Protect datastores and virtual machines

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

Table of Contents

Protect datastores and virtual machines

Protect a host cluster in ONTAP tools

ONTAP tools for VMware vSphere manages the protection of host clusters. All the datastores belonging to the selected SVM and mounted on one or more hosts of the cluster are protected under a host cluster.

Before you begin

Make sure you meet these requirements before you protect a host cluster:

- The host cluster contains datastores from a single SVM only.
- Datastores on the host cluster aren't mounted on hosts outside the cluster.
- Datastores mounted on the host cluster are VMFS datastores with iSCSI or FC protocol. You can't use vVols, NFS, or VMFS datastores with NVMe/FC and NVMe/TCP protocols.
- Datastores based on FlexVol/LUN volumes mounted on a host are not part of any consistency group.
- Datastores based on FlexVol/LUN volumes mounted on a host are not part of any SnapMirror relationships.
- The host cluster contains at least one datastore.

Steps

1. Log in to the vSphere client.
2. Right-click on a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. In the protect cluster window, the system automatically fills in the datastore type and source storage virtual machine (VM) details. Select the datastores link to view the protected datastores.
4. Select **Add Relationship**.
5. In the **Add SnapMirror Relationship** window, select the **Target storage VM** and the **Policy** type.

   The policy type can be Asynchronous or AutomatedFailOverDuplex.

   When you add the SnapMirror relationship as an AutomatedFailOverDuplex type policy, you must add the target storage VM as storage backend to the same vCenter where ONTAP tools for VMware vSphere is deployed.

   In the AutomatedFailOverDuplex policy type, there are uniform and non-uniform host configurations. When you select the **uniform host configuration** toggle button, the host initiator group configuration is implicitly replicated on the target site. For more information, refer to Key concepts and terms.

6. If you choose to have a non-uniform host configuration, select the host access (source/target) for each host inside that cluster.
7. Select **Add**.
8. You can edit the host cluster protection using the **Modify host cluster protection** operation. You can edit or delete the relationships using the ellipsis menu options.
9. Select the **Protect** button.

   The system creates a vCenter task with job ID details and shows its progress in the recent tasks panel. This is an asynchronous task; the user interface shows only the request submission status and does not wait for the task to complete.

10. To view the protected host clusters, go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**. Select a consistency group to view its capacity, associated datastores, and child consistency groups.

> ⓘ   If you need to remove protection within one hour of creation, run storage discovery first.

Related information

VMware vSphere Metro Storage Cluster (vMSC)

Protect using SRA protection

Configure SRA in ONTAP tools to protect datastores

ONTAP tools for VMware vSphere provides the option to enable the SRA capability to configure disaster recovery.

Before you begin

- You should have set up your vCenter Server instance and configured ESXi host.
- You should have deployed ONTAP tools for VMware vSphere.
- You should have downloaded the SRA Adapter `.tar.gz` file from the NetApp Support Site.
- You should have the same custom SnapMirror schedules on both source and destination ONTAP clusters before you run the SRA workflows.
- Enable ONTAP tools for VMware vSphere services to enable the SRA capability.

Steps

1. Log in to the VMware Live Site Recovery appliance management interface using the URL: `https://:<srm_ip>:5480`, and then go to Storage Replication Adapters in VMware VMware Live Site Recovery appliance management interface.
2. Select **New Adapter**.
3. Upload the *.tar.gz* installer for the SRA plug-in to VMware Live Site Recovery.
4. Rescan the adapters to verify that the details are updated on the VMware Live Site Recovery Storage Replication Adapters page.

> ⓘ   After a failover, actions such as expand, mount, and delete might not be available for datastores. Perform datastore discovery to refresh and display the appropriate context menu actions.

> ⓘ   After each reprotect operation, you must perform storage discovery on both sites.

In a new setup with SRA protection, always run a test failover. Skipping the test failover might cause the reprotect operation to fail.

In a fan-out configuration, after a SnapMirror Active Sync failover where the SnapMirror source changes to site B for Automated Failover Duplex and Asynchronous SnapMirror, run a test failover between sites B and C. Skipping this step may result in a failed reprotect operation.

Related information

Configure disaster recovery for NFS datastores using VMware Site Recovery Manager

Configure SRA in ONTAP tools for SAN and NAS environments

You should set up the storage systems before running Storage Replication Adapter (SRA) for VMware Live Site Recovery.

Configure SRA for SAN environments

Before you begin

You should have the following programs installed on the protected site and the recovery site:

- VMware Live Site Recovery: The VMware site provides installation documentation for VMware Live Site Recovery.

  About VMware Live Site Recovery

- SRA: Install the adapter on VMware Live Site Recovery.

Steps

1. Verify that the primary ESXi hosts are connected to the LUNs in the primary storage system on the protected site.

2. Verify that the LUNS are in igroups that have the `ostype` option set to *VMware* on the primary storage system.

3. Verify that the ESXi hosts at the recovery site have appropriate iSCSI and Fibre Channel connectivity to the storage virtual machine (SVM). The secondary site ESXi hosts should have access to the secondary site storage, and the primary site ESXi hosts should have access to the primary site storage.

   You can do this either by verifying that the ESXi hosts have local LUNs connected on the SVM or the `iscsi show initiators` command on the SVMs. Check the LUN access for the mapped LUNs in the ESXi host to verify iSCSI connectivity.

Configure SRA for NAS environments

Before you begin

You should have the following programs installed on the protected site and the recovery site:

- VMware Live Site Recovery: You can find installation documentation for VMware Live Site Recovery on the VMware site - About VMware Live Site Recovery

- SRA: Install the adapter on VMware Live Site Recovery and the SRA server.

Steps

1. Verify that the datastores at the protected site contain virtual machines that are registered with vCenter Server.

2. Verify that the ESXi hosts at the protected site have mounted the NFS exports volumes from the storage virtual machine (SVM).

3. Verify that valid addresses such as the IP address or FQDN on which the NFS exports are present are specified in the **NFS Addresses** field when using the Array Manager wizard to add arrays to VMware Live Site Recovery. Do not use the NFS hostname in the **NFS Addresses** field.

4. Use the `ping` command on each ESXi host at the recovery site to verify that the host has a VMkernel port that can access the IP addresses that are used to serve NFS exports from the SVM.

Configure SRA in ONTAP tools for highly scaled environments

You should configure the storage timeout intervals per the recommended settings for Storage Replication Adapter (SRA) to perform optimally in highly scaled environments.

Storage Provider settings

You should set the following timeout values on VMware Live Site Recovery for scaled environment:

Advanced settings	Timeout values
`StorageProvider.resignatureTimeout`	Increase the value of the setting from 900 seconds to 12000 seconds.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Set a high value (For example: 99999)

You should also enable the `StorageProvider.autoResignatureMode` option.

Refer to Change Storage Provider Settings for more information on modifying Storage Provider settings.

Storage settings

When you hit a timeout, increase the values of `storage.commandTimeout` and `storage.maxConcurrentCommandCnt` to a higher value.

> ⓘ The timeout interval specified is the maximum value. You don't need to wait for the maximum timeout to be reached. Most commands finish within the set maximum timeout interval.

Refer to Change Storage Settings for modifying SAN Provider settings.

Configure SRA on the VMware Live Site Recovery appliance using ONTAP tools

After deploying the VMware Live Site Recovery appliance, configure the Storage Replication Adapter (SRA) to enable disaster recovery management.

Configuring SRA on the VMware Live Site Recovery appliance saves the ONTAP tools for VMware vSphere credentials within the appliance, enabling communication between VMware Live Site Recovery and SRA.

Before you begin

- Download the *.tar.gz* file from the NetApp Support Site.
- Enable SRA services in ONTAP tools Manager. For more information, refer the Enable services section.
- Add vCenter Servers to the ONTATP tools for VMware vSphere appliance. For more information, refer the Add vCenter Servers section.
- Add storage backends to ONTAP tools for VMware vSphere. For more information, refer the Add storage

section.

> ℹ️ If you have applied the vCenter certificate patch from ONTAP tools, update the vCenter configuration in the VMware Live Site Recovery appliance using the (:5480) port. For instructions, refer to Reconfigure the Site Recovery Manager Appliance.

Steps

1. On the VMware Live Site Recovery appliance screen, select **Storage Replication Adapter** > **New Adapter**.

2. Upload the *.tar.gz* file to VMware Live Site Recovery.

3. Log in to the VMware Live Site Recovery appliance using an administrator account through an SSH client such as PuTTY.

4. Switch to the root user using the command: `su root`

5. Run the command `cd /var/log/vmware/srm` to go to the log directory.

6. At the log location, enter the command to get the Docker ID used by SRA: `docker ps -l`

7. To log in to the container ID, enter the command: `docker exec -it -u srm <container id> sh`

8. Configure VMware Live Site Recovery with ONTAP tools for VMware vSphere IP address and password using the command: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`

   - Provide the password in single quotes so the Perl script treats special characters as part of the password, not as delimiters.

   - You can set the application (VASA Provider/SRA) username and password in ONTAP tools Manager when enabling these services for the first time. Use these credentials to register SRA with VMware Live Site Recovery.

   - To locate the vCenter GUID, go to the vCenter Server page in ONTAP tools Manager after adding your vCenter instance. Refer to Add vCenter Servers section.

9. Rescan the adapters to confirm that the updated details appear on the VMware Live Site Recovery Storage Replication Adapters page.

Results A confirmation message appears indicating that the storage credentials have been saved. You can now use SRA to communicate with the SRA server using the specified IP address, port, and credentials.

Update SRA credentials in ONTAP tools

For VMware Live Site Recovery to communicate with SRA, you should update SRA credentials on the VMware Live Site Recovery server if you have modified the credentials.

Before you begin

You should have executed the steps mentioned in the topic Configuring SRA on VMware Live Site Recovery appliance.

Steps

1. Run the following commands to delete the VMware Live Site Recovery machine folder cached ONTAP tools username password:

a. `sudo su <enter root password>`

b. `docker ps`

c. `docker exec -it <container_id> sh`

d. `cd conf/`

e. `rm -rf *`

2. Run the Perl command to configure SRA with the new credentials:

a. `cd ..`

b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` You need to have a single quote around the password value.

A success message confirming that the storage credentials are stored is displayed. SRA can communicate with SRA server using the provided IP address, port and credentials.

Configure protected and recovery sites in ONTAP tools

You should create protection groups to protect a group of virtual machines on the protected site.

When you add a new datastore, you can include it in the existing datastore group or add a new datastore and create a new volume or consistency group for protection. After adding a new datastore to a protected consistency group or volume, update SnapMirror and perform storage discovery on both the protected and recovery sites. You can run discovery manually or on a schedule to ensure the new datastore is detected and protected.

Pair protected and recovery sites

You should pair the protected and recovery sites created using your vSphere Client to enable Storage Replication Adapter (SRA) to discover the storage systems.

> (i) Storage Replication Adapter (SRA) supports fan-out with one sync relationship of type Automated Failover Duplex and async relationship SnapMirror on consistency group. However, fan-out with two async SnapMirror on consistency group or fan-out SnapMirrors on Volume is not supported. Vault type SnapMirror relationships are not considered within these fan-out restrictions.

Before you begin

- You should have VMware Live Site Recovery installed on the protected and recovery sites.
- You should have SRA installed on the protected and recovery sites.

Steps

1. On the vSphere Client home page, double-click the **Site Recovery** icon and then select **Sites**.
2. Select **Objects** > **Actions** > **Pair Sites**.
3. In the **Pair Site Recovery Manager Servers** dialog box, enter the address of the protected site's Platform Services Controller, and then select **Next**.
4. In the Select vCenter Server section, do the following:

    a. Verify that the protected site's vCenter Server appears as a matching candidate to pair.

    b. Enter the SSO administrative credentials, and then select **Finish**.

5. If prompted, select **Yes** to accept the security certificates.

Result

The **Objects** dialog box displays both the protected and recovery sites.

Configure protection groups

Before you begin

You should ensure that both the source and target sites are configured for the following:

- Same version of VMware Live Site Recovery installed
- Virtual machines
- Paired protected and recovery sites
- Source and destination datastores should be mounted on respective sites

Steps

1. Log in to vCenter Server and select **Site Recovery** > **Protection Groups**.
2. In the **Protection Groups** pane, select **New**.
3. Specify a name and description for the protection group, direction and select **Next**.
4. In the **Type** field, select the **Type field option…** as datastore groups (array-based replication) for NFS and VMFS datastore. The fault domain is nothing but SVMs with replication enabled. The SVMs that have only peering implemented and have no issues are displayed.
5. In the Replication groups tab, select either the enabled array pair or the replication groups that have the virtual machine you configured, and then select **Next**.

   All the virtual machines on the replication group are added to the protection group.

6. You can select either the existing recovery plan or create a new one by selecting **Add to new recovery plan.**
7. In the Ready to complete tab, review the details of the protection group that you created, and then select **Finish**.

Configure protected and recovery site resources

Configure network mappings in ONTAP tools

You should configure your resource mappings like VM networks, ESXi hosts, and folders on both sites to enable the mapping of each resource from the protected site to the appropriate resource at the recovery site.

You should complete the following resource configurations:

- Network mappings
- Folder mappings
- Resource mappings

- Placeholder datastores

Before you begin

You should have connected the protected and recovery sites.

Steps

1. Log in to vCenter Server and select **Site Recovery** > **Sites**.

2. Select your protected site and select **Manage**.

3. Select **Network Mappings** > **New** in the manage tab to create a new network mapping.

4. In the Create Network Mapping wizard, do the following:

   a. Select **Automatically Prepare Mappings for Networks with Matching Names** and select **Next**.

   b. Select the required data center objects for the protected and recovery sites and select **Add Mappings**.

   c. Select **Next** after mappings are created successfully.

   d. Select the object used earlier to create reverse mapping, then select **Finish**.

Result

The Network Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configure folder mappings in ONTAP tools

You should map your folders on the protected site and recovery site to enable communication between them.

Before you begin

You should have connected the protected and recovery sites.

Steps

1. Log in to vCenter Server and select **Site Recovery** > **Sites**.

2. Select your protected site and select **Manage**.

3. Select **Folder Mappings** > **Folder** icon in the Manage tab to create a new folder mapping.

4. In the Create Folder Mapping wizard, perform the following:

   a. Select **Automatically Prepare Mappings for Folders with Matching Names** and select **Next**.

   b. Select the required data center objects for the protected and recovery sites and select **Add Mappings**.

   c. Select **Next** after mappings are created successfully.

   d. Select the object used earlier to create reverse mapping and then select **Finish**.

Result

The Folder Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configure resource mappings in ONTAP tools

You should map your resources on the protected site and recovery site so that virtual machines are configured to fail over into one group of hosts or the other.

Before you begin

You should have connected the protected and recovery sites.

> (i) In VMware Live Site Recovery, resources can be resource pools, ESXi hosts, or vSphere clusters.

Steps

1. Log in to vCenter Server and select **Site Recovery** > **Sites**.

2. Select your protected site and select **Manage**.

3. Select **Resource Mappings** > **New** in the manage tab to create a new resource mapping.

4. In the Create Resource Mapping wizard, perform the following:

   a. Select **Automatically Prepare Mappings for Resource with Matching Names** and select **Next**.

   b. Select the required data center objects for the protected and recovery sites and select **Add Mappings**.

   c. Select **Next** after mappings are created successfully.

   d. Select the object used earlier to create reverse mapping and then select **Finish**.

Result

The Resource Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configure placeholder datastores in ONTAP tools

Configure a placeholder datastore to reserve space in the vCenter inventory at the recovery site for protected virtual machines (VMs). Placeholder datastores require minimal capacity, because placeholder VMs are small and typically use only a few hundred kilobytes.

Before you begin

- Ensure that the protected and recovery sites are connected.
- Verify that resource mappings have been configured.

Steps

1. Log in to vCenter Server and select **Site Recovery** > **Sites**.

2. Select your protected site and select **Manage**.

3. Select **Placeholder Datastores** > **New** in the manage tab to create a new placeholder datastore.

4. Select the appropriate datastore and select **OK**.

> (i) Placeholder datastores may reside on local or remote storage, but they don't require replication.

5. Repeat steps 3 to 5 to configure a placeholder datastore for the recovery site.

Configure SRA using the array manager in ONTAP tools

You can configure Storage Replication Adapter (SRA) by using the Array Manager wizard of VMware Live Site Recovery to enable interactions between VMware Live Site

Recovery and storage virtual machines (SVMs).

Before you begin

- You should have paired the protected sites and recovery sites in VMware Live Site Recovery.

- You should have configured your onboarded storage before configuring the array manager.

- You should have configured and replicated the SnapMirror relationships between the protected sites and recovery sites.

- You should have enabled the SVM management LIFs to enable multitenancy.

SRA supports cluster-level management and SVM-level management. If you add storage at a cluster level, then you can discover and perform operations on all the SVMs in the cluster. If you add storage at an SVM level, then you can manage only that specific SVM.

Steps

1. In VMware Live Site Recovery, select **Array Managers** > **Add Array Manager**.

2. Enter the following information to describe the array in VMware Live Site Recovery:

   a. Enter a name to identify the array manager in the **Display Name** field.

   b. In the **SRA Type** field, select **NetApp Storage Replication Adapter for ONTAP**.

   c. Enter the information to connect to the cluster or the SVM:

      - If you're connecting to a cluster, you should enter the cluster management LIF.

      - If you're connecting directly to an SVM, you should enter the IP address of the SVM management LIF.

      > ⓘ When configuring the array manager, you should use the same connection (IP address) for the storage system that was used to onboard the storage system in ONTAP tools for VMware vSphere. For example, if the array manager configuration is SVM scoped, then the storage under ONTAP tools for VMware vSphere should be added at SVM level.

   d. If connecting to a cluster, specify the SVM name in the **SVM name** field, or leave it blank to manage all SVMs in the cluster.

   e. Enter the volumes to be discovered in the **Volume include list** field.

      You can enter the source volume at the protected site and the replicated destination volume at the recovery site.

      For example, if you want to discover volume src_vol1 that is in a SnapMirror relationship with volume dst_vol1, you should specify src_vol1 in the protected site field and dst_vol1 in the recovery site field.

   f. **(Optional)** Enter the volumes to be excluded from discovery in the **Volume exclude list** field.

      You can enter the source volume at the protected site and the replicated destination volume at the recovery site.

      For example, if you want to exclude volume *src_vol1* that is in a SnapMirror relationship with volume *dst_vol1*, you should specify *src_vol1* in the protected site field and *dst_vol1* in the recovery site field.

3. Select **Next**.

4. Verify that the array is discovered and displayed at the bottom of the Add Array Manager window and

select **Finish**.

You can follow the same steps for the recovery site by using the appropriate SVM management IP addresses and credentials. On the Enable Array Pairs screen of the Add Array Manager wizard, you should verify that the correct array pair is selected, and that it shows as ready to be enabled.

Verify replicated storage systems in ONTAP tools

You should verify that the protected site and recovery site are successfully paired after configuring Storage Replication Adapter (SRA). The replicated storage system should be discoverable by both the protected site and the recovery site.

Before you begin
- You should have configured your storage system.
- You should have paired the protected site and recovery site by using the VMware Live Site Recovery array manager.
- You should have enabled FlexClone license and SnapMirror license before performing the test failover operation and failover operation for SRA.
- You should have the same SnapMirror policies and schedules on source and destination sites.

Steps
1. Log in to your vCenter Server.
2. Go to **Site Recovery** > **Array Based Replication**.
3. Select the required Array Pair and verify the corresponding details.

   The storage systems should be discovered at the protected site and recovery site with the Status as "Enabled".

Fan-out protection in ONTAP tools

In a fan-out protection scenario, the consistency group is double protected with synchronous relationship on the first destination ONTAP cluster and with asynchronous relationship on the second destination ONTAP cluster. The create, edit, and delete SnapMirror active sync protection workflows maintain the synchronous protection. VMware Live Site Recovery appliance failover and reprotect workflows maintain the asynchronous protection.

ⓘ   Fan-out is not supported for SVM user.

To set up fan-out protection, peer the three site clusters and SVMs.

Example:

If	then

• Source consistency group is on cluster c1 and SVM svm1 • First destination consistency group is on cluster c2 and SVM svm2 and • Second destination consistency group is on cluster c3 and SVM svm3	• The cluster peering on source ONTAP cluster will be (C1, C2) and (C1, C3). • The cluster peering on first destination ONTAP cluster will be (C2, C1) and (C2, C3) and • The cluster peering on second destination ONTAP cluster will be (C3, C1) and (C3, C2). • SVM peering on source SVM will be (svm1, svm2) and (svm1, svm3). • SVM peering on first destination SVM will be (svm2, svm1) and (svm2, svm3) and • SVM peering on second destination svm will be (svm3, svm1) and (svm3, svm2).

The following diagram shows the fan-out protection configuration:

Synchronous relationships
only (sync peers)

Mediator

C1
SVM1

C2
SVM2

Asynchronous
relationships only

Asynchronous
relationships only

C3
SVM3
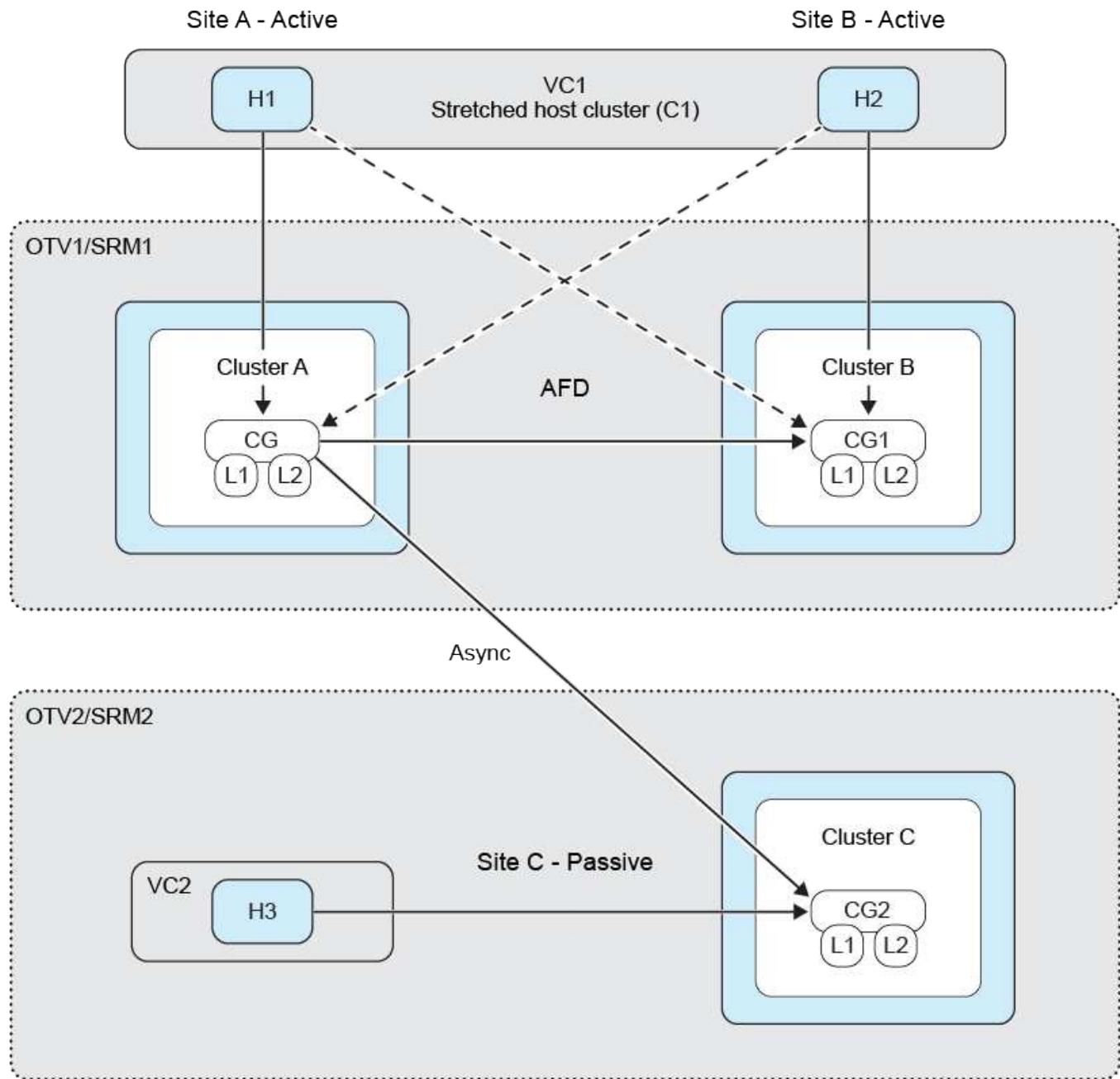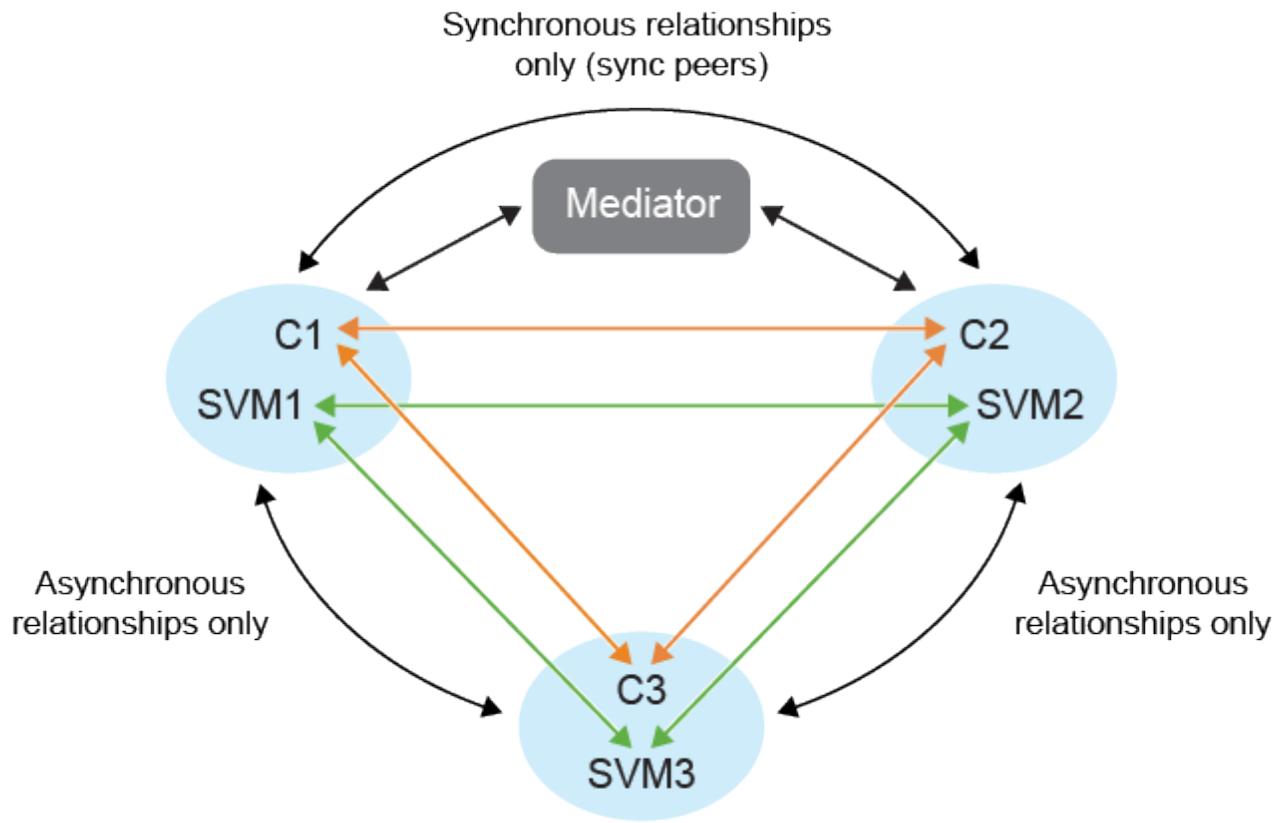
Steps

1. Select a new place holder datastore. The placeholder datastore selection criteria for phased protection are:

   ◦ Do not place the placeholder datastore in the host cluster you are protecting.

   ◦ If you need to include the placeholder datastore in the host cluster, add it to VMware Live Site Recovery appliance before setting up SnapMirror active sync protection. With this setup, you can leave the placeholder datastore out of protection.

   For more information, refer to Select a Placeholder Datastore

2. Add datastore to the host cluster protection by following Modify protected host cluster. Add both asynchronous and synchronous policy types.