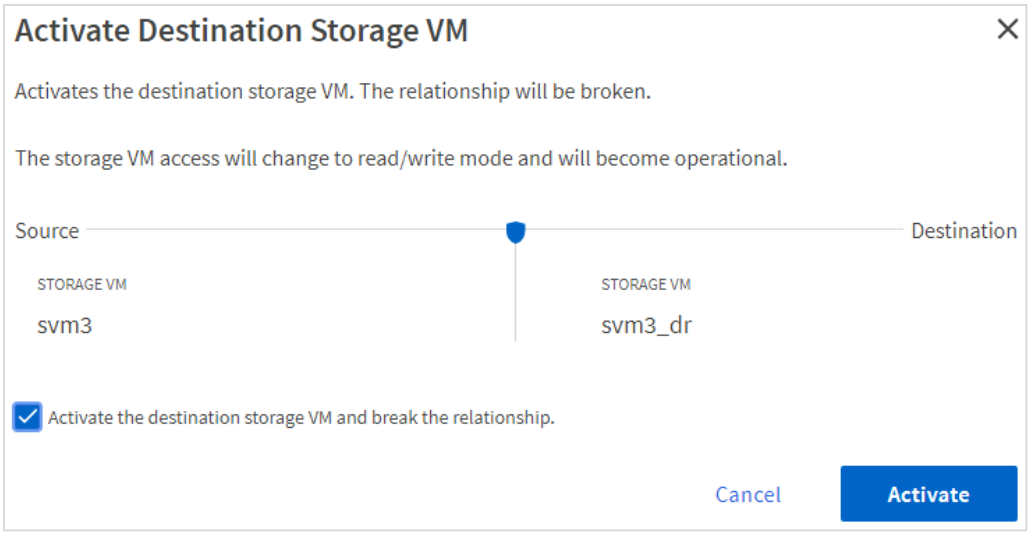
Step	Action
3-17	In the System Manager navigation pane, select **Storage** > **Shares**.
3-18	Examine the shares of the SVM svm3_dr. 
3-19	In the System Manager navigation pane, select **Network** > **Overview**.
3-20	Examine the data LIFs of the SVM svm3_dr. 
3-21	The data LIF should have the same IP address and network mask as the SVM svm3 on the primary cluster. However, the home port for the LIF might differ from the home port on the source cluster and from what is shown in this guide. The SnapMirror SVM feature makes a best effort at LIF placement and has its own set of rules for LIF home-port selection. From the disaster-recovery SVM, you cannot access or view the contents of the shares and volumes, because you are using identity-preserve mode. If you need to access the data in a read-only capacity while the primary cluster actively serves data, you must set identity-preserve mode to false.

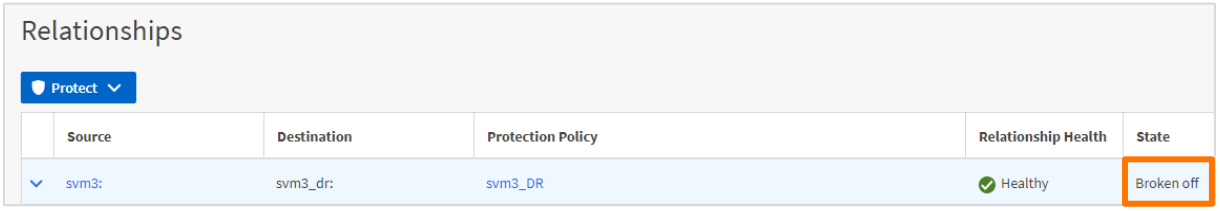
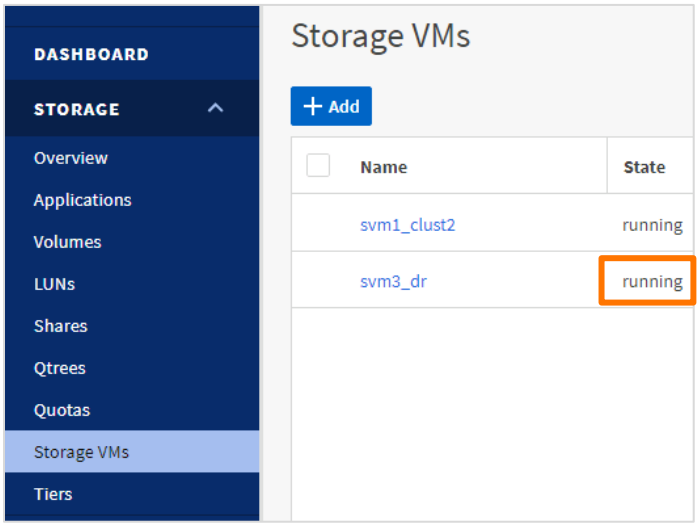
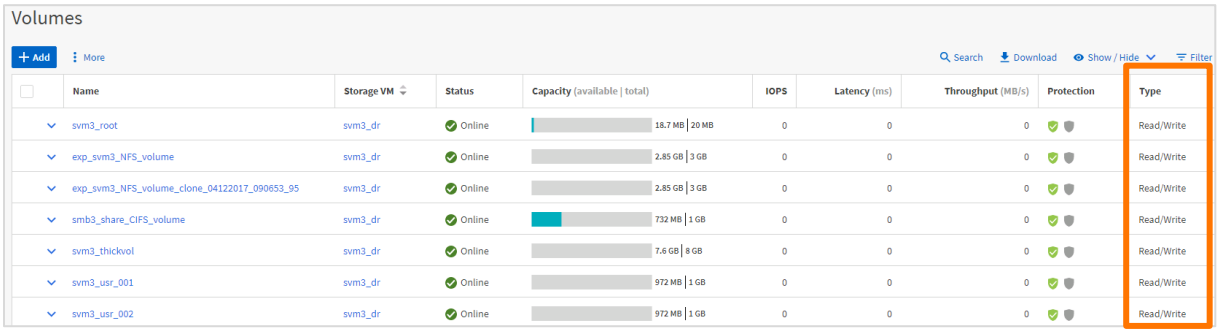
Task 4: Fail Over to the Disaster-Recovery SVM

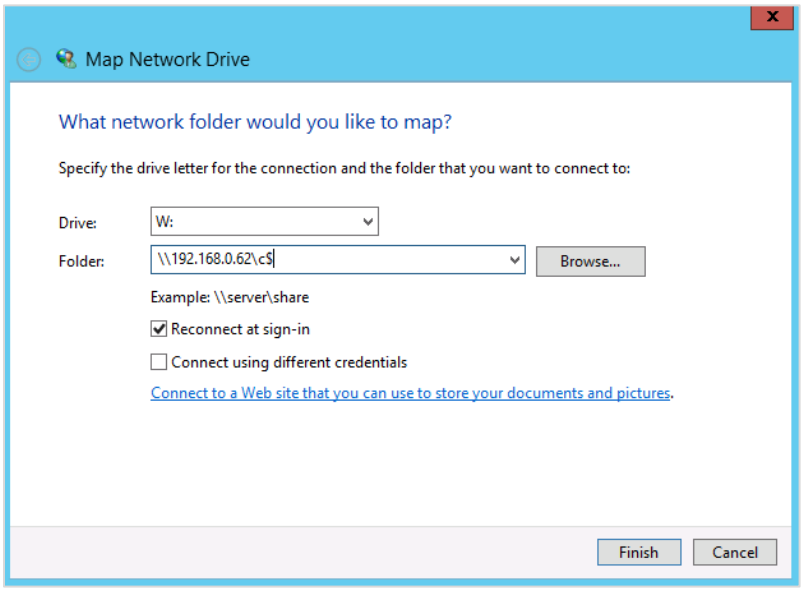
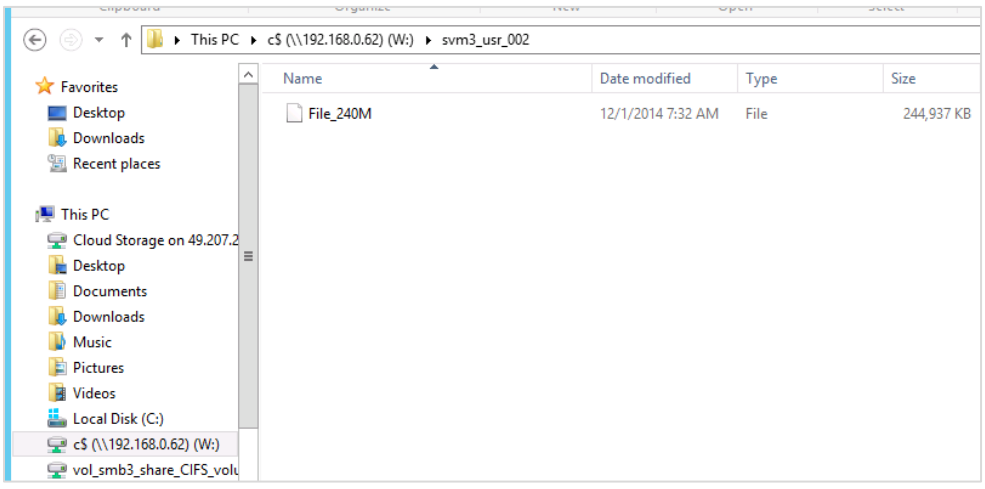
In this task, you recover a system from a disaster on the primary cluster by activating the disaster-recovery SVM. This activation involves the following steps:

1. Stopping the primary SVM
2. Starting the disaster-recovery SVM
3. Verifying the status of the disaster-recovery SVM

Step	Action
4-1	This exercise uses identity-preserve mode for the SnapMirror SVM relationship, and the primary and disaster-recovery SVMs are on the same network subnet. Therefore, you must stop the source SVM before you activate the destination SVM.
4-2	**Cluster1** In the System Manager navigation pane, select **Storage** > **Storage VMs**.
4-3	Click the three vertical dots to the right of svm3, and then select **Stop**. 
4-4	In the Stop Storage VM dialog box, click **Stop**. 
4-5	In the Storage VMs list, verify that the SVM is stopped.

Step	Action
4-6	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.
4-7	In the Source column, click the three vertical dots to the right of svm3, and then select **Activate Destination Storage VM**. 
4-8	In the Activate Destination Storage VM dialog box, select the checkbox, and then click **Activate**. 
4-9	This action breaks the SVM DR relationship, and the SVM svm3_dr starts serving data to clients.

Step	Action
4-10	In the **Relationships** pane, verify that the SVM DR relationship is in the Broken off state. 
4-11	In the System Manager navigation pane, select **Storage** > **Storage VMs** and verify that the SVM **svm3_dr** is in a running state. 
4-12	In the navigation pane, select **Storage** > **Volumes** and verify that the type of the volumes has changed from type **Data Protection** to type **Read/Write**. 
4-13	Because the primary and disaster-recovery SVMs use the same subnet, the LIFs do not need to be updated. When the SVM is activated, the clients can access the SMB share. You verify client access in the following steps.
4-14	To access the volumes from the disaster-recovery SVM, you must unmount and remount NFS clients.

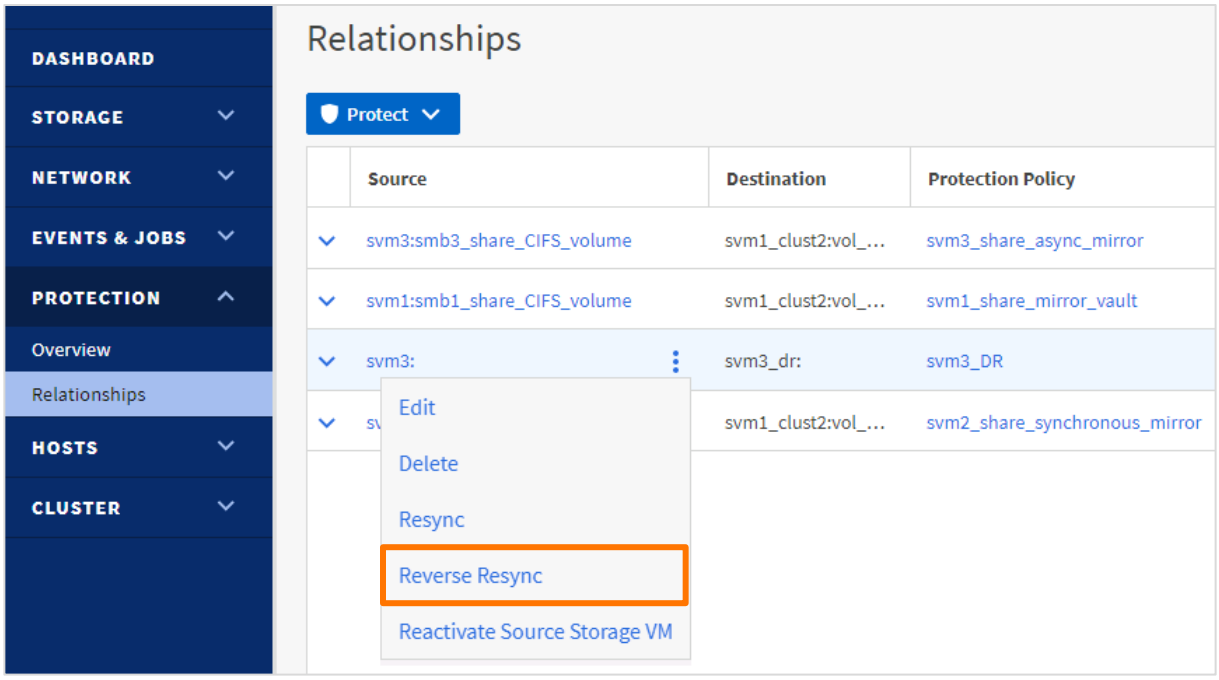
Step	Action
4-15	On the Windows Server desktop, use File Explorer to map a drive letter to the CIFS share on svm3_dr on cluster2 (Folder \\192.168.0.62\c$). 
4-16	The c$ share is the administrative hidden share of the namespace root. You should see folders that represent the junction paths to the other volumes that are involved in the SVM disaster-recovery SnapMirror relationship.
4-17	In File Explorer, double-click the **svm3_usr_002** folder, which accesses the svm3_usr 002 volume.
4-18	To verify that you can write data to the volume, copy File_240M from the CourseFiles folder to the svm3_usr_002 folder. 

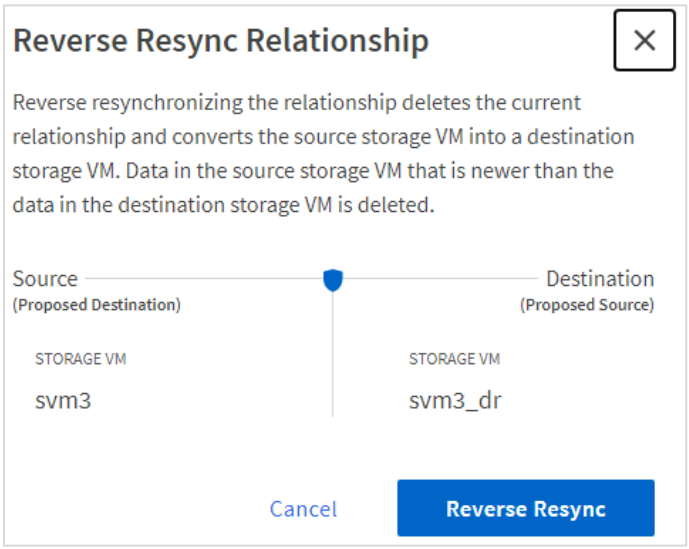
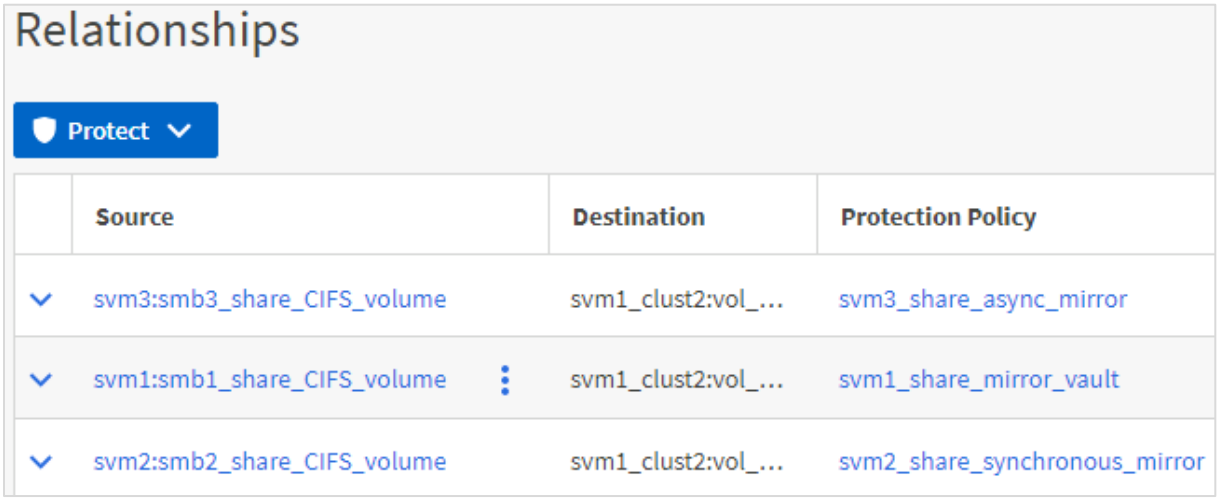
Task 5: Reactivate the Source SVM

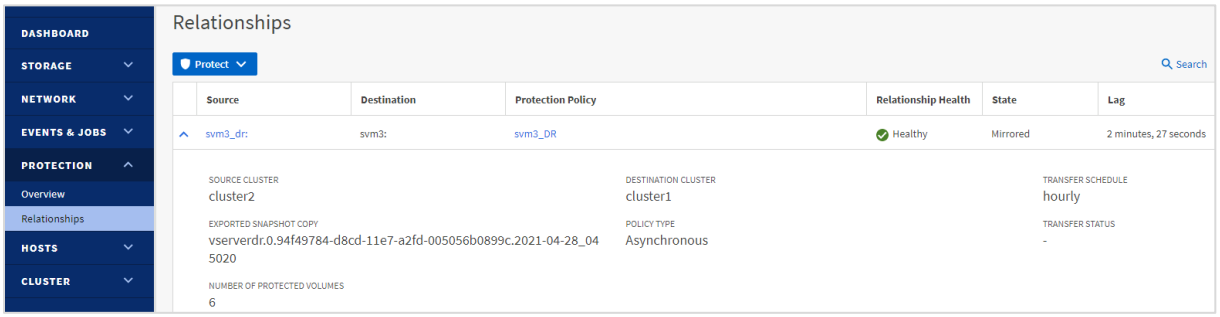
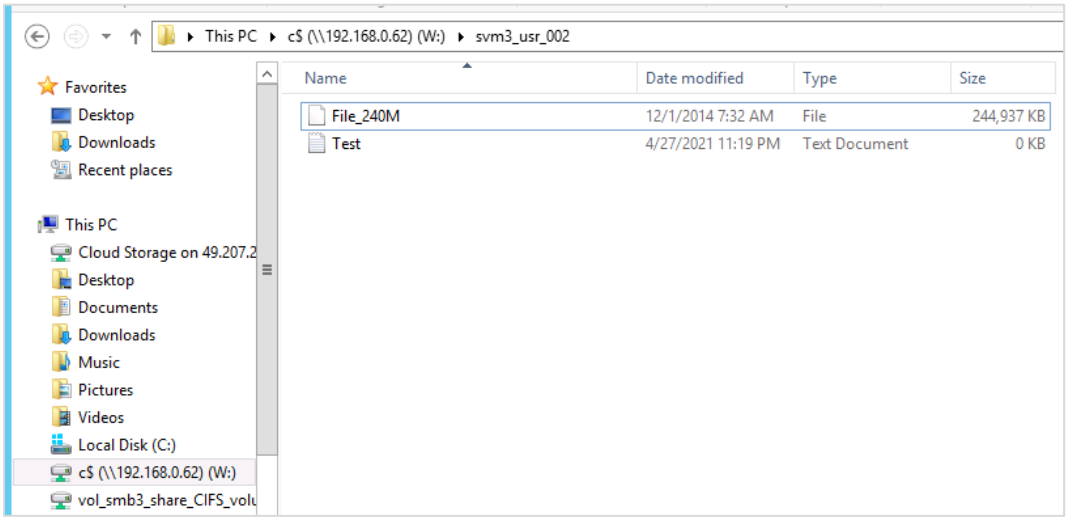
In this task, you activate the source SVM. For these activities, assume that the source SVM is recoverable. You must plan carefully because a short client outage occurs during switchback. During the reverse relationship, an administrator might also apply SVM configuration changes that are based on new business requirements.

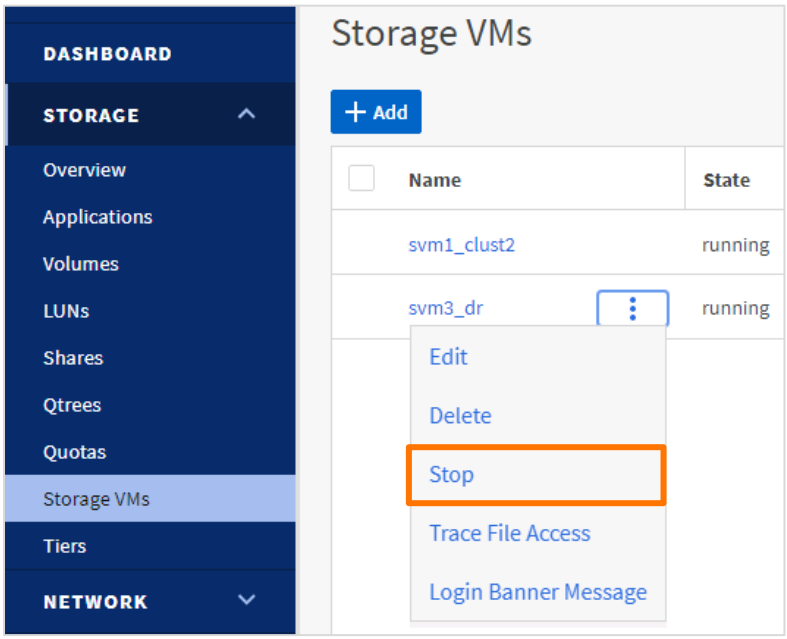
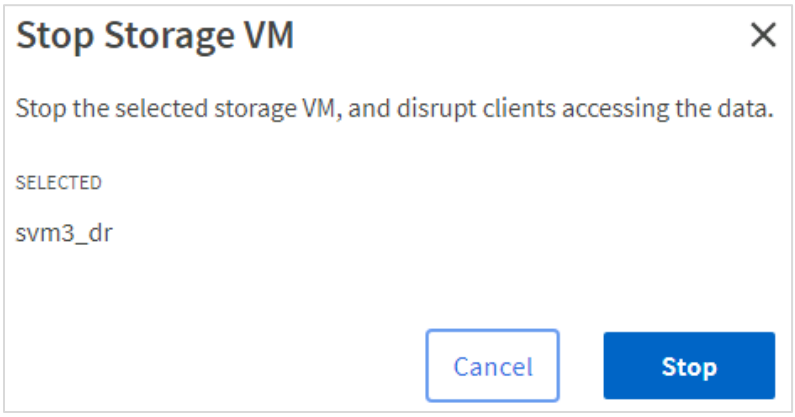
To reactivate the source SVM, follow these steps:

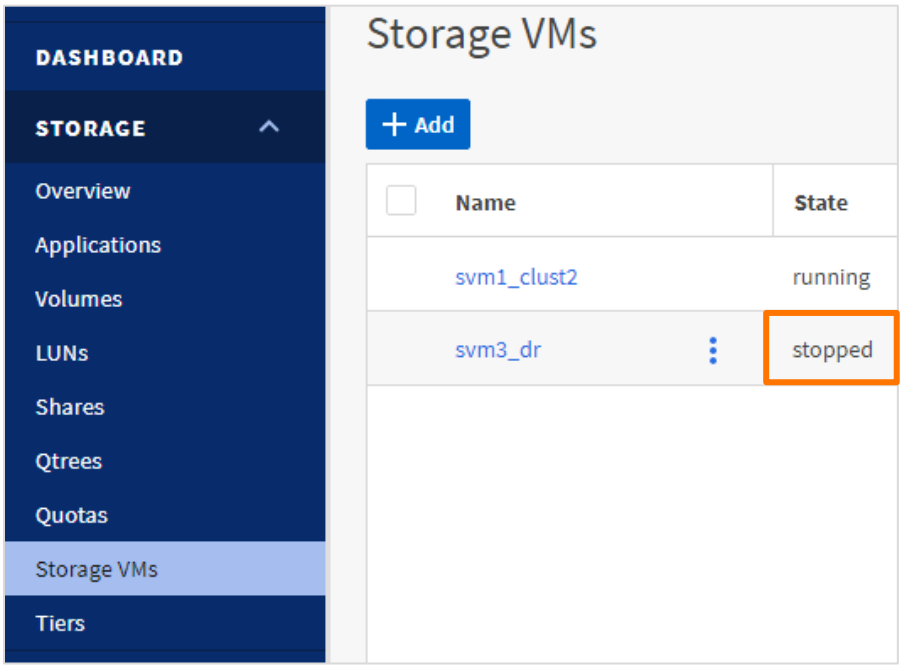
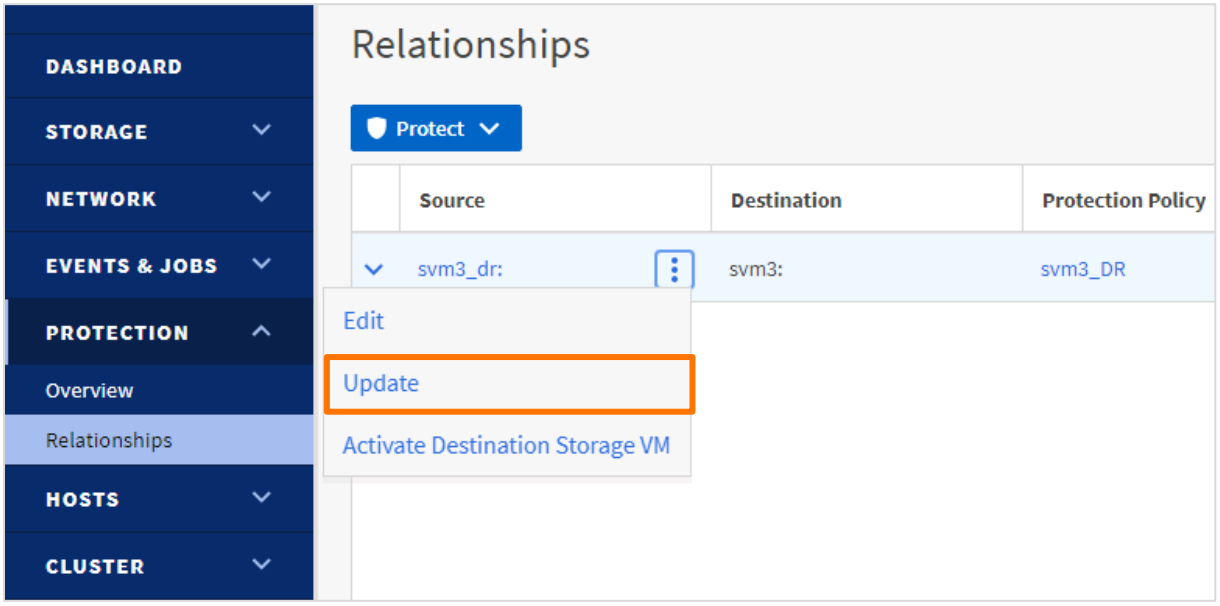
1. Resynchronize the source SVM from the destination SVM (reverse resync).
2. Stop the destination SVM.
3. Update the SnapMirror relationship from the source SVM.
4. Activate the destination SVM from the source SVM.
5. Resynchronize the destination SVM from the source SVM (reverse resync).

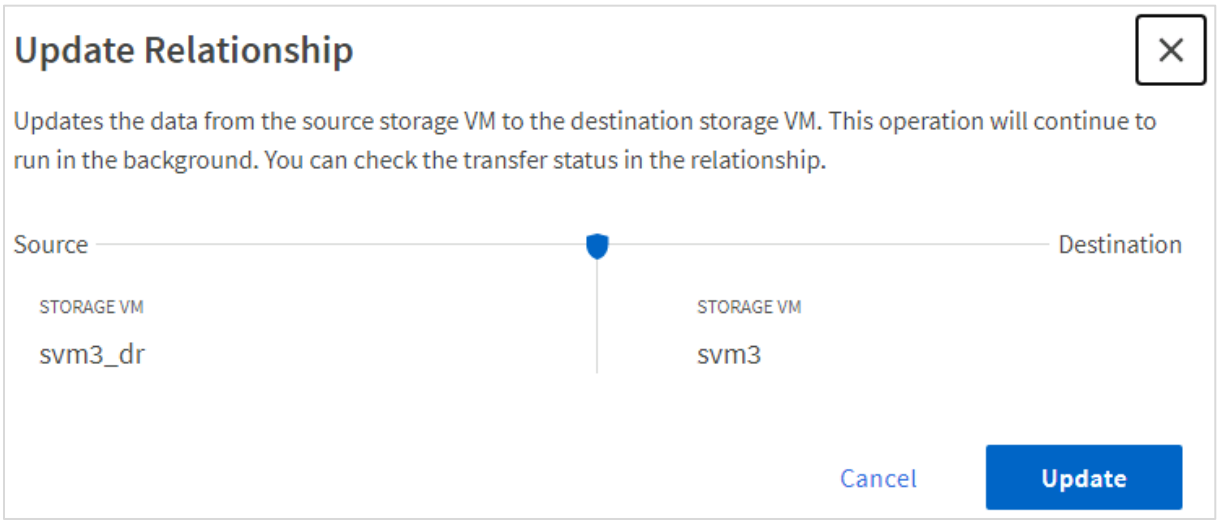
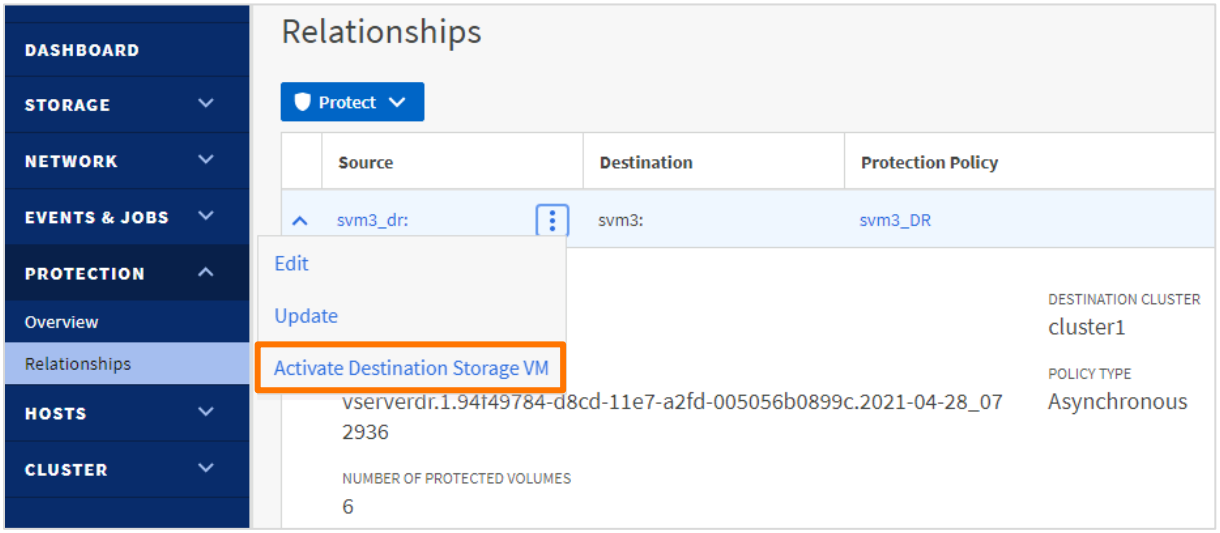
Step	Action
5-1	On a live production system, you must verify the presence of various items. For example, on the primary cluster, you must verify the existence of the following items: ▪ All required feature licenses and protocols ▪ Any required custom schedules ▪ A non-root aggregate with a minimum of 10 GB of free space
5-2	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.
5-3	In the Source column, click the three vertical dots to the right of svm3, and the select **Reverse Resync**. 

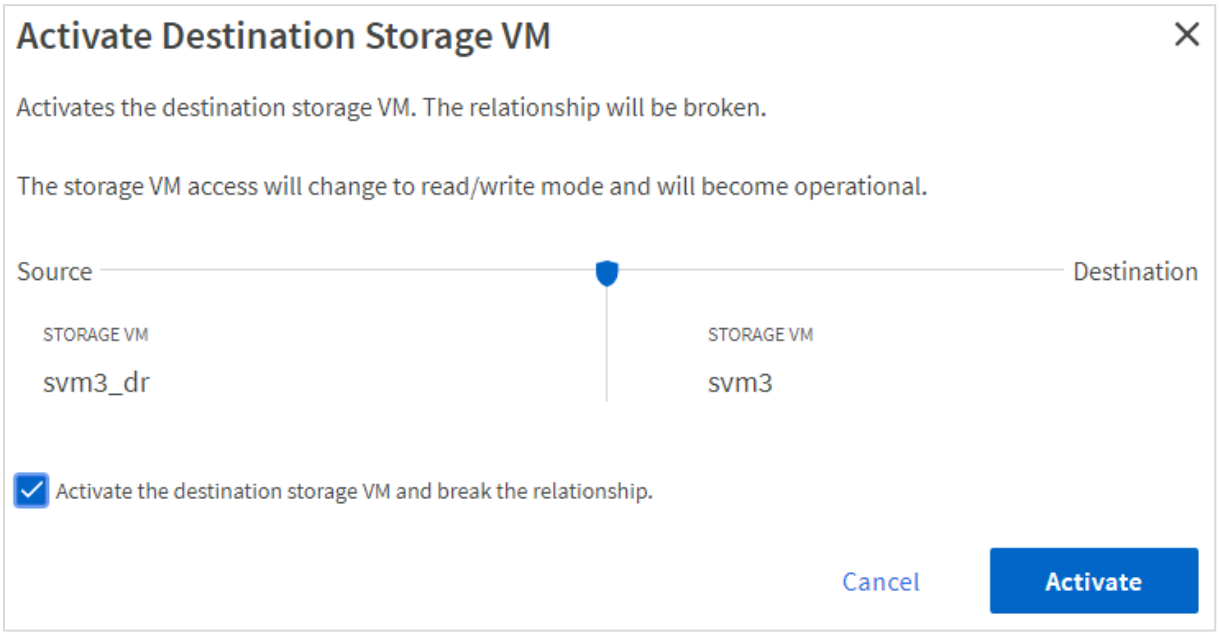
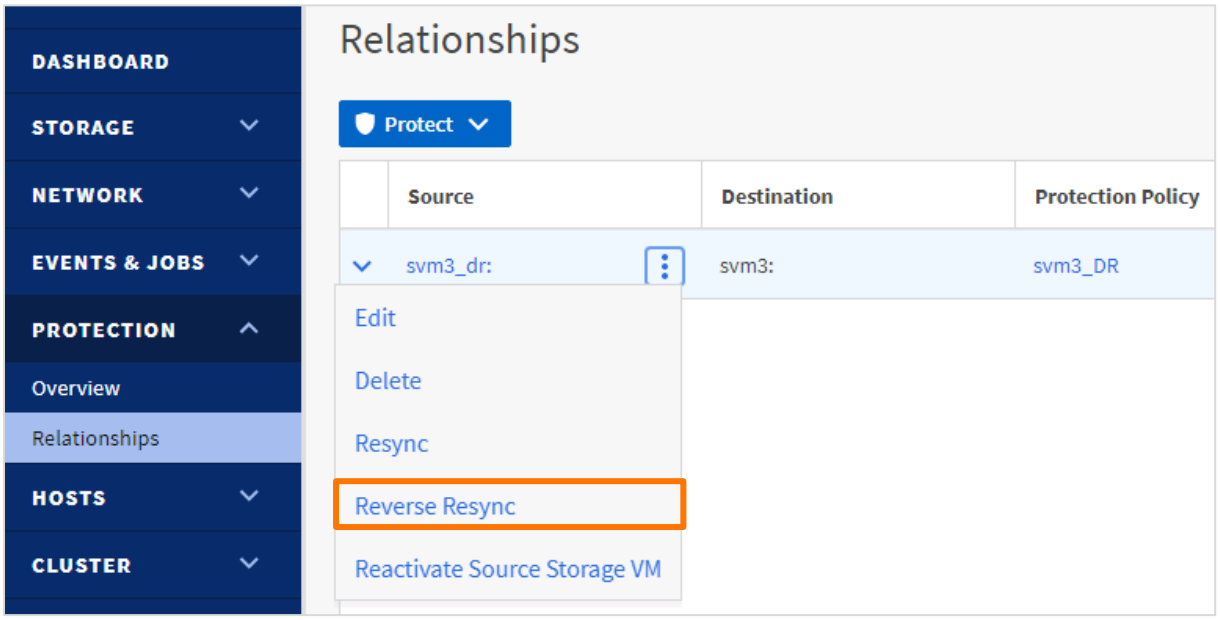
Step	Action
5-4	In the Reverse Resync Relationship dialog box, review the provided information, and then click **Reverse Resync** to resync the data from the destination SVM to the source SVM. 
5-5	You need to wait for multiple seconds for the transfer to complete. The SVM DR relationship is then removed from the relationships list.
5-6	In the Relationships pane, verify that the SVM DR relationship was removed. 
5-7	**Cluster1** In the System Manager navigation pane, select **Protection** > **Relationships**.

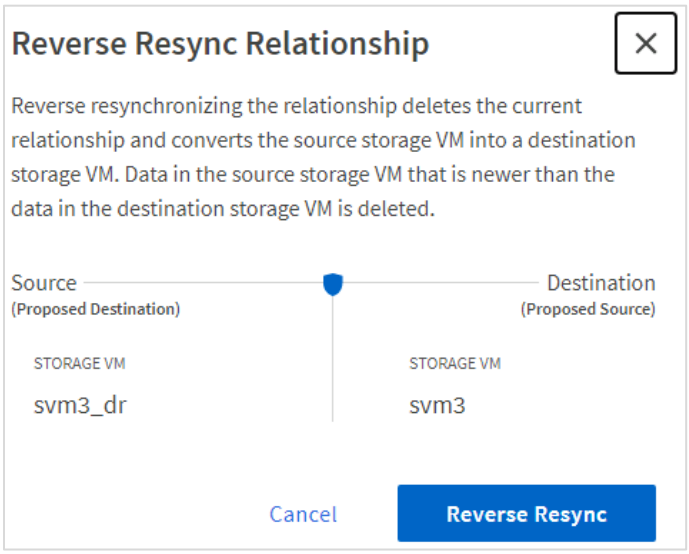
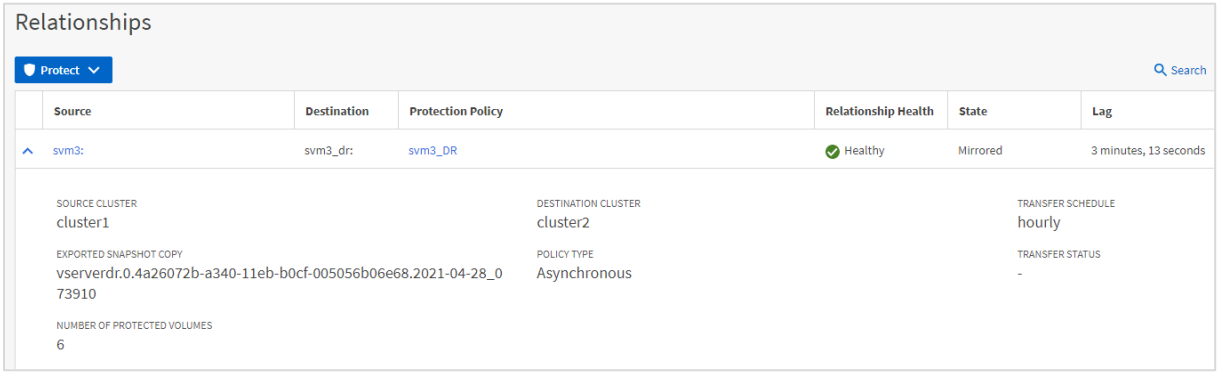
Step	Action
5-8	Verify that the reversed SVM DR relationship is listed and wait for the Transfer Status to change from Transferring to idle. 
5-9	You can continue writing to the volumes on the destination SVM (new source SVM).
5-10	In File Explorer, in folder **svm3_usr_002**, create a text file. 
5-11	**Cluster2** In the System Manager navigation pane, select **Storage** > **Storage VMs**.

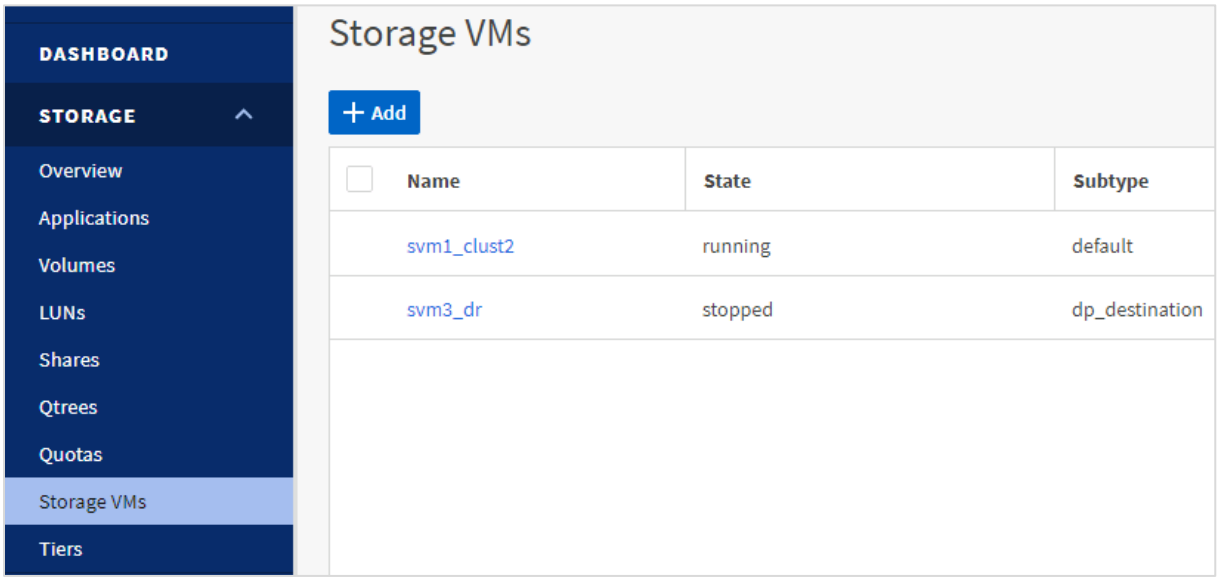
Step	Action
5-12	In the Name column, click the three vertical dots to the right of svm3_dr, and then select **Stop**. 
5-13	In the Stop Storage VM dialog box, click **Stop**. 

Step	Action
5-14	In the Storage VMs pane, verify that the SVM svm3_dr is in a stopped state. 
5-15	**Cluster1** In the System Manager navigation pane, select **Protection** > **Relationships**.
5-16	In the Source column, click the three vertical dots to the right of svm3_dr, and then select **Update**. 

Step	Action
5-17	In the Update Relationship dialog box, click **Update**. 
5-18	Expand the relationship and wait for the Transfer Status to become idle.
5-19	In the Relationships pane, in the Source column, click the three vertical dots to the right of svm3_dr, and then select **Activate Destination Storage VM**. 

Step	Action
5-20	In the Activate Destination Storage VM dialog box, select the **Activate the destination storage VM and break the relationship** checkbox, and then click **Activate** to activate the original source SVM svm3. 
5-21	In the Relationships pane, in the Source column, click the three vertical dots to the right of svm3_dr, and then select **Reverse Resync**. 

Step	Action
5-22	In the Reverse Resync Relationship dialog box, click **Reverse Resync**. 
5-23	In the Relationships pane, verify that the SVM DR relationship was removed.
5-24	**Cluster2** In the System Manager navigation pane, select **Protection** > **Relationships**.
5-25	Verify that the original SVM DR relationship is listed and wait for the Transfer Status to change from Transferring to idle. 
5-26	In the navigation pane, select **Storage** > **Storage VMs**.

Step	Action
5-27	Verify that the SVM svm3_dr is in a stopped state, which indicates that data access now occurs from the source SVM. 
5-28	In the navigation pane, select **Storage** > **Volumes**.
5-29	Verify that the volumes are again of type Data Protection.
5-30	On the Windows Server, open **File Explorer** and verify that you can access the drive that is mapped to c$ (\\192.168.0.62) and that the files that you added exist in the folder svm3_usr_002.

End of exercise

Module 5: MetroCluster Software

Module 5 contains no exercises.

Module 6: SnapMirror Business Continuity

Module 6 contains no exercises.

Module 7: NDMP and Tape Backup

Module 7 contains no exercises.

Module 8: Cloud-Based Data Protection

Module 8 contains no exercises.

Module 9: Course Review

Module 9 contains no exercises.