Manage ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
December 02, 2025

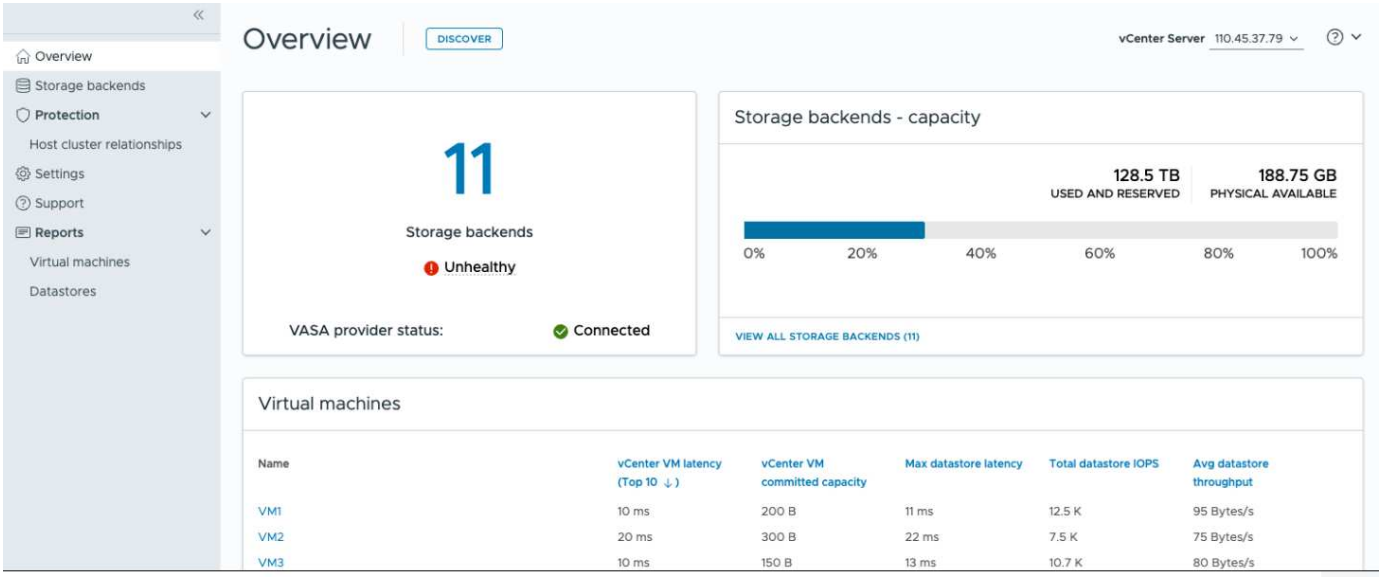
Table of Contents

Manage ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere dashboard overview

When you select the ONTAP tools for VMware vSphere plug-in icon in the shortcuts section on the vCenter client, the user interface navigates to the overview page. This page acts like the dashboard providing you the summary of the ONTAP tools for VMware vSphere plug-in.

In the case of Enhanced Linked Mode setup (ELM), the vCenter Server select dropdown appears and you can select a desired vCenter Server to see the data relevant to it. This dropdown is available for all the other listing views of the plugin. vCenter Server selection made in one page persists across the tabs of the plug-in.



From the overview page, you can run the **Discovery** action. Discovery action runs the discovery at vCenter level to detect any newly added or updated storage backends, hosts, datastores, and protection status/relationships. You can run an on-demand discovery of entities without having to wait for the scheduled discovery.

Action button will be enabled only if you have the privilege to perform the discovery action.

After the discovery request is submitted, you can track the progress of the action in the recent tasks panel.

The dashboard has several cards showing different elements of the system. The following table shows the different cards and what they represent.

Card	Description

Status	The Status card shows the number of storage backends and the overall health status of the storage backends and the VASA Provider. Storage backends status shows **Healthy** when all the storage backends status is normal and it shows **Unhealthy** if any one of the storage backends has an issue (Unknown/Unreachable/Degraded status). Select the tool tip to open the status details of the storage backends. You can select any storage backend for more details. **Other VASA Provider states** link shows the current state of the VASA Provider that is registered in the vCenter Server.
Storage Backends - Capacity	This card shows the aggregated used and available capacity of all storage backends for the selected vCenter Server instance. In case of ASA r2 storage systems, the capacity data is not shown because it is a disaggregated system.
Virtual machines	This card shows the top 10 VMs sorted by performance metric. You can select the header to get the top 10 VMs for the selected metric sorted by either ascending or descending order. The sorting and filtering changes made on the card persists until you change or clear the browser cache.
Datastores	This card shows the top 10 datastores sorted by a performance metric. You can select the header to get the top 10 datastores for the selected metric sorted by either ascending or descending order. The sorting and filtering changes made on the card persists until you change or clear the browser cache. There is a Datastore type drop-down to select the type of the datastores - NFS, VMFS, or vVols.
ESXi Host compliance card	This card shows overall compliance status of all ESXi hosts (for the selected vCenter) settings with respect to the recommended NetApp host settings by settings group/category. You can select **Apply Recommended Settings** link to apply the recommended settings. You can select the compliant status of the hosts to see the list of hosts.

ONTAP tools Manager user interface

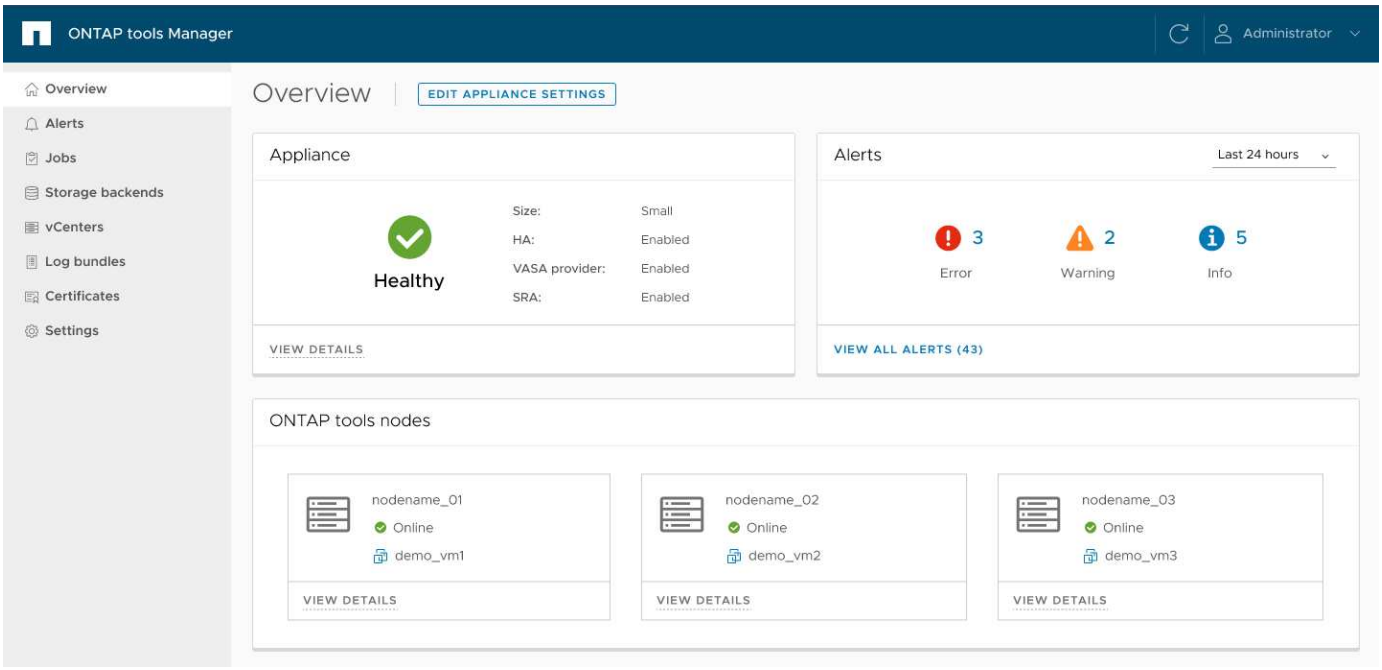
ONTAP tools for VMware vSphere is a multi-tenant system that can manage multiple vCenter Server instances. ONTAP tools Manager provides more control to the ONTAP tools for VMware vSphere administrator over the managed vCenter Server instances and onboarded storage backends.

ONTAP tools Manager helps in:

- vCenter Server instance management - Add and manage vCenter Server instances to ONTAP tools.
- Storage backend management - Add and manage ONTAP storage clusters to ONTAP tools for VMware vSphere and map them to onboarded vCenter Server instances globally.
- Log bundle downloads - Collect log files for ONTAP tools for VMware vSphere.
- Certificate management - Change the self-signed certificate to a custom CA certificate and renew or refresh all certificates of VASA Provider and ONTAP tools.
- Password management - Reset the user's OVA application password.

To access ONTAP tools Manager, launch `https://<ONTAPtoolsIP>:8443/virtualization/ui/` from the browser and login with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.

The ONTAP tools Manager overview section helps manage the appliance configuration, such as services management, node size upscaling, and High availability(HA) enablement. You can also monitor the overall information of ONTAP tools related to the node(s), such as health, network details, and alerts.



Card	Description
Appliance card	The appliance card provides the overall status of the ONTAP tools appliance. It shows the appliance configuration details and the status of the enabled services. For additional information about the ONTAP tools appliance, select the **View details** link. When an edit appliance setting action job is in progress, the appliance portlet shows the status and details of the job.
Alerts card	The Alerts card lists the ONTAP tools alerts by type, including the HA node-level alerts. You can view the list of alerts by selecting on the count text (hyperlink). The link routes you to the alerts view page filtered by the selected type.

Card	Description
vCenters	The vCenter card shows the health status of the vCenters in the system.
Storage backends	The Storage backends card shows the health status of the Storage backends in the system.
ONTAP tools nodes card	ONTAP tools nodes card shows the list of nodes with node name, node VM name, status, and all the network related data. You can select on **View details** to view the additional details related to the selected node. [NOTE] In a non-HA setup, only one node is shown. In the HA setup, three nodes are shown.

Understand igroups and export policies in ONTAP tools for VMware vSphere

Initiator groups (igroups) are tables of FC protocol host World Wide Port Name (WWPNs) or iSCSI host qualified node names. You can define igroups and map them to LUNs to control which initiators have access to LUNs.

In ONTAP tools for VMware vSphere 9.x, igroups were created and managed in a flat structure, where each datastore in vCenter was associated with a single igroup. This model limited flexibility and reuse of igroups across multiple datastores. ONTAP tools for VMware vSphere 10.x introduces nested igroups, where each datastore in vCenter is associated with a parent igroup, while each host is linked to a child igroup under that parent. You can define custom parent igroups with user-defined names for reuse across multiple datastores, enabling more flexible and interconnected management of igroups. Understanding the igroup workflow is essential for managing LUNs and datastores effectively in ONTAP tools for VMware vSphere. Different workflows generate varying igroup configurations, as shown in the following examples:

The names mentioned are for illustration purposes only and do not refer to real igroup names. ONTAP tools managed igroups use the prefix “otv_”. Custom igroups can be given any name.

Term	Description
DS<number>	Datastore
iqn<number>	Initiator IQN
host<number>	Host MoRef
lun<number>	LUN ID
<DSName>Igroup<number>	Default (ONTAP tools-managed) parent igroup
<Host-Moref>Igroup<number>	Child igroup
CustomIgroup<number>	User-defined custom parent igroup
ClassicIgroup<number>	Igroup used in ONTAP tools 9.x versions.

Example 1:

Create datastore on a single host with one initiator

Workflow: [Create] DS1 (lun1): host1 (iqn1)

Result:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)

A parent igroup DS1Igroup is created on the ONTAP systems for DS1, with a child igroup host1Igroup mapped to lun1. LUNs are always mapped to child igroups.

Example 2:

Mount existing datastore to an additional host

Workflow: [Mount] DS1 (lun1): host2 (iqn2)

Result:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

A child igroup host2Igroup is created and added to the existing parent igroup DS1Igroup.

Example 3:

Unmount a datastore from a host

Workflow: [Unmount] DS1 (lun1): host1 (iqn1)

Result:

- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

The host1Igroup is removed from the hierarchy. Child igroups are not explicitly deleted. Deletion occurs under these two conditions:

- If no LUNs are mapped, the ONTAP system deletes the child igroup.
- A scheduled cleanup job removes the dangling child igroups with no LUN mappings. These scenarios only apply to ONTAP tools-managed igroups, not custom-created ones.

Example 4:

Delete datastore

Workflow: [Delete] DS1 (lun1): host2 (iqn2)

Result:

- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

Parent and child igroups are removed if another datastore does not reuse the parent igroup. Child igroups are never explicitly deleted

Example 5:

Create multiple datastores under a custom parent igroup

Workflow:

- [Create] DS2 (lun2): host1 (iqn1), host2 (iqn2)
- [Create] DS3 (lun3): host1 (iqn1), host3 (iqn3)

Result:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

CustomIgroup1 is created for DS2 and reused for DS3. Child igroups are created or updated under the shared parent, with each child igroup mapping to its relevant LUNs.

Example 6:

Delete one datastore under a custom parent igroup.

Workflow: [Delete] DS2 (lun2): host1 (iqn1), host2 (iqn2)

Result:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun3)
  - host3Igroup → (iqn3: lun3)
- Even though CustomIgroup1 is not reused, it is not deleted.
- If no LUNs are mapped, the ONTAP system deletes host2Igroup.
- host1Igroup is not deleted because it is mapped to lun3 of DS3. Custom igroups are never deleted, regardless of the reuse status.

Example 7:

Expand vVols datastore (Add Volume)

Workflow:

Before expansion:

[Expand] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

After expansion:

[Expand] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

A new LUN is created and mapped to the existing child igroup host4Igroup.

Example 8:
Shrink vVols datastore (Remove Volume)

Workflow:

Before Shrink:

[Shrink] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

After Shrink:

[Shrink] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

The specified LUN (lun5) is unmapped from the child igroup. The igroup remains active as long as it has at least one mapped LUN.

Example 9:
Migration from ONTAP tools 9 to 10 (igroup normalization)

Workflow

ONTAP tools for VMware vSPhere 9.x versions do not support hierarchical igroups. During migration to 10.3 or above versions, igroups must be normalized into the hierarchical structure.

Before migration:

[Migration] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

ONTAP tools 9.x logic allows multiple initiators per igroup without enforcing one-to-one host mapping.

After migration:

[Migration] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicIgroup1: otv_ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

During migration:

- A new parent igroup (ClassicIgroup1) is created.
- The original igroup is renamed with otv_ prefix and becomes a child igroup.

This ensures compliance with the hierarchical model.

Related topics
About igroups

Export policies

Export policies control access to NFS datastores in ONTAP tools for VMware vSphere. They define which clients can access the datastores and what permissions they have. Export policies are created and managed in ONTAP systems and can be associated with NFS datastores to enforce access control. Each export policy consists of rules that specify the clients (IP addresses or subnets) that are allowed access and the permissions granted (read-only or read-write).

When you create an NFS datastore in ONTAP tools for VMware vSphere, you can select an existing export policy or create a new one. The export policy is then applied to the datastore, ensuring only authorized clients can access it.

When you mount an NFS datastore on a new ESXi host, ONTAP tools for VMware vSphere adds the host's IP address to the existing export policy associated with the datastore. This allows the new host to access the datastore without creating a new export policy.

When you delete or unmount an NFS datastore from an ESXi host, ONTAP tools for VMware vSphere removes the host's IP address from the export policy. If no other hosts are using that export policy, it will be deleted. When you delete an NFS datastore, ONTAP tools for VMware vSphere removes the export policy associated with that datastore if it is not reused by any other datastores. If the export policy is reused, it retains the host IP address and remains unchanged. When you delete the datastores, the export policy unassigns the host IP address and assigns a default export policy, so that the ONTAP systems can access them if required.

Assigning the export policy differs when it is reused across different datastores. When you reuse the export policy, you can append the policy with the new host IP address. When you delete or unmount a datastore that uses a shared export policy, the policy will not be deleted. It remains unchanged, and the host IP address is not removed, because it is shared with the other datastores. Reusing export policies is not recommended, because it can lead to access and latency issues.

Related topics

Create an export policy

Understand ONTAP tools managed igroups

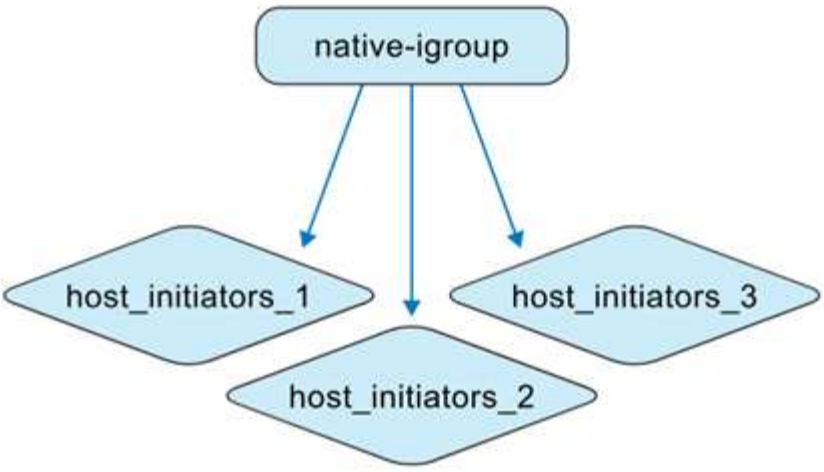
When managing both ONTAP tools VMs and ONTAP storage systems, understanding igroup behavior is essential, especially when migrating datastores from non-ONTAP tools environments to ONTAP tools management. This section describes how igroups are updated during this transition.

ONTAP tools for VMware vSphere 10.4 simplifies datastore management by automating the creation and maintenance of ONTAP and vCenter objects within VMware datacenter environments.

ONTAP tools for VMware vSphere 10.4 interprets igroups in two different contexts:

Non-ONTAP tools managed igroups

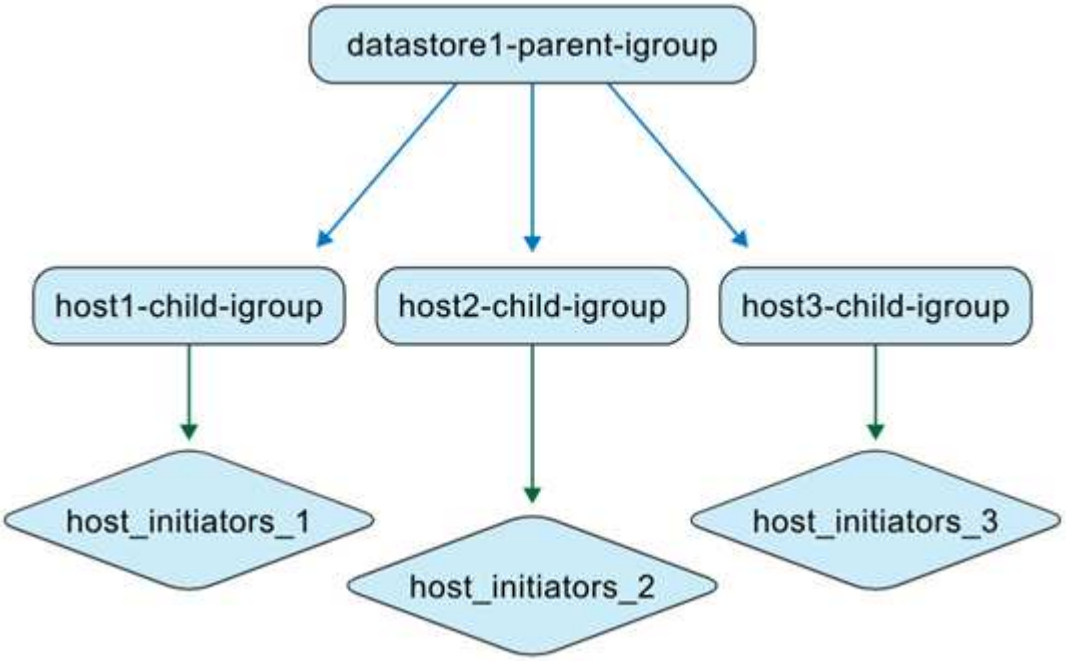
As a storage administrator, you can create igroups on the ONTAP system as flat or nested structures. The illustration shows a flat igroup created in the ONTAP system.

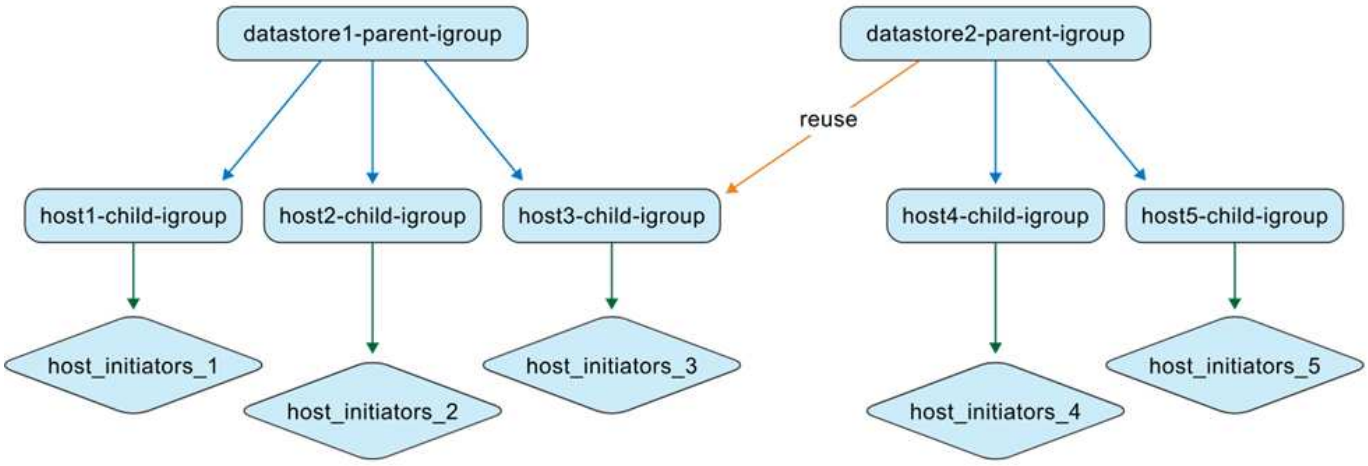


ONTAP tools managed igroups

When you create datastores, ONTAP tools for VMware vSphere 10.4 automatically creates igroups using a nested structure for easier LUN mapping.

For example, when datastore1 is created and mounted on hosts 1, 2, and 3, and a new datastore (datastore2) is created and mounted on hosts 3, 4, and 5, ONTAP tools reuses the host-level igroup for efficient management.





Here are some cases for ONTAP tools for VMware vSphere supported igroups.

When you create a datastore with default igroup settings

When you create a datastore and leave the igroup field blank (default setting), ONTAP tools automatically generates a nested igroup structure for that datastore. The parent igroup at the datastore level is named using the pattern: otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>. Each host-level child igroup follows the pattern: otv_<hostMoref>_<vcguid>. You can view the association between parent (datastore-level) and child (host-level) igroups in the **Parent Initiator Group** section of the ONTAP storage interface.

With the nested igroup approach, LUNs are mapped only to the child igroups. vCenter Server inventory then displays the new datastore.

When you create a datastore with a custom igroup name

During datastore creation in ONTAP tools, you can enter a custom igroup name instead of selecting from the dropdown. ONTAP tools then creates a parent igroup at the datastore level using your specified name. If the same host is used for multiple datastores, the existing host-level (child) igroup is reused. As a result, the LUN for the new datastore is mapped to this existing child igroup, which might now be associated with multiple parent igroups (one for each datastore). The vCenter Server user interface datastore list confirms the successful creation of the new datastore with the custom igroup name.

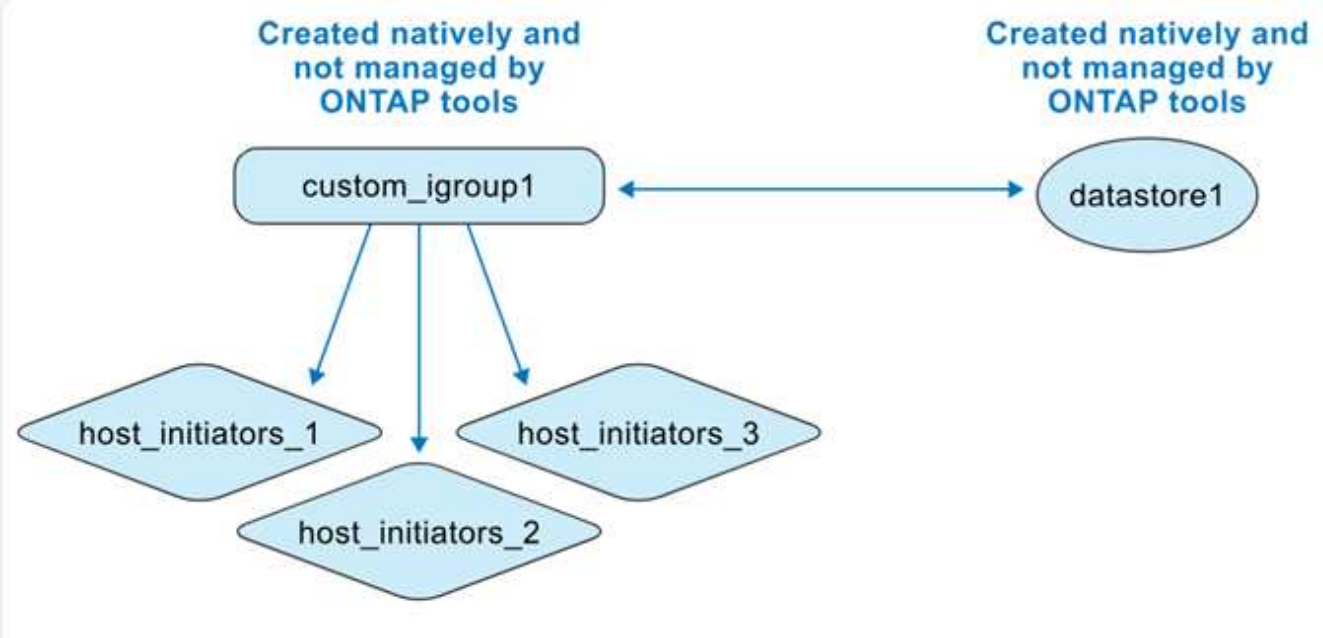
When you reuse the igroup name during datastore creation

When creating a datastore using the ONTAP tools user interface, you can choose an existing custom parent igroup from the drop-down list. After reusing the parent igroup to create another datastore, the ONTAP systems user interface shows this association. The new datastore also appears in the vCenter Server user interface.

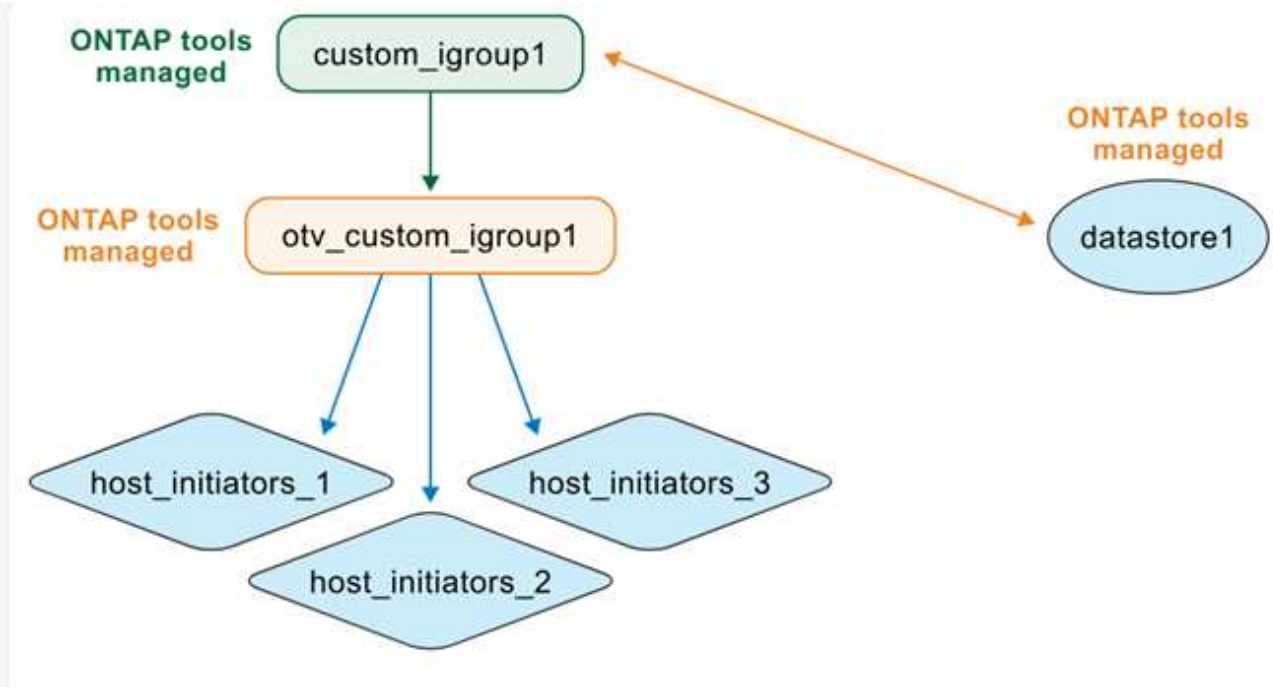
This operation can also be performed using the API. To reuse an existing igroup during datastore creation, specify the igroup UUID in the API request payload.

When you create a datastore and igroup natively from ONTAP and vCenter

If you create the igroup and datastore directly in ONTAP systems and VMware environments, ONTAP tools does not manage these objects at first. This creates a flat igroup structure.



To manage an existing datastore and igroup with ONTAP tools, you should perform a datastore discovery. ONTAP tools identifies and registers the datastore and igroup, and converts them to a nested structure in its database. A new parent igroup is created using the custom name, while the existing igroup is renamed with the "otv_" prefix and becomes the child igroup. The initiator mappings remain unchanged. Only igroups mapped to datastores are converted during discovery. After this, the igroup structure looks like the illustration below.



You can create a datastore directly in vCenter Server and later bring it under ONTAP tools management. First, create a flat igroup in ONTAP systems and map a LUN to it. After running datastore discovery in ONTAP tools, the flat igroup is converted to a nested structure. ONTAP tools then manages the igroup, renaming it with the 'otv_' prefix. The LUN remains mapped to the same igroup throughout this process.

How ONTAP tools reuse igroups created natively

You can provision a datastore in ONTAP tools using an igroup originally created in ONTAP systems, after it is

managed by ONTAP tools. These igroups appear in the custom initiator group name drop-down list. The new LUN for the datastore is then mapped to the corresponding normalized child igroup, such as "otv_NativeIgroup1".

ONTAP tools for VMware vSphere does not detect or use igroups created in ONTAP system that are not managed by ONTAP tools or linked to a datastore.

Enable ONTAP tools for VMware vSphere services

You can change the administrator password using ONTAP tools Manager to enable services like VASA Provider, import of vVols configuration, and disaster recovery (SRA) using ONTAP tools Manager.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Edit Appliance Settings** in the overview section.
4. In the **Services** section, you can enable optional services like VASA Provider, import of vVols configuration, and disaster recovery (SRA) as per your requirement.

   When enabling the services for the first time, you must create the VASA Provider and SRA credentials. These are used to register or enable the VASA Provider and SRA services on the vCenter Server. The username can only contain letters, numbers, and underscores. Password length should be between 8 and 256 characters.

   Before disabling any optional services, ensure that the vCenter Servers managed by ONTAP tools do not use them.

   The **Allow import of vVols configuration** option is shown only when the VASA Provider service is enabled. This option enables the vVols data migration from ONTAP tools 9.xx to ONTAP tools 10.4.

Change ONTAP tools for VMware vSphere configuration

Using the ONTAP tools Manager scale up the ONTAP tools for VMware vSphere configuration to increase the number of nodes in the deployment or change the configuration to High Availability (HA) setup. The ONTAP tools for VMware vSphere appliance is initially deployed in a single node non-HA configuration.

To migrate to HA when non-HA backup is enabled, disable the backup first and re-enable it after the migration.

Before you begin

- Ensure that your OVA template has the same OVA version as Node 1. Node 1 is the default node where the ONTAP tools for VMware vSphere OVA is initially deployed.
- Ensure the CPU hot add and memory hot plug are enabled.

- In the vCenter Server, set the Disaster Recovery Service (DRS) automation level to partially automated. After deploying HA, revert it to fully automated.
- Node hostnames in the HA setup should be in lowercase.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Edit Appliance Settings** in the overview section.
4. In the **Configuration** section, you can scale up to increase the node size and enable HA configuration as per your requirement. You need the vCenter Server credentials to make any changes.

   When ONTAP tools is in HA configuration, you can change the content library details. You should provide the password again for the new edit submission.

   > In ONTAP tools for VMware vSphere, you are only allowed to increase the node size; you cannot reduce the node size. In a non-HA setup, only a medium-size configuration is supported. In an HA setup, medium and large configurations are supported.

5. Use the HA toggle button to enable the HA configuration. On the **HA settings** page, ensure that:
   - The content library belongs to the same vCenter Server where the ONTAP tools node VMs run. vCenter Server credentials are used to validate and download the OVA template for appliance changes.
   - The virtual machine hosting the ONTAP tools is not directly deployed on an ESXi host. The VM should be deployed on a cluster or a resource pool.

   > After the HA configuration is enabled, you cannot revert to a non-HA single node configuration.

6. In the **HA settings** section of the **Edit Appliance Settings** window, you can enter the details of Nodes 2 and 3. ONTAP tools for VMware vSphere supports three nodes in HA setup.

   > Most of the input options are pre-filled with Node 1 network details for ease of workflow. However, you can edit the input data before navigating to the wizard's final page. You can enter IPv6 address details for the other two nodes only when the IPv6 address is enabled on the ONTAP tools management node.

   Ensure that an ESXi host contains only one ONTAP tools VM. The inputs are validated each time you move to the next window.

7. Review the details in the **Summary** section and **Save** the changes.

What's next?

The **Overview** page shows the deployment's status. Using the job ID, you can also track the edit appliance settings job status from the jobs view.

If HA deployment fails and the status of the new node shows as 'New,' then delete the new VM in the vCenter before retrying the enable HA operation.

The **Alerts** tab on the left panel lists alerts for ONTAP tools for VMware vSphere.

Add new VMware vSphere hosts

Add new VMware vSphere hosts to ONTAP tools for VMware vSphere to manage and protect datastores on the hosts.

Steps

1. Add a host to your VMware vSphere cluster following the workflow on page: How to Add an ESX Host to Your vSphere Cluster by Using the Quickstart Workflow
2. After adding the host, go to the ONTAP tools main menu and select **Discover** in the overview panel. Wait for the discovery process to finish. Alternatively, you can wait for the scheduled host discovery to complete.

Result

The new host is now discovered and managed by ONTAP tools for VMware vSphere. You can proceed to manage the datastore on the new host.

Related topics

- Mount a vVols datastore on new hosts.
- Mount NFS and VMFS datastore on new hosts.

Manage datastores

Mount NFS and VMFS datastores

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.

> When you add a new ESXi host using the Add an ESX Host to Your vSphere Cluster workflow, wait for the scheduled host discovery to complete before it shows up in ONTAP tools. Alternatively, you can manually run discovery from the NetApp ONTAP tools overview screen.

About this task

- Some right-click actions are disabled or unavailable depending on the vSphere client version and the type of datastore selected.
  - If you're using vSphere client 8.0 or later versions, some of the right-click options are hidden.
  - From vSphere 7.0U3 to vSphere 8.0 versions, even though the options appear, the action will be disabled.
- The mount datastore option is disabled when the host cluster is protected with uniform configurations.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the left navigation pane, select the data centers containing the hosts.
3. To mount NFS/VMFS datastores on host or host cluster, right-click and select **NetApp ONTAP tools** > **Mount Datastores**.
4. Select the datastores that you want to mount and select **Mount**.

What's next?

You can track the progress in the recent task panel.

Related topic

Add new VMware vSphere hosts

Unmount NFS and VMFS datastores

Unmount datastore action unmounts a NFS or VMFS datastore from ESXi hosts. Unmount datastore action is enabled for NFS and VMFS datastores that are discovered or managed by the ONTAP tools for VMware vSphere.

Steps

1. Log in to the vSphere client.
2. Right-click a NFS or VMFS datastore object and select **Unmount datastore**.

   A dialog box opens and lists the ESXi hosts that the datastore is mounted on. When the operation is performed on a protected datastore, a warning message is displayed on the screen.

3. Select one or more ESXi hosts to unmount the datastore.

   You cannot unmount the datastore from all hosts. The user interface suggests that you use the delete datastore operation instead.

4. Select the **Unmount** button.

   If the datastore is part of a protected host cluster, a warning message is displayed.

If the protected datastore is unmounted the exiting protection setting might result in partial protection. Refer to Modify protected host cluster to enable complete protection.

What's next?

You can track the progress in the recent tasks panel.

Mount a vVols datastore

You can mount a VMware Virtual Volumes (vVols) datastore to one or more additional hosts to provide storage access to additional hosts. You can unmount vVols datastore only through the APIs.

When you add a new ESXi host using the Add an ESX Host to Your vSphere Cluster workflow, wait for the scheduled host discovery to complete before it shows up in ONTAP tools. Alternatively, you can manually run discovery from the NetApp ONTAP tools overview screen.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the navigation pane, select the data center that contains the datastore.
3. Right-click the datastore and select **NetApp ONTAP tools** > **Mount datastore**.

4. In the **Mount datastores on Hosts** dialog box, select the hosts on which you want to mount the datastore, and then select **Mount**.

You can track the progress in the recent task panel.

Related topic

Add new VMware vSphere hosts

Resize NFS and VMFS datastore

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

About this task

You can only increase the size of an NFS and VMFS datastores. A FlexVol volume that is part of a NFS and VMFS datastores cannot shrink below the existing size but can grow by 120% maximum.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the navigation pane, select the data center that contains the datastore.
3. Right-click the NFS or VMFS datastore and select **NetApp ONTAP tools** > **Resize datastore**.
4. In the Resize dialog box, specify a new size for the datastore and select **OK**.

Expand vVols datastores

When you right-click on the datastore object in the vCenter object view, ONTAP tools for VMware vSphere supported actions are shown under the plug-in section. Specific actions are enabled depending on the type of datastore and the current user privileges.

Expand vVols datastore operation is not applicable for ASA r2 system-based vVols datastores.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the navigation pane, select the data center that contains the datastore.
3. Right-click the datastore and select **NetApp ONTAP tools** > **Add storage to datastore**.
4. In the **create or Select Volumes** window, you can either create new volumes or choose from the existing volumes. The user interface is self-explanatory. Follow the instructions as per your choice.
5. In the **Summary** window, review the selections and select **Expand**. You can track the progress in the recent tasks panel.

Shrink vVols datastore

Delete datastore action deletes the datastore when there are no vVols on the selected datastore.

Shrink vVols datastore operation is not supported for ASA r2 system-based vVols datastore.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the navigation pane, select the data center that contains the datastore.
3. Right-click on the vVol datastore and select **NetApp ONTAP tools** > **Remove storage from datastore**.
4. Select volumes which do not have vVols and select **Remove**.

   The option to select the volume on which the vVols is residing is disabled.

5. In the **Remove storage** pop-up, select **Delete volumes from ONTAP cluster** checkbox to delete the volumes from datastore and from ONTAP storage and select **Delete**.

Delete datastores

Remove storage from datastore action is supported on all ONTAP tools for VMware vSphere discovered or managed vVols datastores in the vCenter Server. This action allows the removal of volumes from the vVols datastores.

The remove option is disabled when there are vVols residing on a particular volume. In addition to removing volumes from datastore, you can delete the selected volume on ONTAP storage.

Delete datastore task from ONTAP tools for VMware vSphere in the vCenter Server does the following:

- Unmounts the vVol container.
- Cleans up igroup. If igroup is not in use, removes iqn from igroup.
- Deletes Vvol container.
- Leaves the Flex volumes on the storage array.

Follow the steps below to delete NFS, VMFS, or vVOL datastore from ONTAP tools from the vCenter Server:

Steps

1. Log in to the vSphere client.
2. Right-click a host system or a host cluster or a data center and select **NetApp ONTAP tools** > **Delete datastore**.

   You cannot delete the datastores if there are virtual machines using that datastore. You need to move the virtual machines to a different datastore before deleting the datastore. You cannot select Volume delete checkbox if the datastore belongs to a protected host cluster.

   a. In the case of NFS or VMFS datastore a dialog box appears with the list of VMs that are using the datastore.
   b. If the VMFS datastore is created on ASA r2 systems and if it is part of the protection, you need to unprotect the datastore before deleting it.
   c. In the case of vVols datastores, delete datastore action deletes the datastore only when there are no vVols associated with it. The Delete datastore dialog box provides an option to delete volumes from ONTAP cluster.
   d. In case of ASA r2 systems based vVols datastores, the checkbox to delete the backing volumes is not applicable.

3. To delete the backing volumes on ONTAP storage, select **Delete volumes on ONTAP cluster**.

> You cannot delete the volume on ONTAP cluster for a VMFS datastore that is part of the protected host cluster.

ONTAP storage views for datastores

ONTAP tools for VMware vSphere shows the ONTAP storage side view of the datastores and their volumes in the configure tab.

Steps

1. From the vSphere client, navigate to the datastore.
2. Select the **Configure** tab in the right pane.
3. Select **NetApp ONTAP tools** > **ONTAP Storage**. Depending on the datastore type, the view changes. Refer to the table below for information:

Datastore type	Information available
NFS datastore	The **Storage details** page contains storage backends, aggregate, and volume information. The **NFS details** page contains data related to the NFS datastore.
VMFS datastores	The **Storage details** page contains storage backend, aggregate, volume, and storage availability zone (SAZ) details. The **Storage unit details** page contains details of the storage unit.
vVols datastores	Lists all the volumes. You can expand or remove storage from the ONTAP storage pane. This view is not supported for ASA r2 system-based vVols datastore.

Virtual machine storage view

The storage view shows the list of vVols that are created by the virtual machine.

> This view is applicable for the VM which has at least one ONTAP tools for VMware vSphere managed vVols datastore related disk mounted on it.

Steps

1. From the vSphere Client navigate to the virtual machine.
2. Select the **Monitor** tab in the right pane.
3. Select **NetApp ONTAP tools** > **Storage**. The **Storage** details appear on the right pane. You can see the list of vVols that are present on the VM.

You can use the 'Manage Columns' option to hide or show different columns.

Manage storage thresholds

You can set the threshold to receive notifications in vCenter Server when the volume and the aggregate capacity reaches certain levels.

Steps:

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Settings** > **Threshold Settings** > **Edit**.
4. In the **Edit Threshold** window, provide the desired values in the **Nearly Full** and **Full** fields and select **Save**. You can reset the numbers to recommended values, which is 80 for Nearly full and 90 for full.

Manage storage backends

Storage backends are systems that the ESXi hosts use for data storage.

Discover storage

You can run the discovery of a storage backend on demand without waiting for a scheduled discovery to update the storage details.

Follow the steps below to discover the storage backends.

Steps

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Storage Backends** and select a storage backend.
4. Select the vertical ellipses menu and select **Discover storage**

You can track the progress in the recent tasks panel.

Modify storage backends

Follow the steps in this section to modify a storage backend.

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Storage Backends** and select a storage backend.
4. Select the vertical ellipses menu and select **Modify** to modify the credentials or the port name. You can track the progress in the recent tasks panel.

You can perform the Modify operation for global ONTAP clusters using ONTAP tools Manager using the following steps.

1. Launch ONTAP tools Manager from a web browser:

`https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select storage backends from the sidebar.
4. Select the Storage Backend you want to modify.
5. Select the vertical ellipses menu and select **Modify**.
6. You can modify the credentials or the port. Enter the **Username** and **Password** to modify the storage backend.

Remove storage backends

You need to delete all the datastores attached to the storage backend before removing the storage backend. Follow the steps below to remove a storage backend.

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Storage Backends** and select a storage backend.
4. Select the vertical ellipses menu and select **Remove**. Ensure that the storage backend does not contain any datastores. You can track the progress in the recent tasks panel.

You can perform the remove operation for global ONTAP clusters using ONTAP tools Manager.

1. Launch ONTAP tools Manager from a web browser:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Storage Backends** from the sidebar.
4. Select the storage backend you want to remove
5. Select the vertical ellipses menu and select **Remove**.

Drill down view of storage backend

The storage backend page lists all the storage backends. You can perform discover storage, modify, and remove operations on the storage backends you added and not on the individual child SVM under the cluster.

When you select either the parent cluster or the child under the storage backend, you can see the overall summary of the component. When you select the parent cluster you have the actions dropdown from which you can perform the discover storage, modify, and remove operations.

The summary page provides the following details:

- Status of the storage backend
- Capacity information
- Basic information about the VM
- Network information like the IP address and port of the network. For the child SVM, the information will be same as the parent storage backend.
- Privileges allowed and restricted for the storage backend. For the child SVM, the information will be same

as the parent storage backend. Privileges are shown only on the cluster-based storage backends. If you add SVM as the storage backend, privileges information will not be shown.

- The ASA r2 system cluster drill-down view does not include local tiers tab when the disaggregated property is set as "true" for the SVM or the cluster.
- For ASA r2 SVM systems, the capacity portlet is not shown. The capacity portal is required only when the disaggregated property is set as "true" for the SVM or the cluster.
- For ASA r2 SVM systems, basic information section shows the platform type.

The interface tab provides detailed information about the interface.

The local tiers tab provides detailed information about the aggregate list.

Manage vCenter Server instances

vCenter Server instances are central management platforms that allow you to control hosts, virtual machines, and storage backends.

Dissociate storage backends with the vCenter Server instance

The vCenter Server listing page shows the associated number of storage backends. Each vCenter Server instance has the option to associate or disassociate with a storage backend.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the required vCenter Server instance from the sidebar.
4. Select the vertical ellipses against the vCenter Server that you want to associate or dissociate with storage backends.
5. Select **Dissociate storage backend**.

Modify a vCenter Server instance

Follow the steps below to modify a vCenter Server instances.

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the applicable vCenter Server instance from the sidebar
4. Select the vertical ellipses against the vCenter Server that you want to modify and select **Modify**.
5. Modify the vCenter Server instance details and select **Modify**.

Remove a vCenter Server instance

You need to remove all the storage backends attached to the vCenter Server before removing it.

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the applicable vCenter Server instances from the sidebar
4. Select the vertical ellipses against the vCenter Server that you want remove and select **Remove**.

> After you remove vCenter Server instances, they will no longer be maintained by the application.

When you remove vCenter Server instances in ONTAP tools, the following actions are performed automatically:

- Plug-in is unregistered.
- Plug-in privileges and plug-in roles are removed.

Manage certificates

A self-signed certificate is generated for ONTAP tools and VASA Provider by default during deployment. Using the ONTAP tools Manager interface, you can renew the certificate or upgrade it to a custom CA. Custom CA certificates are mandatory in a multi-vCenter deployment.

Before you begin

- The domain name on which the certificate is issued should be mapped to the virtual IP address.
- Run the nslookup check on the domain name to check if the domain is getting resolved to the intended IP address.
- The certificates should be created with the domain name and the ONTAP tools IP address.

> A ONTAP tools IP address should map to a fully qualified domain name (FQDN). Certificates should contain the same FQDN mapped to the ONTAP tools IP address in subject or subject alternative names.

> You cannot switch from a CA-signed to a self-signed certificate.

Upgrade ONTAP tools certificate

ONTAP tools tab shows details like certificate type (self-signed/CA signed) and domain name. During deployment, self-signed certificate is generated by default. You can renew the certificate or upgrade the certificate to CA.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Certificates** > **ONTAP tools** > **Renew** to renew the certificates.

   You can renew the certificate if it has expired or is nearing its expiration date. The renew option is available when the certificate type is CA-signed. In the pop-up window, provide the server certificate, private key, root CA, and intermediate certificate details.

   The system will be offline until the certificate is renewed, and you will be logged out of the ONTAP tools Manager interface.

4. To upgrade the self-signed certificate to custom CA certificate, select **Certificates** > **ONTAP tools** > **Upgrade to CA** option.
   a. In the pop-up window, upload the server certificate, server certificate private key, root CA certificate, and intermediate certificate files.
   b. Enter the domain name for which you generated this certificate and upgrade the certificate.

   The system will be offline until the upgrade is complete, and you will be logged out of the ONTAP tools Manager interface.

Upgrade VASA Provider certificate

ONTAP tools for VMware vSphere is deployed with a self-signed certificate for VASA Provider. With this, only one vCenter Server instance can be managed for vVols datastores. When you manage multiple vCenter Server instances and want to enable vVols capability on them, you need to change the self-signed certificate to a custom CA certificate.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Certificates** > **VASA Provider** or **ONTAP tools** > **Renew** to renew the certificates.
4. Select **Certificates** > **VASA Provider** or **ONTAP tools** > **Upgrade to CA** to upgrade the self-signed certificate to custom CA certificate.
   a. In the pop-up window, upload the server certificate, server certificate private key, root CA certificate, and intermediate certificate files.
   b. Enter the domain name for which you generated this certificate and upgrade the certificate.

The system will be offline until the upgrade is complete, and you will be logged out of the ONTAP tools Manager interface.

Access ONTAP tools for VMware vSphere maintenance console

Overview of ONTAP tools for VMware vSphere maintenance console

You can manage your application, system, and network configurations by using the maintenance console of the ONTAP tools. You can change your administrator password and maintenance password. You can also generate support bundles, set different log levels, view and manage TLS configurations, and start remote diagnostics.

You should have VMware tools installed after deploying the ONTAP tools for VMware vSphere to access the maintenance console. You should use `maint` as the username and the password you configured during deployment to log in to the maintenance console of the ONTAP tools. You should use **nano** for editing the files in maintenance or root login console.

You should set a password for the `diag` user while enabling remote diagnostics.

You should use the **Summary** tab of your deployed ONTAP tools for VMware vSphere to access the maintenance console. When you select  , the maintenance console starts.

Console Menu	Options
Application Configuration	1. Display server status summary 2. Change LOG level for VASA Provider Services and SRA Services
System Configuration	1. Reboot virtual machine 2. Shutdown virtual machine 3. Change 'maint' user password 4. Change time zone 5. Increase jail disk size (/jail) 6. Upgrade 7. Install VMware Tools

Network Configuration	1. Display IP address settings 2. Display domain name search settings 3. Change domain name search settings 4. Display static routes 5. Change static routes 6. Commit changes 7. Ping a host 8. Restore default settings
Support and Diagnostics	1. Access diagnostic shell 2. Enable remote diagnostic access 3. Provide vCenter credentials for backup 4. Take backup

Configure remote diagnostic access

You can configure ONTAP tools for VMware vSphere to enable SSH access for the diag user.

Before you begin

The VASA Provider extension should be enabled for your vCenter Server instance.

About this task

Using SSH to access the diag user account has the following limitations:

- You are allowed only one login account per activation of SSH.
- SSH access to the diag user account is disabled when one of the following happens:
  - The time expires.

    The login session remains valid only until midnight the next day.
  - You log in as a diag user again using SSH.

Steps

1. From the vCenter Server, open a console to VASA Provider.
2. Log in as the maintenance user.
3. Enter `4` to select Support and Diagnostics.
4. Enter `2` to select Enable remote diagnostics access.
5. Enter `y` in the Confirmation dialog box to enable remote diagnostic access.
6. Enter a password for remote diagnostic access.

Start SSH on other nodes

You need to start SSH on other nodes before you upgrade.

Before you begin

The VASA Provider extension should be enabled for your vCenter Server instance.

About this task

Perform this procedure on each of the nodes before you upgrade.

Steps

1. From the vCenter Server, open a console to VASA Provider.
2. Log in as the maintenance user.
3. Enter `4` to select Support and Diagnostics.
4. Enter `1` to select Access diagnostic shell.
5. Enter `y` to proceed.
6. Run the command *sudo systemctl restart ssh*.

Update the vCenter Server credentials

You can update the vCenter Server instance credentials using the maintenance console.

Before you begin

You need to have maintenance user login credentials.

About this task

If you have changed the credentials for vCenter Server post deployment, then you need to update the credentials using this procedure.

Steps

1. From the vCenter Server, open a console to VASA Provider.
2. Log in as the maintenance user.
3. Enter `2` to select System Configuration Menu.
4. Enter `8` to change vCenter credentials.

ONTAP tools reports

ONTAP tools for VMware vSphere plug-in provides reports for virtual machines and datastores. When you select the NetApp ONTAP tools for VMware vSphere plug-in icon in the shortcuts section on the vCenter client, the user interface navigates to the Overview page. Select the Reports tab to view the virtual machine and the datastores report.

The virtual Machines report shows the list of discovered virtual machines (should have at least one disk from ONTAP storage based datastores) with performance metrics. When you expand the VM record, all the disk

related datastore info is displayed.

Datastores report shows the list of discovered or recognized ONTAP tools for VMware vSphere managed Datastores that are provisioned from ONTAP storage backend of all types with performance metrics.

You can use the Manage Columns option to hide or show different columns.

Collect the log files

You can collect log files for ONTAP tools for VMware vSphere from the options available in ONTAP tools Manager user interface. Technical support might ask you to collect the log files to help troubleshoot a problem.

> Generating logs from the ONTAP tools Manager includes all logs for all vCenter Server instances. Generating logs from the vCenter client user interface are scoped for the selected vCenter Server.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Log Bundles** from the sidebar.

   This operation can take several minutes.
4. Select **Generate** to generate the log files.
5. Enter the label for the Log Bundle and select **Generate**.

   Download the tar.gz file and send it to technical support.

Follow the steps below to generate log bundle using the vCenter client user interface:

Steps

1. Log in to the vSphere client.
2. From the vSphere Client home page, go to **Support** > **Log bundle** > **Generate**.
3. Provide the log bundle label and generate the log bundle. You can see the download option when the files are generated. Downloading might take some time.

> The log bundle generated replaces the log bundle that was generated within the last 3 days or 72 hrs.

Manage virtual machines

Considerations to migrate or clone virtual machines

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

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 the virtual machine is migrated to a different FlexVol volume, then the 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 metadata file 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 machines cloned to a VM template.

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

Refer to Creating a Virtual Machine for Cloning for more details.

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 machines that have memory Snapshot. For this release, you are expected to delete memory snapshot before enabling protection for the virtual machine.

For windows VM with ASA r2 storage type, when you take a snapshot of the virtual machine, it will be a read-only snapshot. When there is power on call for the VM, the VASA Provider creates a LUN using the read-only snapshot and then it enables it for IOPS. During the power-off request, VASA Provider deletes the LUN that was created and then disables the IOPS.

Migrate virtual machines with NFS and VMFS datastores to vVols datastores

You can migrate virtual machines from NFS and VMFS 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

Ensure 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 NFS and VMFS datastore to a vVols 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 select **Migrate**.
2. Select **Change storage only** and then select **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.
4. Review the settings and select **Finish**.

VASA cleanup

Use the steps in this section to perform VASA cleanup.

It is recommended that you remove any vVols datastores before performing the VASA Cleanup.

Steps

1. Unregister the plug-in by going into https://OTV_IP:8143/Register.html
2. Verify that the plug-in is no longer available on the vCenter Server.
3. Shut down ONTAP tools for VMware vSphere VM.
4. Delete ONTAP tools for VMware vSphere VM.

Attach or detach a data disk from a virtual machine

Attach a data disk to a virtual machine

Attach a data disk to a virtual machine to expand the storage capacity.

Steps

1. Log in to the vSphere client.
2. Right-click a virtual machine in the inventory and select **Edit Settings**.
3. On the **Virtual Hardware** tab, select **Existing hard disk**.
4. Select the virtual machine where the disk exists.
5. Select the disk you want to attach and select **OK**

Result

The hard disk appears in the Virtual Hardware devices list.

Detach a data disk from the virtual machine

You can detach a data disk attached to a virtual machine when it is no longer needed. When you detach the disk from the virtual machine, it is not automatically deleted; it remains on the ONTAP storage system.

Steps

1. Log in to the vSphere client.
2. Right-click a virtual machine in the inventory and select **Edit Settings**.
3. Move your pointer over the disk and select **Remove**.

> The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files aren't deleted.

Related information

Add a New Hard Disk to a Virtual Machine

Add an Existing Hard Disk to a Virtual Machine

Discover storage systems and hosts

When you first run ONTAP tools for VMware vSphere in a vSphere Client, ONTAP tools discovers the ESXi hosts, their LUNs and NFS exports, and the NetApp storage systems that own those LUNs and exports.

Before you begin

- All the ESXi hosts should be powered on and connected.
- All the storage virtual machines (SVMs) to be discovered should be running, and each cluster node should have at least one data LIF configured for the storage protocol in use (NFS or iSCSI).

About this task

You can discover new storage systems or update information about existing storage systems to obtain the latest capacity and configuration information at any time. You can also modify the credentials that ONTAP tools for VMware vSphere uses to log in to the storage systems.

While discovering the storage systems, ONTAP tools for VMware vSphere collects information from the ESXi hosts that are managed by the vCenter Server instance.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. Right-click the required data center and select **NetApp ONTAP tools** > **Update Host Data** .

   In the **Confirm** dialog box, confirm your choice.

3. Select the discovered storage controllers that have the status `Authentication Failure` and select **Actions** > **Modify**.
4. Fill in the required information in the **Modify Storage System** dialog box.
5. Repeat steps 4 and 5 for all storage controllers with `Authentication Failure` status.

After the discovery process is complete, perform the following actions:

- Use ONTAP tools for VMware vSphere to configure ESXi host settings for hosts that display the alert icon in the adapter settings column, the MPIO settings column, or the NFS settings column.
- Provide the storage system credentials.

Modify ESXi host settings using ONTAP tools

You can use the dashboard of ONTAP tools for VMware vSphere to edit your ESXi host settings.

Before you begin

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 select the issue to view the host name or the IP address of the ESXi host that has the issue.

Steps

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. Go to **ESXi Host compliance** portlet in the Overview (dashboard) of the ONTAP tools for VMware vSphere plug-in.
4. Select **Apply Recommended Settings** link.
5. In the **Apply recommended host settings** window, select the hosts that you want to comply with NetApp recommended host settings and select **Next**.

   You can expand the ESXi host to see the current values.

6. In the settings page, select the recommended values as required.
7. In the summary pane, check the values and select **Finish**. You can track the progress in the recent task panel.

Related information

Configure ESXi host settings

Manage passwords

Change ONTAP tools Manager password

You can change the administrator password using ONTAP tools Manager.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **administrator** icon on the top right corner of the screen and select **Change password**.

4. In the change password pop-up window, enter the old password and the new password details. The constraint for changing the password is displayed on the user interface screen.
5. Select **Change** to implement the changes.

Reset ONTAP tools Manager password

If you've forgotten the ONTAP tools Manager password, you can reset the administrator credentials using the token generated by ONTAP tools for VMware vSphere maintenance console.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. On the login screen, select **Reset password** option.

   To reset the Manager password, you need to generate the reset token using the ONTAP tools for VMware vSphere maintenance console.

   a. From the vCenter Server, open the maintenance console
   b. Enter '2' to select System Configuration option
   c. Enter '3' to Change 'maint' user password.
3. In the change password pop-up window, enter the password reset token, username, and the new password details.
4. Select **Reset** to implement the changes. On successful password reset, you can use new password to log in.

Reset application user password

The application user password is used for SRA and VASA Provider registration with vCenter Server.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Settings** from the sidebar.
4. In the **VASA/SRA credentials** screen, select **Reset password**.
5. Provide a new password and confirm the new password inputs.
6. Select **Reset** to implement the changes.

Reset maintenance console user password

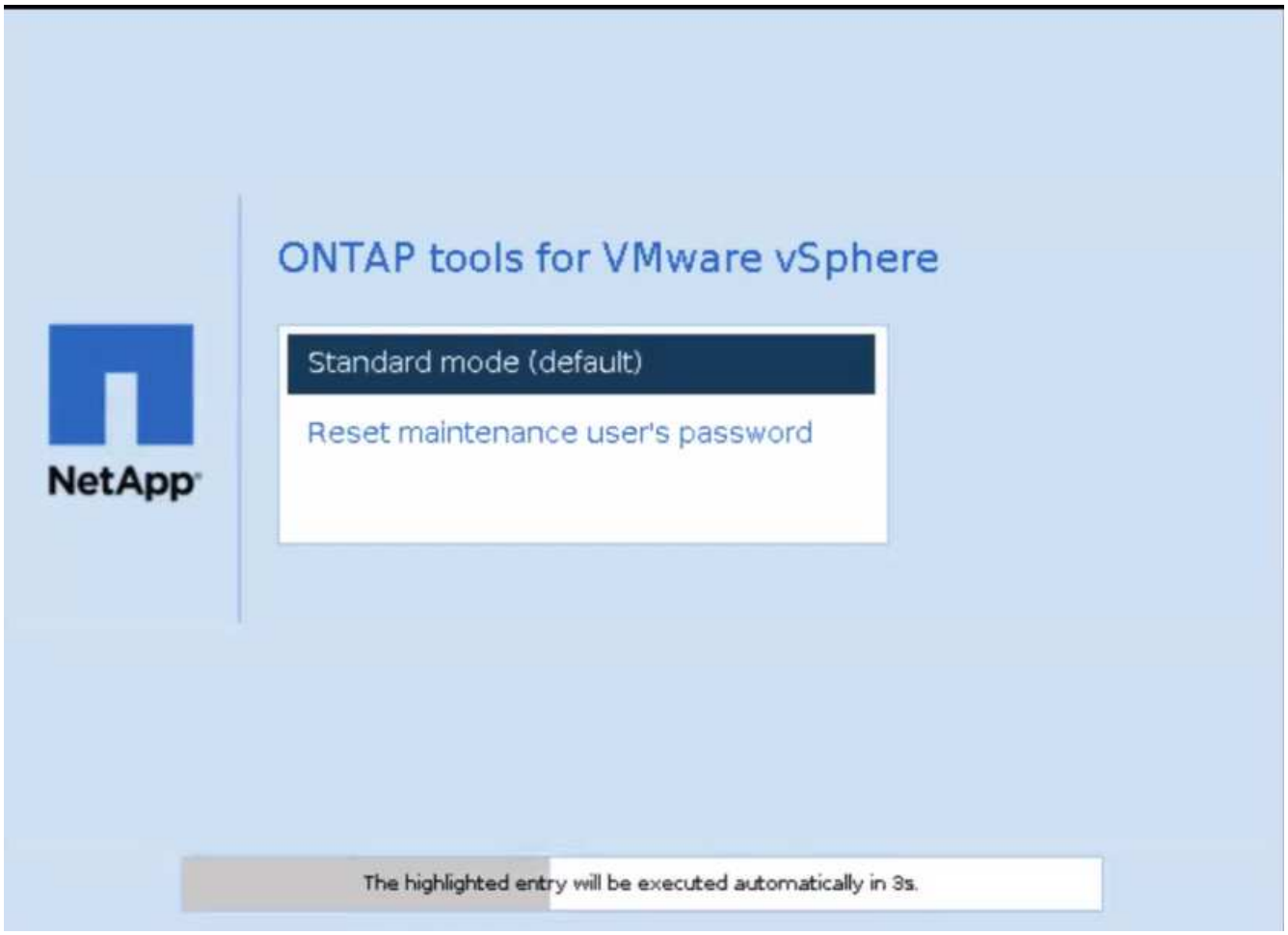
During guest OS restart operation, grub menu displays an option to reset maintenance console user password. This option is used to update the maintenance console user password present on the corresponding VM. After the reset password is complete, the

VM restarts to set the new password. In HA deployment scenario, after the VM restart, the password is automatically updated on the other two VMs.

For ONTAP tools for VMware vSphere HA deployment, you should change the maintenance console user password on the ONTAP tools management node, which is node1.

Steps

1. Log in to your vCenter Server
2. Right-click on the VM and select **Power** > **Restart Guest OS** During system restart, you get the following screen:



   You have 5 seconds to choose your option. Press any key to stop the progress and freeze the GRUB menu.

3. Select **Reset maintenance user's password** option. The maintenance console opens.
4. In the console, enter the new password details. New password and retype new password details should match to successfully reset the password. You have three chances to enter the correct password. The system restarts after successfully entering the new password.
5. Press Enter to continue. The password is updated on the VM.

The same GRUB menu comes up during power on of the VM as well. However, you should use the reset password option only with **Restart Guest OS** option.

Manage host cluster protection

Modify protected host cluster

You can perform the following tasks as part of modify protection. You can perform all the changes in the same workflow.

- Add new datastores or hosts to the protected cluster.
- Add new SnapMirror relationships to the protection settings.
- Delete existing SnapMirror relationships from the protection settings.
- Modify an existing SnapMirror relationship.

Monitor host cluster protection

Use this procedure to monitor the status of the host cluster protection. You can monitor every protected host cluster along with its protection state, SnapMirror relationships, datastores, and the corresponding SnapMirror status.

Steps

1. Log in to the vSphere client.
2. Navigate to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**.

   The icon under the protection column shows the status of the protection

3. Hover over the icon to see more details.

Add new datastores or hosts

Use this procedure to protect the newly added datastores or hosts. You can add new hosts to the protected cluster or create new datastores on host cluster using the vCenter native user interface.

Steps

1. Log in to the vSphere client.
2. To edit the properties of a protected cluster, you can either
   a. Navigate to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu against the cluster and select **Edit** or
   b. Right-click a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. If you have created a datastore in vCenter native user interface, then that datastore is shown as unprotected. The user interface shows all datastores in the cluster and their protection status in a dialog box. Select **Protect** button to enable complete protection.
4. If you have added a new ESXi host, the protection status shows as partially protected. Select the ellipsis menu under the SnapMirror settings and select **Edit** to set the proximity of the newly added ESXi host.

   In case of Asynchronous type relationship, edit action is not supported because you cannot add the target SVM for tertiary site to the same ONTAP tools instance. However, you can use the system manager or CLI of the target SVM to change the relationship configuration.

5. Select **Save** after making the necessary changes.

6. You can see the changes in the **Protect Cluster** window.

A vCenter task is created and you can track the progress in the **Recent task** panel.

Add a new SnapMirror relationship

Steps

1. Log in to the vSphere client.
2. To edit the properties of a protected cluster, you can either
   a. Navigate to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu against the cluster and select **Edit** or
   b. Right-click a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. Select **Add relationship**.
4. Add new relationship as either **Asynchronous** or **AutomatedFailOverDuplex** policy type.
5. Select **Protect**.

   You can see the changes in the **Protect Cluster** window.

A vCenter task is created and you can track the progress in the **Recent task** panel.

Delete an existing SnapMirror relationship

To delete an asynchronous SnapMirror relationship, secondary site SVM or cluster should be added as storage backend on ONTAP tools for VMware vSphere. You cannot delete all the SnapMirror relationships. When you delete a relationship, respective relationship on ONTAP cluster is also removed. When you delete an AutomatedFailOverDuplex SnapMirror relationship, the datastores on the destination are unmapped and consistency group, LUNs, volumes, and igroups are removed from the destination ONTAP cluster.

Deleting the relationship triggers a rescan on secondary site to remove the unmapped LUN as active path from the hosts.

Steps

1. Log in to the vSphere client.
2. To edit the properties of a protected cluster, you can either
   a. Navigate to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu against the cluster and select **Edit** or
   b. Right-click a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. Select the ellipsis menu under the SnapMirror settings and select **Delete**.

A vCenter task is created and you can track the progress in the **Recent task** panel.

Modify an existing SnapMirror relationship

To modify an asynchronous SnapMirror relationship, secondary site SVM or cluster should be added as storage backend on ONTAP tools for VMware vSphere. If it is an AutomatedFailOverDuplex SnapMirror relationship, you can modify the host proximity in case of uniform configuration and the host access in case of non-uniform configuration. You cannot interchange Asynchronous and AutomatedFailOverDuplex policy types. You can set the proximity or access for the newly discovered hosts on the cluster.

You cannot edit an existing asynchronous SnapMirror relationship.

Steps

1. Log in to the vSphere client.
2. To edit the properties of a protected cluster, you can either
   a. Navigate to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu against the cluster and select **Edit** or
   b. Right-click a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. If AutomatedFailOverDuplex policy type is selected, add host proximity or host access details.
4. Select **Protect** button.

A vCenter task is created and you can track the progress in the **Recent task** panel.

Remove host cluster protection

When you remove the host cluster protection, the datastores become unprotected.

Steps

1. To view the protected host clusters, navigate to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**.

   In this page, you can monitor the protected host clusters along with its protection state, SnapMirror relationship, and its corresponding SnapMirror status.

2. In the **Host cluster protection** window, select the ellipsis menu against the cluster, and then select **Remove protection**.

Disable AutoSupport

When configuring your storage system for the first time, AutoSupport is enabled by default. It sends messages to technical support 24 hours after it is enabled. When you disable AutoSupport, you will no longer receive proactive support and monitoring.

It is recommended that you keep the AutoSupport enabled. It helps speed up problem detection and resolution. The system collects AutoSupport information and stores it locally, even when disabled. However, it does not send the report to any network.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Settings** > **Telemetry** > **Edit** option.
4. Deselect the **AutoSupport** option and save the changes.

Update AutoSupport proxy URL

Update the AutoSupport proxy URL to ensure the proper functioning of the AutoSupport feature in scenarios where a proxy server is used for network access control or security measures. It allows the AutoSupport data to be routed through the appropriate proxy, enabling secure transmission and compliance.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Settings** from the sidebar.
4. Select the **Settings** > **Telemetry** > **Edit** option.
5. Enter a valid **Proxy URL** and save the changes.

   If you disable AutoSupport, the proxy URL is also disabled.

Add NTP servers

Enter the NTP server details to synchronize the time clocks of the ONTAP tools appliance.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Settings** > **NTP server** > **Edit** option.
4. Enter the comma-separated fully qualified domain name (FQDN), IPv4, or IPv6 addresses.

   Refresh to screen to see the updated values.

Create backup and recover the ONTAP tools setup

Beginning with ONTAP tools for VMware vSphere 10.3, the appliance uses dynamic storage provisioner, you cannot achieve zero-RPO. However, you can achieve near zero-RPO. To achieve near zero-RPO, you need to create backup of the setup and restore it on a new virtual machine.

To migrate to HA when non-HA backup is enabled, disable the backup first and re-enable it after the migration.

Create backup and download the backup file

Steps

1. From the vCenter Server, open the maintenance console.
2. Log in as the maintenance user.
3. Enter `4` to select **Support and Diagnostics**.
4. Enter `3` to select **Enable System Backup** option.
5. In case of non-HA, enter the vCenter credentials where the ONTAP tools virtual machine is deployed.
6. Enter the backup frequency value between 5 and 60 minutes.
7. Press **Enter**

   This creates the backup and pushes the backup to the datastore of the virtual machine at a regular interval.

8. To access the backup, navigate to the storage section and select the datastore of the virtual machine
9. Select the **Files** section.

   In the file section, you can see the directory. The name of the directory will be the ONTAP tools IP address where the dots (.) are replaced by underscores, suffixed with *backup*.

10. For more backup information, download the backup_info.txt file from **Files** > **Download**.

Recover

To recover the setup, power off the existing virtual machine and deploy a new virtual machine using the OVA that was used in the initial deployment.

You need to use the same ONTAP tools IP address for the new virtual machine and the system configuration such as services enabled, node size, and HA mode must be same as the initial deployment.

Perform the following steps to recover the setup from the backup file.

1. From the vCenter Server, open the maintenance console.
2. Log in as the maintenance user.
3. Enter `4` to select **Support and Diagnostics**.
4. Enter `2` to select **Enable remote diagnostic access** option and create a new password for the diagnostic access.
5. Select any one backup from the downloaded directory. The lastest backup file name is recorded in *backup_info.txt* file.
6. Run the below command to copy the backup to the new virtual machine and enter the diagnostic password when prompted.

```
scp <Backup_X.tar.enc> diag@<node_ip>:/home/diag/system_recovery.tar.enc
```

> Do not alter the destination path and file name (/home/diag/system_recovery.tar.enc) mentioned in the command.

7. After the backup file is copied, login to diagnostic shell and run the following command:

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

   The logs are recorded in */var/log/post-deploy-upgrade.log* file.

8. After successful recovery, services and vCenter objects are restored.

Uninstall ONTAP tools for VMware vSphere

Uninstalling the ONTAP tools for VMware vSphere deletes all the data in the tools.

Steps

1. Remove or move all the virtual machines from the ONTAP tools for VMware vSphere managed datastores.
   - To remove the virtual machines, refer to Remove and reregister VMs and VM templates
   - To move them to an unmanaged datastore, refer to How to Migrate Your Virtual Machine with Storage vMotion
2. Delete datastores created on ONTAP tools for VMware vSphere.
3. If you have enabled the VASA provider, select **Settings** > **VASA Provider settings** > **Unregister** in ONTAP tools to unregister the VASA providers from all the vCenter servers.
4. Disassociate all storage backends from the vCenter Server instance. Refer to Dissociate storage backends with the vCenter Server instance.
5. Delete all storage backends. Refer to Manage storage backends.
6. Remove the SRA adapter from VMware Live Site Recovery:
   a. Log in as admin to the VMware Live Site Recovery appliance management interface using port 5480.
   b. Select **Storage Replication Adapters**.
   c. Select the appropriate SRA card, and from the drop-down menu, select **Delete**.
   d. Confirm that you know the results of deleting the adapter and select **Delete**.
7. Delete the vCenter server instances onboarded to ONTAP tools for VMware vSphere. Refer to Manage vCenter Server instances.
8. Power off the ONTAP tools for VMware vSphere VMs from the vCenter Server and delete the VMs.

What's next?

Remove FlexVol volumes

Remove FlexVol volumes

When you use a dedicated ONTAP cluster for ONTAP tools for VMware deployment, it creates many unused FlexVol volumes. After removing ONTAP tools for VMware vSphere, you should remove the FlexVol volumes to avoid possible performance impacts.

Steps

1. Determine the ONTAP tools for VMware vSphere deployment type from the ONTAP tools management node VM.

cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol

If it is an iSCSI deployment, you need to delete igroups as well.

2. Get the list of FlexVol volumes.

   kubectl describe persistentvolumes | grep internalName | awk -F'=' '{print $2}'

3. Remove the VMs from the vCenter Server. Refer to Remove and reregister VMs and VM templates.
4. Delete FlexVol volumes. Refer to Delete a FlexVol volume. In the CLI command to delete a volume, give the exact name of the FlexVol volumes.
5. Delete SAN igroups from the ONTAP storage system in case of iSCSI deployment. Refer to View and manage SAN initiators and igroups.

Copyright information

Trademark information