



Manage

VSC, VASA Provider, and SRA 9.7

NetApp
April 01, 2025

This PDF was generated from <https://docs.netapp.com/us-en/vsc-vasa-provider-sra-97/manage/concept-workflow-for-configuring-the-unified-appliance.html> on April 01, 2025. Always check docs.netapp.com for the latest.

Table of Contents

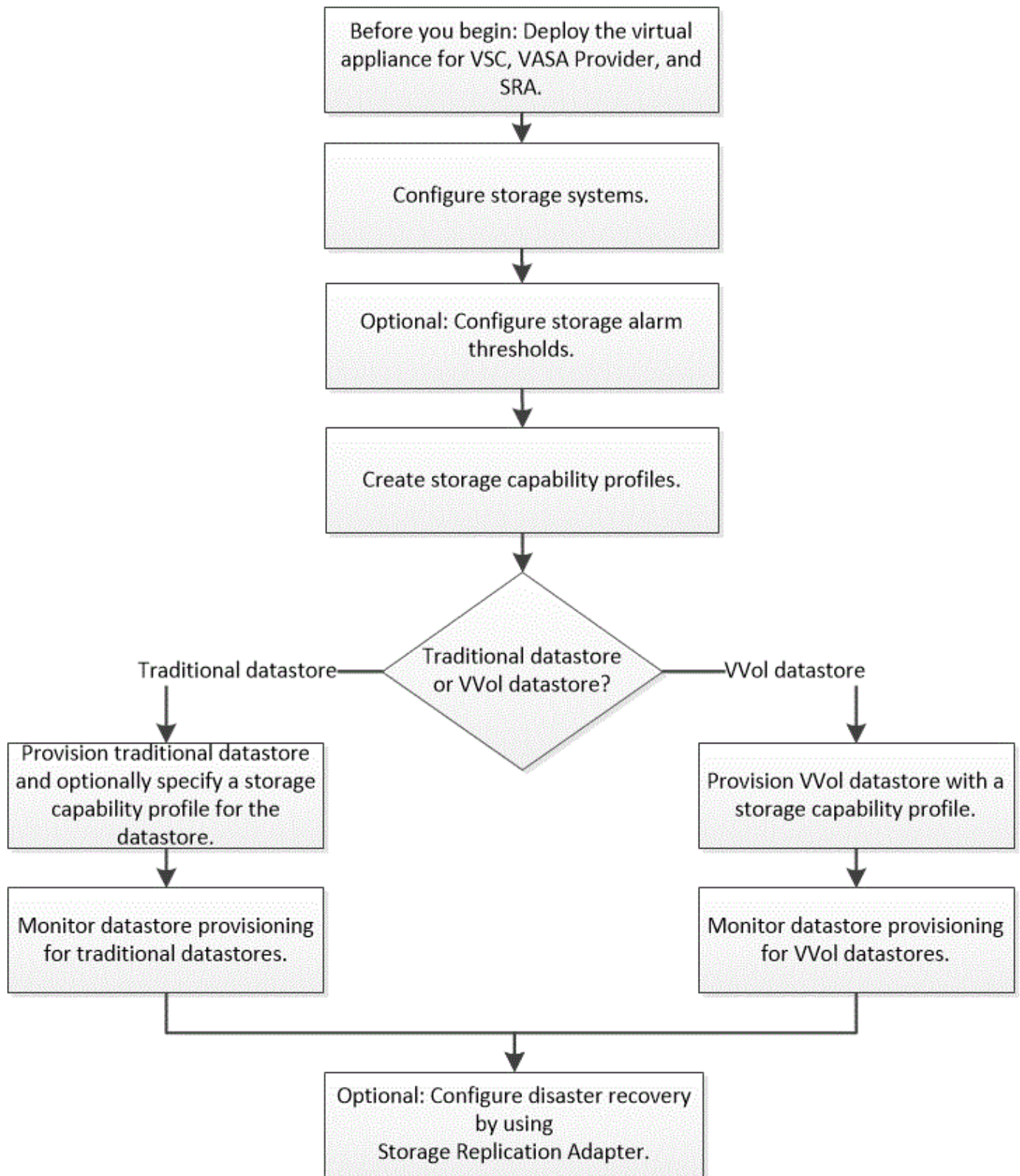
Manage	1
Workflow for configuring the virtual appliance for VSC, VASA Provider, and SRA	1
Configure storage systems for VSC, VASA Provider, and SRA	2
Add storage systems to VSC	3
Set default credentials for storage systems	3
Configure alarm thresholds	4
Create storage capability profiles	4
What storage capabilities are	5
Considerations for creating and editing storage capability profiles	5
Configure storage capability profiles	6
Configure traditional datastores and virtual machines	9
Provision datastores	10
Map datastores to storage capability profiles	12
Verify datastore compliance with the mapped storage capability profile	13
Monitor datastores and virtual machines using the traditional dashboard	14
Edit ESXi host settings for VSC, VASA Provider, and SRA	14
Configure vVols datastores	15
Configure replication for vVols datastore	17
Provision vVols datastores	18
Monitor vVols datastores and virtual machines using the vVol dashboard	21
Manage disaster recovery setup by using Site Recovery Manager	23
Configure VM Storage Policies	23
Configure protection groups	24
Pair protected and recovery sites	25
Configure protected and recovery site resources	25
Verify replicated storage systems	30
Protect unprotected virtual machines	30
Manage traditional and vVols datastores	30
Mount datastore on additional hosts	31
Resize datastores	31
Edit a vVols datastore	31
Add storage to a vVols datastore	32
Remove storage from a vVols datastore	33
Mount a vVols datastore	34
Considerations for migrating or cloning virtual machines	34
Migrate traditional virtual machines to vVols datastores	35
Migrate virtual machines with older storage capability profiles	36
Understand Virtual Storage Console reports	36
What reports do	36
Datastore Reports	37
vVols reports	38
Troubleshoot issues with the virtual appliance for VSC, VASA Provider, and SRA	39
Collect the log files	39

Issue while editing VM Storage Policies after upgrade	40
VASA Provider status shows as “Offline” in vCenter Server GUI	40
Error while accessing the VSC Summary page of virtual appliance	41
Error deleting a datastore after network settings are changed	41
Datastore inaccessible when volume status is changed to offline	42
Add storage system with IPv4 results in authentication error with IPv6 status in storage system grid ...	42
File creation error while provisioning virtual machines on VVol datastores	43
Incorrect status 'Failover in Progress' is reported for SRA in SRM	43

Manage

Workflow for configuring the virtual appliance for VSC, VASA Provider, and SRA

Configuring the virtual machine for VSC, VASA Provider, and SRA involves configuring your storage systems, creating a storage capability profile, provisioning the datastore, and optionally configuring SRA for disaster recovery.



Configure storage systems for VSC, VASA Provider, and SRA

You should add storage systems to the virtual appliance and set default credentials, if required, by using the VSC interface.

Add storage systems to VSC

You can manually add storage system to Virtual Storage Console (VSC).

About this task

Each time you start Virtual Storage Console (VSC) or select the **REDISCOVER All** option, VSC automatically discovers the available storage systems.

Steps

1. Add a storage system to VSC by using the VSC home page:
 - Click **Storage Systems > Add**.
 - Click **Overview > Getting Started**, and then click **ADD** button under **Add Storage System**.
2. In the **Add Storage System** dialog box, enter the management IP address and credentials for that storage system.

You can also add storage systems using the IPv6 address of the cluster or SVM. You can also change the defaults for TLS and the port number in this dialog box.

When you add storage from the VSC **Storage System** page, you must also specify the vCenter Server instance where the storage will be located. The **Add Storage System** dialog box provides a drop-down list of the available vCenter Server instances. VSC does not display this option if you are adding storage to a datacenter that is already associated with a vCenter Server instance.

3. Click **OK** after you have added all of the required information.

Set default credentials for storage systems

You can use Virtual Storage Console for VMware vSphere to set default credentials for a storage system in your vCenter Server.

Before you begin

You must have selected the vCenter Server that you want to use for creating default credentials.

About this task

If you set up default credentials for storage systems, Virtual Storage Console (VSC) uses these credentials to log in to a storage system that VSC has just discovered. If the default credentials do not work, you must manually log in to the storage system. VSC and SRA support addition of storage system credentials at the cluster level or the SVM level. But VASA Provider will only work with cluster level credentials.

Steps

1. On the VSC **Home** page, click **Settings > Administrative Settings > Configure Default Credentials for Storage System**.
2. In the **Storage System Default Credentials** dialog box, enter the user name and password for the storage system.

Storage controller credentials are assigned in ONTAP based on the user name and password pair. The storage controller credentials can either be the administrator account or a custom account that uses role-based access control (RBAC).

You cannot use VSC to change the roles that are associated with the user name and password pair of the storage controller. To modify or create a new ONTAP user role for use with the virtual appliance for VSC,

VASA Provider, and SRA, you can use System Manager.

See the “Configuring user roles and privileges” section in the *Virtual Storage Console, VASA Provider, and Storage Replication Adapter for VMware® vSphere Deployment and Setup Guide For 9.7 Release*.

3. Click **OK** to save the default credentials.

After you finish

If you updated the storage system credentials because a storage system reported “Authentication Failure” status, you should click the **REDISCOVER ALL** option available on the **Storage Systems** page. When you do this, VSC tries to connect to the storage system by using the new credentials.

Configure alarm thresholds

You can use VSC to set alarms to notify you when volume thresholds and aggregate thresholds reach the set limits.

Steps

1. From the Virtual Storage Console **Home** page, click **Settings**.
2. Click **Unified Appliance Settings**.
3. Specify the percent values for the **Nearly full threshold (%)** field and the **Full threshold (%)** field for both the volume alarm thresholds and the aggregate alarm thresholds.

While setting the values, you must keep the following information in mind:

- Clicking **Reset** resets the thresholds to the previous values.

Clicking **Reset** does not reset the thresholds to the default values of 80 percent for “Nearly full” and 90 percent for “Full”.

- There are two ways to set the values:
 - You can use the up and down arrows next to the values to adjust the threshold values.
 - You can slide the arrows on the track bar below the values to adjust the threshold values.
- The lowest value that you can set for the **Full threshold (%)** field for volumes and aggregates is 6 percent.

4. After specifying the required values, click **Apply**.

You must click **Apply** for both volume alarm and aggregate alarm.

Create storage capability profiles

VASA Provider for ONTAP allows you to create storage capability profiles and map them to your storage. This helps you maintain consistency across the storage. You can also use VASA Provider to check for compliance between the storage and the storage capability profiles.

What storage capabilities are

A storage capability is a set of storage system attributes that identifies a specific level of storage performance, storage efficiency, and other capabilities such as encryption for the storage object that is associated with the storage capability.

For traditional datastores, you can use a storage capability profile to create datastores consistently with common attributes, and assign QoS policy to them. During provisioning VSC displays clusters, SVMs, and aggregates that match the storage capability profile. You can generate a storage capability profile from existing traditional datastores by using the **GLOBAL AUTO-GENERATE PROFILES** option from the **Storage Mapping** menu. After the profile is created, you can use VSC to monitor the compliance of datastores with the profile.

When used with VVol datastores, the provisioning wizard can use multiple storage capability profiles to create different FlexVol volumes in the datastore. You can use the VM storage policy to automatically create VVols for a virtual machine in appropriate FlexVol volumes as defined. For example, you can create profiles for common storage classes (such as for performance limits and other capabilities like encryption or FabricPool). You can later create VM storage policies in vCenter Server representing business classes of virtual machines and link these to the appropriate storage capability profile by name (for example Production, Test, HR).

When used with VVols, the storage capability profile is also used to set the storage performance for the individual virtual machine and place it on the FlexVol volume in the vVol datastore that best satisfies the performance requirement. You can specify QoS policy with minimum and/or maximum IOPS for performance. You can use the default policies when you initially provision a virtual machine, or change your VM storage policy later if your business requirements change.

The vCenter Server then associates the storage capability of a LUN or volume with the datastore that is provisioned on that LUN or volume. This enables you to provision a virtual machine in a datastore that matches the storage profile of the virtual machine and to ensure that all of the datastores in a datastore cluster have the same storage service levels.

With the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), you can configure every virtual volume (VVol) datastore with a new storage capability profile that supports the provisioning of virtual machines with varying IOPS requirements on the same vVol datastore. While executing the VM provisioning workflow with IOPS requirement, all of the VVol datastores are listed in the compatible datastore list.



When you try to provision or modify virtual machines for vCenter Server earlier than 6.5, only the vVol datastores that contain storage capability profiles with performance set to “MAX_IOPS” are listed in the compatible datastore list. The remaining vVol datastores are listed in the incompatible datastore list. You can ignore this classification and select any vVol datastore from the incompatible datastore list to provision or modify the virtual machine.

Considerations for creating and editing storage capability profiles

You should be aware of the considerations for creating and editing storage capability profiles.

- You can configure Min IOPS only on AFF systems.
- You can configure QoS metrics at a virtual volume (VVol) datastore level.

This capability provides greater flexibility in assigning varied QoS metrics for different VMDKs of the same virtual machine that is provisioned on a virtual datastore.

- You can configure storage capability profiles for both FAS and AFF datastores.

For FAS systems, you can configure space reserve to be either thick or thin, but for AFF systems, space reserve can only be configured to thin.

- You can use storage capability profiles to provide encryption for your datastores.
- You cannot modify existing storage capability profiles after upgrading from an earlier version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) to the latest version of the virtual appliance for VSC, VASA Provider, and SRA.

The legacy storage capability profiles are retained for backward compatibility. If the default templates are not in use, then during the upgrade to the latest version of the virtual appliance for VSC, VASA Provider, and SRA, the existing templates are overridden to reflect the new QoS metrics related to the performance of the storage capability profiles.

- You cannot modify or use the legacy storage capability profiles to provision new virtual datastores or VM storage policies.
- You must use new storage capability profiles for all new datastores.

Configure storage capability profiles

You can use VSC to manually create storage capability profiles, automatically generate a profile based on the capabilities of a datastore, or modify a profile to meet your requirements.

Before you begin


You must have registered your VASA Provider instance with Virtual Storage Console for VMware vSphere.

About this task

After setting up a profile, you can edit the profile as required.

Steps

1. On the Virtual Storage Console (VSC) **Home** page, click **Storage Capability Profiles**.
2. Create a profile or edit an existing profile, as required:

If you want to...	Do this...
Create a profile	Click  .
Edit an existing profile	Click the profile that you want to modify from the profiles listed on the Storage Capability Profiles page.




To view the values that are associated with an existing profile, you can click the profile name in the Storage Capabilities Profile page. VASA Provider then displays the Summary page for that profile. - You cannot modify any existing storage capability profiles that were created before the 9.6 virtual appliance for VSC, VASA Provider, and SRA.

3. Complete the pages in the **Create Storage Capability Profile** wizard to set up a profile or to edit values to modify an existing profile.

Most of the fields in this wizard are self-explanatory. The following table describes some of the fields for which you might require guidance.

Field	Explanation
Identifying multiple profiles	<p>You can use the Description field on the Name and Description tab to describe the purpose of the storage capability profile. Providing a good description is useful because it is a good practice to set up different profiles based on the applications that are being used.</p> <p>For example, a business-critical application requires a profile with capabilities that support higher performance, such as an AFF platform. A datastore that is used for testing or training might use a profile with a lower performance FAS platform, and enable all of the storage efficiency capabilities and tiering to control costs.</p> <p>If you have enabled “linked” mode for your vCenter Servers, then you must select the vCenter Server for which you are creating the storage capability profile.</p>
Platform	<p>You can select your storage system to have either the AFF or FAS platform type. The options on the subsequent screens are updated based on your selection of the type of storage system.</p>

Field	Explanation
Performance	<p>You can set traditional QoS policies for your storage system by using the Performance tab.</p> <ul style="list-style-type: none"> • When you select None, a QoS policy with no limit (infinite) is applied to a data VVol. • When you select QoS Policy Group, then a traditional QoS policy is applied to a VVol. <p>You can set the value for Max IOPS and Min IOPS which enables you to use the QoS functionality. If you select Infinite IOPS, the Max IOPS field is disabled. When applied for a traditional datastore, a QoS policy with “Max IOPS” value is created and assigned to a FlexVol volume. When used with a VVol datastore, a QoS policy with Max IOPS and Min IOPS values is created for each data VVol.</p> <div>  <ul style="list-style-type: none"> ◦ Max IOPS and Min IOPS can also be applied to the FlexVol volume for a traditional datastore. ◦ You must ensure that the performance metrics are not also set separately at an storage virtual machine (SVM) level, an aggregate level, or a FlexVol volume level. </div>

Field	Explanation
Storage Attributes	<p>The storage attributes that you can enable in this tab depend on the storage type that you select in the Personality tab.</p> <ul style="list-style-type: none"> If you select FAS storage, you can configure space reserve (thick or thin), enable deduplication, compression, and encryption. <p>The tiering attribute is disabled because this attribute is not applicable to FAS storage.</p> <ul style="list-style-type: none"> If you select AFF storage, you can enable encryption and tiering. <p>Deduplication and compression are enabled by default for AFF storage and cannot be disabled. Space reserve is configured as thin and cannot be changed to thick (thin is required for aggregate efficiency and tiering).</p> <p>The tiering attribute enables the use of volumes that are part of a FabricPool-enabled aggregate (supported by VASA Provider for AFF systems with ONTAP 9.4 and later). You can configure one of the following policies for the tiering attribute:</p> <ul style="list-style-type: none"> Any: Allows use of this storage capability profile with any FlexVol volume whether Fabric Pool is used or not None: Prevents volume data from being moved to the capacity tier Snapshot-Only: Moves user data blocks of volume Snapshot copies that are not associated with the active file system to the capacity tier Auto: Moves cold user data blocks in the Snapshot copies and the active file system to the capacity tier

4. Review your selections on the **Summary** page, and then click **OK**.

After you create a profile, you can return to the Storage Mapping page to view which profiles match which datastores.

Configure traditional datastores and virtual machines

You can use Virtual Storage Console (VSC) to configure datastores and virtual machines in your vCenter Server. The datastores and virtual machines that are provisioned by VSC are displayed on the dashboard of VSC. This enables you to easily monitor and manage

these datastores and virtual machines.

Provision datastores

Provisioning a datastore creates a logical container for your virtual machines and their virtual machine disks (VMDKs). You can provision a datastore, and then attach the datastore to a single host, to all of the hosts in a cluster, or to all of the hosts in a datacenter.

Before you begin

- To provision a datastore on an SVM that is directly connected to Virtual Storage Console (VSC), you must have added the SVM to VSC by using a user account that has the appropriate privileges, not the default vsadmin user account or vsadmin role.

You can also provision a datastore by adding a cluster.

- You must ensure that the subnet details of all the networks to which the ESXi host is connected is entered in the `kaminoprefs.xml`.

See "Enabling datastore mounting across different subnets" section in *VSC 9.6 Deployment and Setup Guide*.

- If you use NFS or iSCSI, and the subnet is different between your ESXi hosts and your storage system, then the NFS or iSCSI settings in the `kaminoprefs` preferences file must include ESXi host subnet masks.

This preference file is also applicable to VVol datastore creation. *Virtual Storage Console, VASA Provider, and Storage Replication Adapter Deployment and Setup Guide for 9.6 release* has more information on preferences file and enabling datastore mounting across different subnets.

- If you have enabled VASA Provider and you want to specify storage capability profiles for your NFS datastores or VMFS datastores, then you must have created one or more storage capability profiles.
- To create an NFSv4.1 datastore, you must have enabled NFSv4.1 at the SVM level.

About this task

The **Provision Datastore** option enables you to specify a storage capability profile for the datastore. Storage capability profiles help in specifying consistent service level objectives (SLOs) and simplify the provisioning process. You can specify a storage capability profile only if you have enabled VASA Provider. The virtual appliance for VSC, VASA Provider, and SRA supports the following protocols:

- NFSv3 and NFSv4.1
- VMFS5 and VMFS6

VSC can create a datastore on either an NFS volume or a LUN:

- For an NFS datastore, VSC creates an NFS volume on the storage system, and then updates the export policies.
- For a VMFS datastore, VSC creates a new volume (or uses an existing volume, if you selected that option), and then creates a LUN and an igroup.



VMware does not support NFSv4.1 with datastore clusters.

If a storage capability profile is not specified during provisioning, you can later use the Storage Mapping page to map a datastore to a storage capability profile.

Steps

1. You can access the datastore provisioning wizard using one of the following:

If you select from ...	Perform the following...
vSphere Client Home page	<ol style="list-style-type: none">a. Click Hosts and Clusters.b. In the navigation pane, select the datacenter on which you want to provision the datastore.c. To specify the hosts to mount the datastore, see the next step.
Virtual Storage Console Home page	<ol style="list-style-type: none">a. Click Overview.b. Click Getting Started tab.c. Click Provision button.d. Click Browse to select the destination to provision the datastore as per the next step.

2. Specify the hosts on which you want to mount the datastore.

To make the datastore available to...	Do this...
All of the hosts in a datacenter	Right-click a datacenter, and then select NetApp VSC › Provision Datastore .
All of the hosts in a cluster	Right-click a host cluster, and then select NetApp VSC › Provision Datastore .
A single host	Right-click a host, and select NetApp VSC › Provision Datastore .

3. Complete the fields in the **New Datastore** dialog box to create the datastore.

Most of the fields in the dialog box are self-explanatory. The following table describes some of the fields for which you might require guidance.

Section	Description
General	The General section of the New Datastore provisioning dialog box provides options to enter the destination, name, size, type, and protocol for the new datastore. You can select NFS or VMFS protocol to configure a traditional datastore. The VVol datastore type is used to configure a VVol datastore. If VASA Provider is enabled, then you can also decide whether to use storage capability profiles. The Datastore cluster option is available only for traditional datastores. You should use the Advanced option to specify VMFS5 or VMFS6 file system.
Storage system	You can select one of the listed storage capability profiles if you have selected the option in the General section. The system-recommended values for the storage system and storage virtual machine are populated for ease. But you can modify the values if required.
Storage attributes	By default, VSC populates the recommended values for Aggregates and Volumes options. You can customize the values based on your requirements. The Space reserve option available under Advanced menu is also populated to give optimum results.
Summary	You can review the summary of the parameters you specified for the new datastore.

4. In the **Summary** section, click **Finish**.

Map datastores to storage capability profiles

You can map the datastores that are associated with VASA Provider for ONTAP to storage capability profiles. You can assign a profile to a datastore that is not associated with a storage capability profile.

Before you begin

- You must have registered your VASA Provider instance with Virtual Storage Console for VMware vSphere.
- Virtual Storage Console (VSC) must have already discovered your storage.

About this task

You can map traditional datastore with a storage capability profile or change the storage capability profile that is associated with a datastore. VASA Provider does *not* display any virtual volume (VVol) datastores on the **Storage Mappings** page. All the datastores that are referred to in this task are traditional datastores.

Steps

1. From the VSC **Home** page, click **Storage Mapping**.

From the **Storage Mapping** page, you can determine the following information:

- The vCenter Server that is associated with the datastore
- How many profiles match the datastore

The **Storage Mapping** page displays only traditional datastores. This page does not display any VVol datastores or qtree datastores.

- Whether the datastore is currently associated with a profile

A datastore can match multiple profiles, but a datastore can be associated with only one profile.

- Whether the datastore is compliant with the profile that is associated with it

2. To map a storage capability profile to a datastore or to change the existing profile of a datastore, select the datastore.

To locate specific datastores or other information on the **Storage Mapping** page, you can enter a name or a partial string in the search box. VSC displays the search results in a dialog box. To return to the full display, you should remove the text from the search box, and then click **Enter**.

3. From the **Actions** menu, select **Assign matching profile**.
4. Select the profile that you want to map to the datastore from the list of matching profiles that is provided in the **Assign profile to datastore** dialog box, and then click **OK** to map the selected profile to the datastore.
5. Refresh the screen to verify the new assignment.

Verify datastore compliance with the mapped storage capability profile

You can quickly verify whether your datastores are compliant with the storage capability profiles that are mapped to the datastores.

Before you begin

- You must have registered your VASA Provider instance with Virtual Storage Console for VMware vSphere (VSC).
- VSC must have discovered your storage.

Steps

1. From the VSC **Home** page, click **Storage Mapping**.
2. Review the information in the **Compliance Status** column to identify non-compliant datastores and review the alerts for non-compliance reason.



When you click the **COMPLIANCE CHECK** button, VSC performs a rediscovery operation for all of the storage, which might take few minutes.

If a datastore is no longer compliant with its profile, then the **Compliance Status** column displays an alert stating the reason for non-compliance. For example, a profile might require compression. If that setting has been changed on the storage, compression is no longer used, and the datastore is non-compliant.

After you finish

When you discover a datastore that is not compliant with its profile, you can modify the settings on the volume backing the datastore to make the datastore compliant, or you can assign a new profile to the datastore.

You can modify the settings from the **Storage Capability Profile** page.

Monitor datastores and virtual machines using the traditional dashboard

You can monitor the traditional datastores and virtual machines using the traditional dashboard of the virtual appliance for Virtual Storage Console, VASA Provider, and Storage Replication Adapter. The dashboard data enables you to analyze the datastore usage and to take corrective action to prevent the virtual machines from running into space-related constraints.

Before you begin

You should select either the **Enable Storage I/O Control and statistics collection** or **Disable Storage I/O Control but enable statistics collection** option in the Configure Storage I/O Control dialog box. You can enable Storage I/O Control only if you have the Enterprise Plus license from VMware.

[VMware vSphere Documentation: Enable Storage I/O Control](#)

About this task

The VSC dashboard displays IOPS, space utilized, latency, and committed capacity metrics that are obtained from your vCenter Server. ONTAP provides volume space saving metrics to the VSC dashboard. These performance parameters enable you to identify performance bottlenecks in the virtual environment and to take corrective action to resolve the issues.

The traditional dashboard of the virtual appliance for VSC, VASA Provider, and SRA enables you to view either NFS datastores or VMFS datastores. You can click a datastore to navigate to the datastore details view that is provided by the vCenter Server instance to view and fix any issues with the datastores in your vCenter Server.

Steps

1. From the vSphere Client home page, click **Virtual Storage Console**.
2. Select the required vCenter Server using the **vCenter Server** drop-down menu to view the datastores.
3. Click **Traditional Dashboard**.

The **Datastores** portlet provides the following details:

- The number of traditional datastores along with their performance metrics that are managed by VSC in your vCenter Server instance
- The top five datastores based on resource usage and performance parameters that can be modified, if required. You can change the listing of the datastores based on the space utilized, IOPS, or latency and in the order required.

The **Virtual Machines** portlet provides the following details:

- Number of virtual machines using NetApp datastores in your vCenter Server
- Top five virtual machines based on committed capacity, latency, and uptime

Edit ESXi host settings for VSC, VASA Provider, and SRA

You can use the dashboard of the virtual appliance for Virtual Storage Console (VSC),

VASA Provider, and Storage Replication Adapter (SRA) to editing your ESXi host settings.

Before you begin

You must have configured an ESXi host system for your vCenter Server instance.

About this task

If there is an issue with your ESXi host settings, the issue is displayed in the ESXi Host Systems portlet of the dashboard. You can click the issue to view the host name or the IP address of the ESXi host that has the issue.

Steps

1. From the vSphere Client **Home** page, click **Virtual Storage Console**.
2. Edit the ESXi host settings.

If you want to edit the ESXi host settings from...	Do this...
Issues displayed	<ol style="list-style-type: none">a. Click the issue in the ESXi Host Systems portlet.b. Click the ESXi host names for which you want to modify the settings.c. Right-click the ESXi host name, and click NetApp VSC > Set Recommended Values.d. Modify the required settings, and then click OK.
vSphere Client home page	<ol style="list-style-type: none">a. Click Menu > Hosts and Clusters.b. Right-click the required ESXi host, and select NetApp VSC > Set Recommended Value.c. Click OK.
ESXi Host Systems portlet	<ol style="list-style-type: none">a. Click the Traditional dashboard tab in the Overview section of VSC.b. Click Edit ESXi Host Settings.c. Select the ESXi host name in the Host settings and status tab for which you want to modify the settings, and click NEXT.d. Select the required settings in the Recommended host settings tab, and then click Next.e. Review your selection in the Summary tab, and then click FINISH.

Configure vVols datastores

You can use VASA Provider for ONTAP to create and manage VMware Virtual Volumes (vVols). You can provision, edit, mount, and delete a vVols datastore. You can also add

storage to the vVols datastore or remove storage from the vVols datastore. to provide greater flexibility. You can provision and manage every virtual machine and the related VMDK.

A vVols datastore consists of one or more FlexVol volumes within a storage container (also called “backing storage”). A virtual machine can be spread across one vVols datastore or multiple vVols datastores.

While you can create a vVols datastore that has multiple FlexVol volumes, all of the FlexVol volumes within the storage container must use the same protocol (NFS, iSCSI, or FCP) and the same storage virtual machines (SVMs).

You do not require detailed knowledge of the underlying storage. For example, you do not have to identify a specific FlexVol volume to contain the storage. After you add FlexVol volumes to the vVols datastore, the storage container manages the storage requirements and prevents any situations during VM provisioning where VM are provisioned to a backing volume with no capacity.



It is a good practice to include multiple FlexVol volumes in a vVols datastore for performance and flexibility. Because FlexVol volumes have LUN count restrictions that limit the number of virtual machines, including multiple FlexVol volumes allows you to store more virtual machines in your vVols datastore.

As part of the setup process, you must specify a storage capability profile for the vVols datastore that you are creating. You can select one or more VASA Provider storage capability profiles for a vVols datastore. You can also specify a default storage capability profile for any vVols datastores that are automatically created in that storage container.

VASA Provider creates different types of vVols during virtual machine provisioning or VMDK creation, as required.

- **Config**

VMware vSphere uses this vVols datastore to store configuration information.

In SAN (block) implementations, the storage is a 4 GB LUN.

In an NFS implementation, this is a directory containing VM config files such as the vmx file and pointers to other vVols datastores.

- **Data**

This vVols contains operating system information and user files.

In SAN implementations, this is a LUN that is the size of the virtual disk.

In an NFS implementation, this is a file that is the size of the virtual disk.

- **Swap**

This vVols is created when the virtual machine is powered on and is deleted when the virtual machine is powered off.

In SAN implementations, this is a LUN that is the size of the virtual memory.

In an NFS implementation, this is a file that is the size of the virtual memory.

- **Memory**

This vVols is created if the memory snapshots option is selected when creating VM snapshot.

In SAN implementations, this is a LUN that is the size of the virtual memory.

In an NFS implementation, this is a file that is the size of the virtual memory.

Configure replication for vVols datastore

You can configure replication for your vVols datastore using the virtual appliance for VSC, VASA Provider, and SRA. The main aim of vVols replication is to protect critical virtual machines during disaster recovery using VMware Site Recovery Manager (SRM).

However, to configure vVols replication for your virtual appliance for VSC, VASA Provider, and SRA, VASA Provider capability and vVols replication must be enabled. VASA Provider is enabled by default in the virtual appliance for VSC, VASA Provider, and SRA. The Array Based Replication is performed at the FlexVol level. Each vVols datastore is mapped to a storage container that consists of one or more FlexVol volumes. The FlexVol volumes should be pre-configured with SnapMirror from ONTAP.

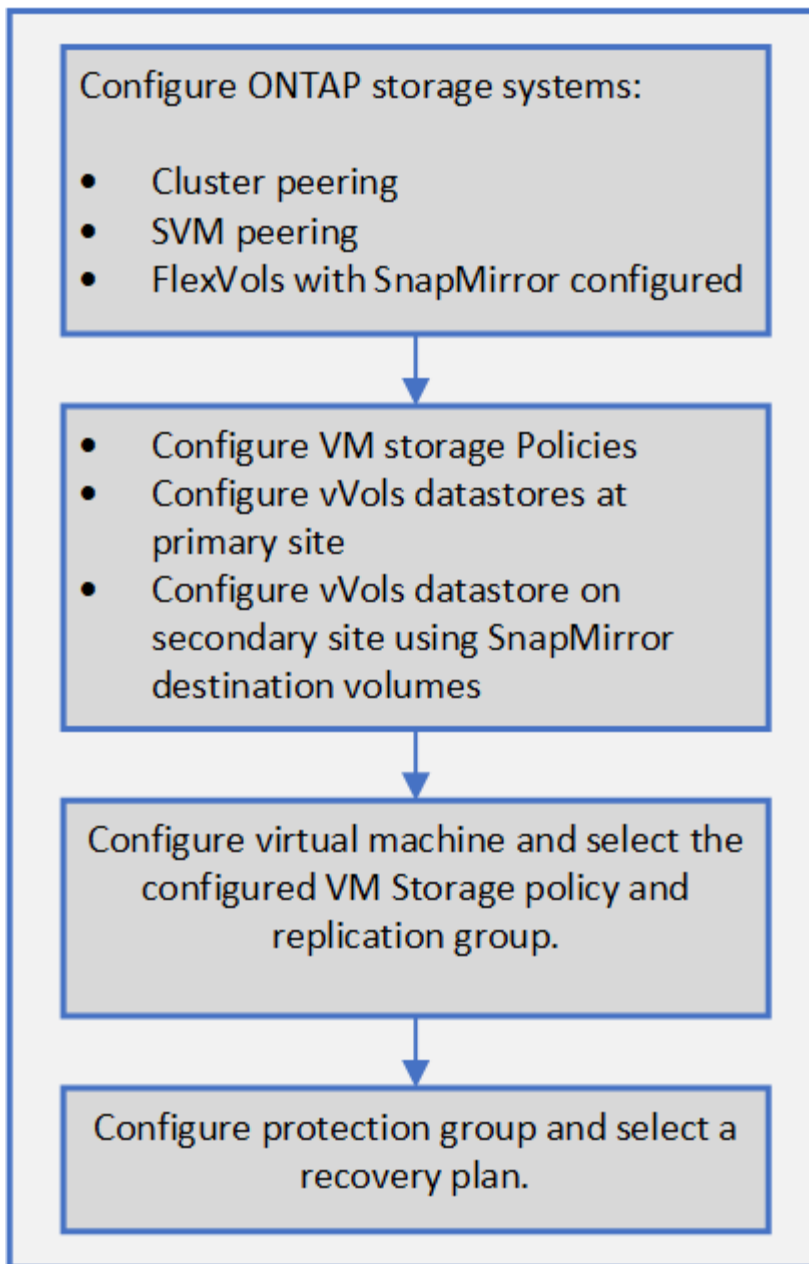


You should not configure a mix of protected and unprotected virtual machines in a single vVols datastore. A reprotect operation after failover will cause unprotected virtual machines to be deleted. Ensure that all virtual machines in a vVols datastore are protected when using replication.

Replication groups are created during vVols datastore create workflow for each FlexVol volume. To use vVols replication, you will need to create VM Storage Policies that include replication status and schedule along with storage capability profile. A Replication group includes virtual machines that are replicated as part of disaster recovery to the target site. You can configure replication groups with protection groups and recovery plans using SRM console, for DR workflows.



If you are using disaster recovery for vVols datastore, then you do not need to configure Storage Replication Adapter (SRA) separately as VASA Provider capability is enhanced to have vVols replication.



Provision vVols datastores

You can provision a vVols datastore using the **Provision Datastore** wizard only if VASA Provider is enabled in your virtual appliance for VSC, VASA Provider, and SRA.

Before you begin

- You should ensure that the subnet details of all the networks to which the ESXi hosted is connected is entered in the `Kaminoprefs.xml`.

See **Enabling datastore mounting across different subnets** section in *VSC 9.7 Deployment and Setup Guide*.

- You should configure similar replication policy and schedule on the datastores at both the source and target sites for reverse replication to be successful.

About this task

The **Provision datastore** menu enables you to specify a storage capability profile for the datastore, which helps in specifying consistent service level objectives (SLOs) and simplifies the provisioning process. You can specify a storage capability profile only if you have enabled VASA Provider.

FlexVol volumes that are used as backing storage are displayed on the vVol dashboard only if they are running ONTAP 9.5 or later. You should not use the vCenter Server **New Datastore** wizard to provision vVols datastores.

- You must use cluster credentials to create vVols datastores.

You cannot use SVM credentials to create vVols datastores.

- VASA Provider does not support the cloning of a virtual machine that is hosted on the vVols datastore of one protocol to another datastore with a different protocol.
- You should have completed cluster pairing and SVM pairing both on the source and destination sites.



Steps

1. From the vSphere Client home page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter on which you want to provision the datastore.
3. Specify the hosts on which you want to mount the datastore.

To make the datastore available to...	Do this...
All of the hosts in a datacenter	Right-click a datacenter, and then select NetApp VSC › Provision Datastore .
All of the hosts in a cluster	Right-click a cluster, and then select NetApp VSC › Provision Datastore .
A single host	Right-click a host, and then select NetApp VSC › Provision Datastore .

4. Complete the fields in the **New Datastore** dialog box to create the datastore.

Most of the fields in the dialog box are self-explanatory. The following table describes some of the fields for which you might require guidance.

Section	Description
General	<p>The General section of the New Datastore dialog box provides options to enter the location, name, description, type, and protocol for the new datastore. The vVols datastore type is used to configure a vVols datastore.</p> <div data-bbox="873 447 927 499">  </div> <p>If you are provisioning iSCSI vVols datastore for vVols replication, then before creating vVols datastore at the target site, you need to perform SnapMirror update and cluster rediscovery.</p>
Storage system	<p>This section enables you to select whether you want the vVols datastore to have either replication enabled or disabled. Only asynchronous type replication profile is allowed for this release. You can then select one or more storage capability profiles listed. The system recommended values of paired Storage system and Storage VM are populated automatically. The recommended values are populated only if they are paired in ONTAP. You can modify these values if required.</p> <div data-bbox="873 1115 927 1167">  </div> <p>While creating FlexVol volumes in ONTAP, you should ensure to create them with the attributes you wish to select in the storage capability profile. Both read write and data protection FlexVol volumes should have similar attributes.</p> <p>After FlexVol volumes are created and SnapMirror is initialized in ONTAP, you should run a storage rediscovery in VSC to be able to see the new volumes.</p>
Storage attributes	<p>You should select the schedule for SnapMirror and the required FlexVol volume from the existing list. This schedule should be similar to the one selected in the VM Storage Policies page. The user should have created FlexVol volumes on ONTAP with SnapMirror that are listed. You can select the default storage capability profile to be used for creating vVols using the Default storage capability profile option.</p>

5. In the **Summary** section, click **Finish**.

A Replication group is created in the backend when a vVols datastore is configured.

Related information

[vVol dashboard data requirements](#)

Monitor vVols datastores and virtual machines using the vVol dashboard

You can monitor the performance and view the top five SAN VMware Virtual Volumes (vVols) datastores in your vCenter Server based on the parameters that you select by using the vVol dashboard of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA).

Before you begin

- You should have enabled OnCommand API Services 2.1 or later if you are using ONTAP 9.6 or earlier.

You do not require to register OnCommand API Services with VASA Provider to get the details of SAN vVols datastore or SAN vVols VM datastore report for ONTAP 9.7.

NetApp Support

- You should be using ONTAP 9.3 or later for your storage system.

[vVol dashboard data requirements](#)

About this task

The IOPS data that is provided by ONTAP is rounded off and displayed on the vVol dashboard. There might be a difference between the actual IOPS value that is provided by ONTAP and the IOPS value that is displayed on the vVol dashboard.



- If you are registering OnCommand API Services for the first time, then you can view all of the performance metrics data for SAN vVols datastores on the vVol dashboard only after 15 to 30 minutes.
- The vVol dashboard data is refreshed periodically, at an interval of 10 minutes.
- If you have added, modified, or deleted a storage system from your vCenter Server instance, then you might not notice any change in the data on the vVols dashboard for some time.

This is because OnCommand API Services takes time to obtain updated metrics from ONTAP.

- The Total IOPS value that is displayed in the **Overview** portlet of the vVol dashboard is not a cumulative value of the Read IOPS value and Write IOPS value.

Read IOPS, Write IOPS, and Total IOPS are separate metrics that are provided by OnCommand API Services. If there is a difference between the Total IOPS value and the cumulative IOPS value (Read IOPS value + Write IOPS value) provided by OnCommand API Services, then the same difference is observed in the IOPS values on the vVol dashboard.

Steps

1. From the vSphere Client home page, click **Virtual Storage Console**.

2. Select the required vCenter Server using the **vCenter server** drop-down menu to view the datastores.
3. Click **vVol Dashboard**.

The **Datastores** portlet provides the following details:

- The number of vVols datastores that are managed by VASA Provider in your vCenter Server instance
 - The top five vVols datastores based on resource usage and performance parameters You can change the listing of the datastores based on the space utilized, IOPS, or latency and in the order required.
4. View the details of the virtual machines using the **Virtual Machines** portlet.

The **Virtual Machines** portlet provides the following details:

- Number of virtual machines using ONTAP datastores in your vCenter Server
- Top five virtual machines based on IOPS, latency, throughput, committed capacity, uptime, and logical space You can customize how the top five virtual machines are listed in the vVol dashboard.

vVol dashboard data requirements

You must verify some important requirements of the vVol dashboard to display dynamic details of the VMware Virtual Volumes (vVols) datastores and virtual machines.

The following table presents an overview of what you should verify if the vVol dashboard does not display the performance metrics for the provisioned SAN vVols datastores and virtual machines.

Considerations	Description
First-time deployment of OnCommand API Services	<ul style="list-style-type: none"> • If you are having ONTAP clusters 9.6 or earlier, then you are using OnCommand API Services 2.1 or later. <p>You do not require OnCommand API Services to be registered with VASA Provider if you are using ONTAP 9.7 and later.</p> <ul style="list-style-type: none"> • You must have followed the installation instructions that are provided in the <i>OnCommand API Services Installation and Setup guide</i> after downloading and installing OnCommand API Services from the NetApp Support Site. • Each VASA Provider instance must have a dedicated OnCommand API Services instance. <p>OnCommand API Services must not be shared among multiple VASA Provider instances or vCenter Servers.</p> <ul style="list-style-type: none"> • OnCommand API Services is running and accessible.

Considerations	Description
Storage system	<ul style="list-style-type: none"> • You are using ONTAP 9.3 or later. • You are using appropriate credentials for the storage system. • Your storage system is active and accessible. • The virtual machine that you selected must be using at least one vVols datastore, and I/O operations are executing on the disk of the virtual machine.

Manage disaster recovery setup by using Site Recovery Manager

You can create and manage the disaster recovery setup in your vCenter Server by using Site Recovery Manager (SRM) along with VMware's Site Recovery Manager (SRM).

This release of VASA Provider now comes built-in with the capabilities of Storage Repliation Adapter (SRA). If you have configured vVols datastores in your datacenter, then for recovery of vVols datastores, you do not need to install SRA separately for disaster recovery. In Site Recovery Manager(SRM), you must pair the protected and recovery sites. After the site pairing has occurred, the next part of the SRM configuration involves setting up an array pair which enables SRM to communicate with storage system to discover devices and device replication. Before you can configure the array pair, you must first create a site pair in SRM.

Configure VM Storage Policies

You should configure VM storage policies to manage virtual machines that are configured on vVols datastore and to enable services like replication for the virtual disks. For the traditional datastores, it is optional to use these VM storage policies.

About this task

The vSphere web client provides default storage policies. But you can create policies and assign them to the virtual machines.

Steps

1. On the vSphere Client page, click **Menu > Policies and Profiles**.
2. Click **VM Storage Policies > Create VM Storage Policy**.
3. In the Create VM Storage Policy page, provide the following details:
 - a. Enter a name and description for the VM Storage Policy.
 - b. Select **Enable rules for "NetApp clustered Data ONTAP.VP.vvol" storage**.
 - c. Select the required storage capability profile in the **Placement** tab.
 - d. Select the **Custom** option to enable Replication.
 - e. Click **ADD RULE** to select **Asynchronous** replication and required **SnapMirror Schedule**, and then click **NEXT**.
 - f. Verify the compatible datastores listed, and then click **NEXT** in the **Storage compatibility** tab.

For vVols datastores having data protection FlexVol volumes, compatible datastores check is not performed.

4. Review your VM Storage Policy selection in the **Review and finish** tab, and then click **Finish**.

Configure protection groups

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

Before you begin

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

- Same version of SRM installed
- vVols datastore configured with replication enabled and datastore mounted
- Similar storage capability profiles
- Similar VM Storage Policies with replication capability that must be mapped in SRM
- Virtual machines
- Paired protected and recovery sites
- Source and destination datastores should be mounted on respective sites

Steps

1. Log in to your vCenter Server, and then click **Site Recovery > Protection Groups**.
2. In the **Protection Groups** pane, click **New**.
3. Specify a name and description for the protection group, direction, and then click **NEXT**.
4. In the **Type** field, select one of the following:

For...	Type field option...
Traditional datastore	Datastore groups (array-based replication)
vVols datastore	Virtual Volumes (vVol replication)

The fault domain is nothing but SVMs with replication enabled. The SVMs that have only peering implemented and with 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 click **NEXT**.

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

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

Pair protected and recovery sites

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

Before you begin

- You must have installed Site Recovery Manager (SRM) on the protected and recovery sites.
- You must have installed SRA on the protected and recovery sites.

About this task

SnapMirror fan-out configurations are those where a source volume is replicated to two different destinations. These create a problem during recovery when SRM needs to recover the virtual machine from destination.



Storage Replication Adapter (SRA) does not support fan-out SnapMirror configurations.

Steps

1. Double-click **Site Recovery** on the vSphere Client home page, and then click **Sites**.
2. Click **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 click **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 click **Finish**.
5. If prompted, click **Yes** to accept the security certificates.

Results

Both the protected and recovery sites will appear in the Objects dialog box.

Configure protected and recovery site resources

You must 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 must complete the following resource configurations:

- Network mappings
- Folder mappings
- Resource mappings
- Placeholder datastores

Configure network mappings


You must map your networks on the protected site and the recovery site to enable communication between them.

Before you begin

You must have connected the protected and recovery sites.

Steps

1. Log in to your vCenter Server and click on **Site Recovery > Sites**.
2. Select your protected site, and then click **Manage**.
3. In the Manage tab, select **Network Mappings**.

4. Click the  icon to create a new network mapping.

The Create Network Mapping wizard appears.

5. In the Create Network Mapping wizard, perform the following:
 - a. Select **Automatically Prepare Mappings for Networks with Matching Names**, and click **Next**.
 - b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.
 - c. Click **Next** after mappings are created successfully.
 - d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Results

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

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

Before you begin

You must have connected the protected and recovery sites.

Steps

1. Log in to your vCenter Server, and click on **Site Recovery > Sites**.
2. Select your protected site, and then click **Manage**.
3. In the Manage tab, select **Folder Mappings**.
4. Click the  icon to create a new folder mapping.

The Create Folder Mapping wizard appears.

5. In the **Create Folder Mapping** wizard, perform the following:
 - a. Select **Automatically Prepare Mappings for Folders with Matching Names**, and click **Next**.
 - b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.
 - c. Click **Next** after mappings are created successfully.
 - d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Results

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

You must 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 must have connected the protected and recovery sites.

About this task



In Site Recovery Manager (SRM), resources can be resource pools, ESXi hosts, or vSphere clusters.

Steps

1. Log in to your vCenter Server, and click on **Site Recovery > Sites**.
2. Select your protected site, and then click **Manage**.
3. In the Manage tab, select **Resource Mappings**.
4. Click the  icon to create a new resource mapping.

The Create Resource Mapping wizard appears.

5. In the **Create Resource Mapping** wizard, perform the following:
 - a. Select **Automatically Prepare Mappings for Resource with Matching Names**, and click **Next**.
 - b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.
 - c. Click **Next** after mappings are created successfully.
 - d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Results

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.

Map storage policies

You should map the storage policies on the protected site to the storage policies on the recovery site for your recovery plan to place the recovered virtual machines on the appropriate datastores based on your mappings. After the virtual machine is recovered on recovery site, mapped VM Storage Policy will be assigned to virtual machine.

Steps

1. On the vSphere Client, click **Site Recovery > Open Site Recovery**.
2. In the **Site Pair** tab, click **Configure > Storage Policy Mappings**.
3. Select the required site, and then click **New** to create a new mapping.
4. Select the option **Automatically prepare mappings for storage policies with matching names**, and then click **NEXT**.

SRM will select storage policies on the protected site for which a storage policy with the same name exists

on the recovery site. But if you select the manual mapping option, you can select multiple storage policies.

5. Click **Add mappings**, and then click **NEXT**.
6. In the **Reverse mapping** section, select the required check boxes for mapping, and then click **NEXT**.
7. In the **Ready to complete** section, review your selections and click **FINISH**.


Configure placeholder datastores

You must configure a placeholder datastore to hold a place in the vCenter inventory at the recovery site for the protected virtual machine (VM). The placeholder datastore does not need to be large as the placeholder VMs are small and use only a few hundred or fewer kilobytes.

Before you begin

- You must have connected the protected and recovery sites.
- You must have configured your resource mappings.

Steps

1. Log in to your vCenter Server, and click on **Site Recovery > Sites**.
2. Select your protected site, and then click **Manage**.
3. In the Manage tab, select **Placeholder Datastores**.
4. Click the  icon to create a new placeholder datastore.
5. Select the appropriate datastore, and then click **OK**.



Placeholder datastores can be local or remote and should not be replicated.

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

Configure SRA using array manager

You can configure Storage Replication Adapter (SRA) by using the **Array Manager** wizard of Site Recovery Manager (SRM) to enable interactions between SRM and storage virtual machines (SVMs).

Before you begin

- You must have paired the protected sites and recovery sites in SRM.
- You must have configured your storage before configuring the array manager.
- You must have configured and replicated the SnapMirror relationships between the protected sites and recovery sites.
- You must have enabled the SVM management LIFs to enable multitenancy.

About this task

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 of the SVMs in the cluster. If you add storage at an SVM level, then you can manage only that specific SVM.



VMware does not support NFS4.1 protocol for SRM.

Steps

1. In SRM, click **Array Managers**, and then click **Add Array Manager**.
2. Enter the following information to describe the array in SRM:
 - 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 are connecting to a cluster, you should enter the cluster management LIF.
 - If you are connecting directly to an SVM, you should enter the IP address of the SVM management LIF.



When configuring the array manager, you must use the same connection and credentials for the storage system that was used to add the storage system in Virtual Storage Console's **Storage Systems** menu. For example, if the array manager configuration is SVM scoped, then the storage under VSC must be added at SVM level.

- d. If you are connecting to a cluster, enter the name of the SVM in the **SVM name** field.

You can also leave this field blank.

- e. **Optional:** 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. You can enter either the full volume name or the partial volume name.

For example, if you want to discover volume *src_vol1* that is in a SnapMirror relationship with volume *dst_vol1*, you must 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. You can enter either the full volume name or the partial volume name.

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

- g. Enter the user name of the cluster-level account or SVM-level account in the **Username** field.
 - h. Enter the password of the user account in the **Password** field.

3. Click **Next**.
4. Verify that the array is discovered and displayed at the bottom of the **Add Array Manager** window.
5. Click **Finish**.

After you 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

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

Before you begin

- You must have configured your storage system.
- You must have paired the protected site and recovery site by using the SRM array manager.
- You must have enabled FlexClone license and SnapMirror license before performing the test failover operation and failover operation for SRA.

Steps

1. Log in to your vCenter Server.
2. Navigate to **Site Recovery > Array Based Replication**.
3. Select the required SVM, and then verify the corresponding details in the **Array Pairs**.

The storage systems must be discovered at the protected site and recovery site with the Status as “Enabled”.

Protect unprotected virtual machines

You can configure protection for your existing unprotected virtual machines that were created using VM storage Policy with replication disabled. To provide protection, you should change the VM storage policy and assign a replication group.

About this task

If SVM is having both IPv4 and IPv6 LIFs, then you should disable IPv6 LIFs and later perform disaster recovery workflows.

Steps

1. Click the required virtual machine and verify that it is configured with default VM storage policy.
2. Right-click the selected virtual machine, and click **VM Policies > Edit VM Storage Policies**.
3. Select a VM Storage policy that has replication enabled from the **VM storage policy** drop-down.
4. Select a replication group from the **Replication group** drop-down, and then click **OK**.

Verify the Summary of the virtual machine to confirm that the virtual machine is protected.



This release of virtual appliance for VSC, VASA Provider, and SRA does not support hot clone of protected virtual machines. You should power off the virtual machine and then perform the clone operation.

Manage traditional and vVols datastores

You can use the VSC interface to manage both traditional and VMware Virtual Volumes (vVols) datastores and perform mount, resize, edit, and remove datastore operations.

Mount datastore on additional hosts

Mounting a datastore provides storage access to additional hosts. You can mount the datastore on the additional hosts after you add the hosts to your VMware environment.

Before you begin

You must ensure that the subnet details of all the networks to which the ESXi host is connected is entered in the `Kaminoprefs.xml`.

See Enabling datastore mounting across different subnets section in *VSC 9.6 Deployment and Setup Guide*.

Steps

1. From the vSphere Client **Home** page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the host.
3. Repeat Step 2 for any additional hosts.
4. Right-click the host and select **NetApp VSC › Mount Datastores**.
5. Select the datastores that you want to mount, and then click **OK**.

Resize datastores

Resizing a datastore enables you to increase or decrease the storage for your virtual machine files. You might need to change the size of a datastore as your infrastructure requirements change.

Before you begin

If you want VSC to resize the containing volume when it resizes the VMFS datastore, you should not use the **Use existing volume** option under **Storage attributes** section when initially provisioning VMFS datastore, but instead let it automatically create a new volume for each datastore.

About this task

You can increase or decrease the size of an NFS datastore. You can only increase the size of a VMFS datastore.

Steps

1. From the vSphere Client **Home** page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the datastore.
3. Right-click the datastore and select **NetApp VSC › Resize**.
4. In the **Resize** dialog box, specify a new size for the datastore, and then click **OK**.

You can run the **REDISCOVER ALL** option in the **Storage Systems** menu to manually update the storage listing under Storage Systems and dashboard, or wait for the next scheduled refresh.

Edit a vVols datastore

You can edit an existing VMware Virtual Volumes (vVols) datastore to change the default storage capability profile. The default storage capability profile is primarily used for Swap vVols.

Steps

1. From the vSphere Client page, click **Hosts and Clusters**.
2. Right-click the datastore, and then select **NetApp VSC › Edit Properties of vVol Datastore**.

The Edit Properties of vVol Datastore dialog box is displayed.

3. Make the required changes.

You can change the default storage capability profile for the vVols datastore by selecting a new profile from the drop-down list in the Edit vVol Datastore dialog box. You can also change the vVols datastore name and description.



You cannot change the vCenter Server where the vVols datastore is located.

4. When you have made your changes, click **OK**.

A message box asks whether you want to update the vVols datastore.

5. Click **OK** to apply your changes.

A success message appears to inform that the vVols datastore has been updated.

Add storage to a vVols datastore

You can increase the available storage by using the **Add Storage** wizard to add FlexVol volumes to an existing VMWare Virtual Volumes (vVols) datastore.

About this task

When you add a FlexVol volume, you also have the option of changing the storage capability profile associated with that volume. You can either use the VASA Provider auto-generate feature to create a new profile for the volume, or you can assign one of the existing profiles to the volume.



- While expanding a vVols datastore with replication capabilities, you cannot create new FlexVol volumes but can only select pre-configured FlexVol volumes from the existing list.
- When cloning a protected virtual machine deployed on a datastore with vVols replication fails due to insufficient space, then you should increase the FlexVol volume size.
- When a vVols datastore is created on an AFF cluster, then you cannot expand the datastore with another FlexVol volume that has an auto-generated storage capability profile.

You can expand the vVols datastore with FlexVol volumes that have pre-created storage capability profiles.

Steps

1. On the vSphere Client **Home** page, click **Hosts and Clusters**.
2. Right-click the vVols datastore, and then select **NetApp VSC › Expand Storage of vVol Datastore**.
3. On the **Expand Storage of vVol Datastore** page, you can either add an existing FlexVol volume to the vVols datastore, or create a new FlexVol volume to add to the database.

If you select...	Perform the following...
Select volumes	<p>a. Select the FlexVol volumes that you want to add to the vVols datastore.</p> <p>b. In the Storage Capability Profiles column, use the drop-down list to either create a new profile based on the FlexVol volumes, or select one of the existing profiles.</p> <p>The auto-generate feature creates a profile based the storage capabilities that are associated with that FlexVol volume. For example: disk type, high availability, disaster recovery, performance features, and deduplication.</p>
Create new volumes	<p>a. Enter the name, size, and storage capability profile for the FlexVol.</p> <p>The aggregates are selected by the system based on the storage capability profile selected.</p> <p>b. Select the Auto Grow option and provide the maximum size.</p> <p>c. Click ADD to add the FlexVol to the list of volumes.</p>

Reminder: All FlexVol volumes in a vVols datastore must be from the same storage virtual machine (SVM, formerly known as Vserver).

After you create a FlexVol volume, you can edit it by clicking the **Modify** button. You can also delete it.

4. Select a default storage capability profile to be used during virtual machine creation, and then click **Next** to review the summary of the storage added to vVols datastore.
5. Click **Finish**.

The wizard adds the storage that you specified to the vVols datastore. It displays a success message when it finishes.



The **Expand Storage of vVol Datastore** wizard automatically handles any ESXi storage rescans or any other significant operations that are required. Because a vVols datastore is a logical entity controlled by VASA Provider, adding the FlexVol volume is the only thing you need to do to enlarge the capacity of your storage container.

Remove storage from a vVols datastore

If a VMware Virtual Volumes (vVols) datastore has multiple FlexVol volumes, you can remove one or more of the FlexVol volumes from the vVols datastore without deleting the datastore.

About this task

A vVols datastore exists until there is at least one FlexVol volume on the datastore.

Steps

1. From the vSphere Client **Home** page, click **Hosts and Clusters**.
2. Right-click the vVols datastore that you want to modify, and then select **NetApp VSC › Remove Storage from vVol Datastore**.

The **Remove Storage from vVol Datastore** dialog box is displayed.

3. Select the FlexVol volumes that you want to remove from the vVols datastore, and click **Remove**.
4. Click **OK** in the confirmation dialog box.



If you select all of the FlexVol volumes, an error message is displayed, indicating that the operation will fail.

Mount a vVols datastore

You can mount a VMware Virtual Volumes (vVols) datastore to one or more additional hosts by using the Mount vVol Datastore dialog box. Mounting the datastore provides storage access to additional hosts.

Steps

1. From the vSphere Client **Home** page, click **Hosts and Clusters**.
2. Right-click the datastore that you want to mount, and then select **NetApp VSC › Mount vVol Datastore**.

The **Mount vVol Datastore** dialog box is displayed, which provides a list of the hosts that are available in the datacenter where you can mount the datastore. The list does not include the hosts on which the datastore has already been mounted, hosts that are running ESX 5.x or earlier, or hosts that do not support the datastore protocol. For example, if a host does not support the FC protocol, you cannot mount an FC datastore to the host.



Even though the vSphere Client provides a mount dialog box for the vCenter Server, you must always use the VASA Provider dialog box for this operation. VASA Provider sets up access to storage systems that are running ONTAP software.

3. Select the host on which you want to mount the datastore, and then click **OK**.

Considerations for migrating or cloning virtual machines

You should be aware of some of the considerations while migrating existing virtual machines in your datacenter.

Migrate protected virtual machines

You can migrate the protected virtual machines to:

- Same vVols datastore in a different ESXi host
- Different compatible vVols datastore in same ESXi host

- Different compatible vVols datastore in a different ESXi host

If virtual machine is migrated to different FlexVol volume, then respective metadata file also gets updated with the virtual machine information. If a virtual machine is migrated to a different ESXi host but same storage then underlying FlexVol volume metadatafile will not be modified.

Clone protected virtual machines

You can clone protected virtual machines to the following:

- Same container of same FlexVol volume using replication group

Same FlexVol volume's metadata file is updated with the cloned virtual machine details.

- Same container of a different FlexVol volume using replication group

The FlexVol volume where the cloned virtual machine is placed, the metadata file gets updated with the cloned virtual machine details.

- Different container or vVols datastore

The FlexVol volume where the cloned virtual machine is placed, the metadata file gets updated virtual machine details.

VMware presently does not support virtual machine cloned to a VM template.

Clone-of-Clone of a protected virtual machine is supported.

Virtual Machine snapshots

Presently only virtual machine Snapshots without memory are supported. If virtual machine has Snapshot with memory, then the virtual machine is not considered for protection.

You also cannot protect unprotected virtual machine that has memory Snapshot. For this release, you are expected to delete memory snapshot before enabling protection for the virtual machine.

Migrate traditional virtual machines to vVols datastores

You can migrate virtual machines from traditional datastores to Virtual Volumes (vVols) datastores to take advantage of policy-based VM management and other vVols capabilities. vVols datastores enable you to meet increased workload requirements.

Before you begin

You must have ensured that VASA Provider is not running on any of the virtual machines that you plan to migrate. If you migrate a virtual machine that is running VASA Provider to a vVols datastore, you cannot perform any management operations, including powering on the virtual machines that are on vVols datastores.

About this task

When you migrate from a traditional datastore to a VVol datastore, the vCenter Server uses vStorage APIs for Array Integration (VAAI) offloads when moving data from VMFS datastores, but not from an NFS VMDK file. VAAI offloads normally reduce the load on the host.

Steps

1. Right-click the virtual machine that you want to migrate, and then click **Migrate**.
2. Select **Change storage only**, and then click **Next**.
3. Select a virtual disk format, a VM Storage Policy, and a VVol datastore that matches the features of the datastore that you are migrating, and then click **Next**.
4. Review the settings, and then click **Finish**.

Migrate virtual machines with older storage capability profiles

If you are using the latest version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), then you should migrate your virtual machines that are provisioned with the “MaxThroughput MBPS” or “MaxThroughput IOPS” QoS metrics to new VVol datastores that are provisioned with the “Max IOPS” QoS metrics of the latest version of the virtual appliance for VSC, VASA Provider, and SRA.

About this task

With the latest version of the virtual appliance for VSC, VASA Provider, and SRA, you can configure QoS metrics for each virtual machine or virtual machine disk (VMDK). The QoS metrics were earlier applied at the ONTAP FlexVol volume level and were shared by all of the virtual machines or VMDKs that were provisioned on that FlexVol volume.

Starting with the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA, the QoS metrics of one virtual machine is not shared with other virtual machines.



You must not modify the existing VM Storage Policy as the virtual machines might become non-compliant.

Steps

1. Create VVol datastores by using a new storage capability profile with the required “Max IOPS” value.
2. Create a VM Storage Policy, and then map the new VM Storage Policy with the new storage capability profile.
3. Migrate the existing virtual machines to the newly created VVol datastores by using the new VM Storage Policy.

Understand Virtual Storage Console reports

You can use the Virtual Storage Console (VSC) **Reports** menu to view pre-defined reports for all the datastores managed by a selected VSC instance in a particular vCenter Server. You can perform operations such as sorting and exporting reports.

What reports do

Reports display detailed information about datastores and virtual machines, that enables you to review and identify potential issues with datastores and virtual machines in your vCenter Server.

You can view, sort, and export reports.

Virtual Storage Console (VSC) provides the following pre-defined reports:

- Datastore Report
- Virtual Machine Report
- VVol Datastore Report
- VVol Virtual Machine Report

Datastore Reports

The datastore reports provide detailed information about traditional datastores and the virtual machines that are created on these datastores.

The traditional dashboard enables you to review and identify potential issues with the datastores and virtual machines in your vCenter Server. You can view, sort, and export reports. The data for the traditional datastores and virtual machines report is provided by the vCenter Server.

The datastore provides the following pre-defined reports:

- Datastore Report
- Virtual Machine Report

Datastore Report

The Datastore Report menu provides information on the following parameters for datastores:

- Name of the datastore
- Type of datastore: NFS or VMFS
- Free space
- Used space
- Total space
- Percentage of space utilized
- Percentage of space available
- IOPS

The report displays the IOPS for the datastore.

- Latency

The report displays the latency information for the datastore.

You can also verify the time at which the report was generated. The Datastore Report menu enables you to organize the report as per your requirement, and then export the organized report using the **Export to CSV** button. The datastore names in the report are links that navigate to the Monitor tab of the selected datastore, where you can view the datastore performance metrics.

Virtual Machine Report

The Virtual Machine Report menu provides the following performance metrics for all the virtual machines that use datastores provisioned by VSC for a selected vCenter Server:

- Name of the virtual machine
- Committed capacity

The report displays the value for the committed capacity for a virtual machine.

- Uptime

The report displays the time for which the virtual machine is powered on and is available on an ESXi host.

- Latency

The report displays the latency for virtual machines across all datastores associated with the virtual machines.

- Power state

The report displays whether the virtual machine is powered on or powered off.

- Host

The report displays the host systems on which the virtual machine is available.

Each virtual machine name in the report is a link to the Monitor tab of the selected virtual machine. You can sort the virtual machine report as per your requirement and export the report in a .CSV file, and save the report on your local system. The timestamp of the report is also appended to the saved report.

vVols reports

vVols reports display detailed information about VMware Virtual Volumes (vVols) datastores and the virtual machines that are created on these datastores. The vVol dashboard enables you to review and identify potential issues with the vVols datastores and virtual machines in your vCenter Server.

You can view, organize, and export reports. The data for the vVols datastores and virtual machines report is provided by the ONTAP along with OnCommand API Services.

vVols provides the following pre-canned reports:

- vVol Datastore Report
- vVol VM Report

vVol Datastore Report

The **vVol Datastore Report** menu provides information about the following parameters for datastores:

- vVols datastore name
- Free space
- Used space
- Total space
- Percentage of space utilized

- Percentage of space available
- IOPS
- Latency

You can also verify the time at which the report was generated. The **vVol Datastore Report** menu enables you to organize the report as per your requirement, and then export the organized report by using the **Export to CSV** button. Each SAN vVols datastore name in the report is a link that navigates to the **Monitor** tab of the selected SAN vVols datastore, which you can use to view the performance metrics.

vVols Virtual Machine Report

The **vVol Virtual Machine Summary Report** menu provides the following performance metrics for all of the virtual machines that use the SAN vVols datastores that are provisioned by VASA Provider for ONTAP for a selected vCenter Server:

- Name of the virtual machine
- Committed capacity
- Uptime
- Throughput

The report displays whether the virtual machine is powered on or powered off.

- Logical space
- Host
- Power state
- Latency

The report displays the latency for virtual machines across all of the vVols datastores that are associated with the virtual machines.

Each virtual machine name in the report is a link to the **Monitor** tab of the selected virtual machine. You can organize the virtual machine report according to your requirement, export the report in .CSV format, and then save the report on your local system. The timestamp of the report is appended to the saved report.

Troubleshoot issues with the virtual appliance for VSC, VASA Provider, and SRA

If you encounter unexpected behavior during the configuration or management of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), then you can follow specific troubleshooting procedures to identify and resolve the cause of such issues.

Collect the log files

You can collect log files for Virtual Storage Console for VMware vSphere from the option available in the VSC graphical user interface (GUI). Technical support might ask you to collect the log files to help troubleshoot a problem.

About this task

If you need VASA Provider log files, you can generate a support bundle from the **Vendor Provider Control Panel** screen. This page is part of the VASA Provider maintenance menus, which are accessible from the virtual appliance's console.

https://vm_ip:9083

You can collect the VSC log files by using the “Export VSC Logs” feature in the VSC GUI. When you collect a VSC log bundle with VASA Provider enabled, the VSC log bundle will also have the VP logs. The following steps tell you how to collect the VSC log files:

Steps

1. From the Virtual Storage Console home page, click **Configuration › Export VSC Logs**.

This operation can take several minutes.

2. When prompted, save the file to your local computer.

You can then send the .zip file to technical support.

Issue while editing VM Storage Policies after upgrade

After upgrading from the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) to the latest version of the virtual appliance for VSC, VASA Provider, and SRA, if you attempt to edit an existing VM Storage Policy before you configure any new storage capability profiles, the following error message might be displayed: There are incorrect or missing values below.

Cause

You might get this error if you have not created any new storage capability profiles.

Corrective action

You must perform the following:

1. Stop editing the VM Storage Policy.
2. Create a new storage capability profile.
3. Modify the required VM Storage Policy.

VASA Provider status shows as “Offline” in vCenter Server GUI

The status of VASA Provider for ONTAP might appear as “Offline” in the vCenter Server GUI after you restart the VASA Provider service.

Workaround

1. Check the status of VASA Provider from the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), and ensure that VASA Provider is active.

2. In the VSC page of vCenter Server, verify that VASA Provider is enabled by navigating to **Configuration > Manage Extensions**.
3. On the vCenter Server, check the `/var/log/vmware/vmware-sps/sps.log` file for any connection errors with VASA Provider.
4. If there are any errors, restart the “vmware-sps” service.

Error while accessing the VSC Summary page of virtual appliance

The error message `/opt/netapp/vscserver/etc/vsc/performance.json` (No such file or directory) might be displayed when you try to access the VSC Summary page after you deploy the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA).

Description

When you try to access the VSC dashboard after the deployment of the virtual appliance for VSC, VASA Provider, and SRA, you might encounter an error because the scheduler initialization process is not complete.

Workaround

You must wait for a few seconds after the deployment of the virtual appliance for the performance scheduler initialization process to complete, and then click the  button to get the latest data.

Error deleting a datastore after network settings are changed

Issue

After changing the IP address of the virtual appliance for VSC, VASA Provider, and SRA, an error is displayed while using the VSC interface to perform certain operations. For example, deleting a datastore or trying to access VASA Provider server on ESXi host.

Cause

The vCenter Server does not use the updated IP address and continues to use the old IP address to make calls to VASA Provider.

Corrective action

When IP address of the virtual appliance for VSC, VASA Provider, and SRA changes, you should perform the following:

1. Unregister VSC from vCenter Server.
2. Access https://<vcenter_ip>/mob.
3. Click **Content > Extension Manager > Unregister Extension > Unregister all com.netapp.extensions**.
4. Log in to the vCenter Server as root using putty.
5. Change to the `vsphere-client-serenity` directory using: `cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`.
6. Stop the vSphere Client: service using `vsphere-client stop`.

7. Remove the directories containing the UI extensions: `rm -rf com.netapp*`

8. Start the vSphere Client: service using `vsphere-client start`.

This operation can take several minutes for the vSphere Client to restart and initialize correctly.

9. Change to the vsphere-ui serenity directory using: `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`.

10. Stop the vSphere UI: service using `vsphere-ui stop`.

11. Remove the directories containing the UI extensions: `rm -rf com.netapp*`

12. Start the vSphere UI using: `service-control --start vsphere-ui`.

Datastore inaccessible when volume status is changed to offline

Issue

When a volume of a datastore is made offline, the datastore is inaccessible. Even if you bring the volume online, VSC fails to discover the datastore. On the vSphere Client, if you right-click the datastore, no VSC actions are available.

Cause

When volume is made offline from the cluster, the volume is unmounted first and then made offline or restricted. The junction path is removed when the volume is made offline and the datastore becomes inaccessible. If the volume is made online, the junction path is not available and not mounted on the by default. This is the ONTAP behavior.

Corrective action

You should bring the volume online and then manually mount the volume with the same junction path as before. You can run the storage discovery to view that the datastore is discovered and actions for the datastore are available.

Add storage system with IPv4 results in authentication error with IPv6 status in storage system grid

Issue

The storage system grid displays authentication failure status with IPv6 address for a storage system even though the storage system is added with IPv4 address.

Cause

When you have a dual stack storage system with IPv4 and IPv6 LIFs and you add a storage system with IPv4 LIF, then during the periodic discovery process, VSC can discover the IPv6 LIF too. This IPv6 discovery fails with authentication error as the IPv6 LIF is not added explicitly. This error does not have any impact on any of the operations performed for the storage system.

Corrective action

You must perform the following:

1. In the VSC home page, click **Storage Systems**.
2. Click the storage system that has unknown status with IPv6 address.
3. Change the IP address to IPv4 using the set default credentials.
4. Click **Back to listing**, and then click **REDISCOVER ALL**.

The stale IPv6 entry from the storage systems list is deleted and storage system is discovered without authentication errors.

File creation error while provisioning virtual machines on VVol datastores

Issue

Cannot create virtual machine using the default storage virtual machine (SVM) or any mixed storage virtual machine (SVM) that has both IPv6 and IPv4 data LIFS configured.

Cause

The issue occurs because the default vs0 has both IPv6 and IPv4 data LIFs, and is not a purely IPv4 datastore.

Corrective action

You can provision a virtual machine with vs0 using the following steps:

1. Use System Manager application to disable all the IPv6 LIFs .
2. Rediscover the cluster.
3. Provision a virtual machine on the VVol datastore on which the provisioning was failing.

The virtual machine is successfully provisioned.

Incorrect status 'Failover in Progress' is reported for SRA in SRM

Issue

VMware Site Recovery Manager (SRM) displays the status of the device as “In progress” for the newly SnapMirrored device.

Cause

This issue occurs due to the presence of an entry with the same device name as the newly created device in the `/opt/netapp/vpserver/conf/devices.txt` file.

Corrective action

You should manually delete the entries matching the device that you newly created from both the sites (site A and site B) from located at `/opt/netapp/vpserver/conf/devices.txt` and rerun discover devices. After the discovery completes, the devices will display the correct status.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.