Manage ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

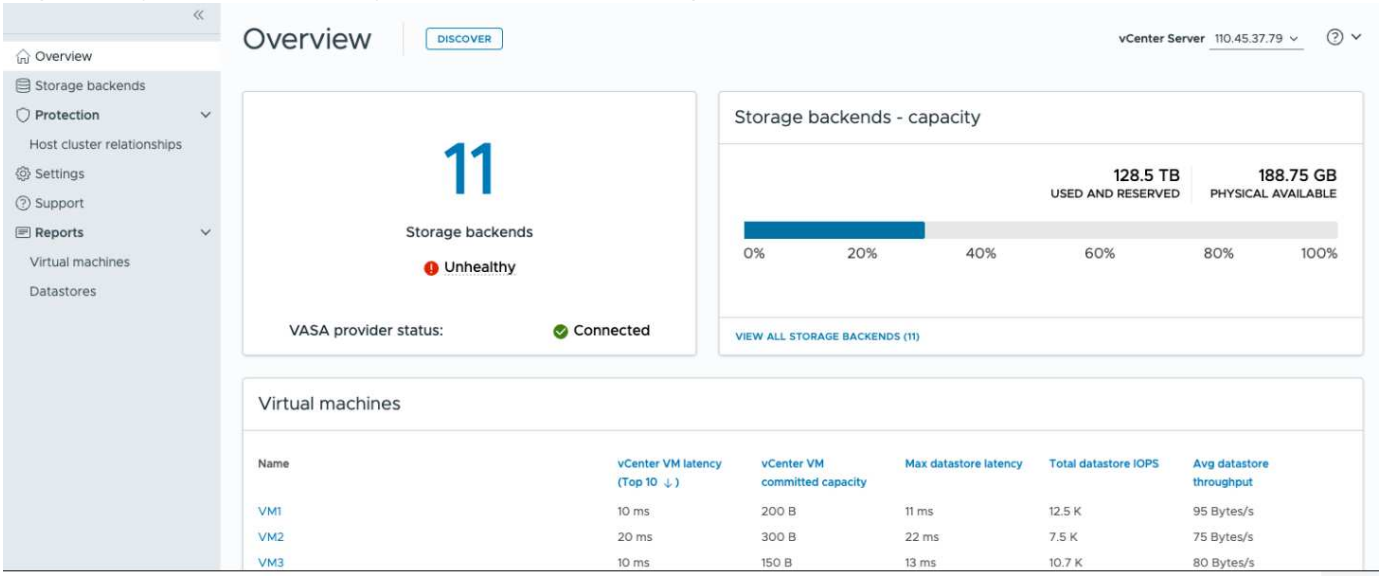
Table of Contents

Manage ONTAP tools for VMware vSphere

Learn about the ONTAP tools dashboard

Selecting the ONTAP tools for VMware vSphere plug-in icon from the shortcuts section in the vCenter client opens the overview page. This dashboard provides a summary of the ONTAP tools for VMware vSphere plug-in.

In Enhanced Linked Mode (ELM), the vCenter Server dropdown appears. Choose a vCenter Server to view its data. The dropdown is available in all listing views of the plug-in. When you select a vCenter Server on one page, it stays the same when you switch tabs in the plug-in.



From the overview page, you can run the **Discovery** action. The discovery action detects newly added or updated storage backends, hosts, datastores, and protection status or relationships at the vCenter level. Run on-demand discovery without waiting for the scheduled discovery.

The **Discovery** action button is enabled only if you have the required 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 if all ESXi hosts (for the selected vCenter) follow the recommended NetApp host settings by group or 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.

How ONTAP tools manages igroups and export policies

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 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 datastores to make igroup management easier. Understand the igroup workflow to manage LUNs and datastores 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 don't 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)

ONTAP creates the parent igroup DS1Igroup for DS1 and maps the child igroup host1Igroup to lun1. The system always maps LUNs 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)

ONTAP tools for VMware vSphere create a child igroup host2Igroup and add it 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)

ONTAP tools for VMware vSphere remove host1Igroup from the hierarchy. The system does not explicitly delete child igroups. It deletes them 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 unless another datastore reuses the parent igroup. Child igroups are not 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 don’t 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 NFS datastore access and client permissions in ONTAP tools for VMware vSphere. Export policies are created and managed in ONTAP systems and can be used 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 keeps the host IP address and does not change. 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

How ONTAP tools manages igroups

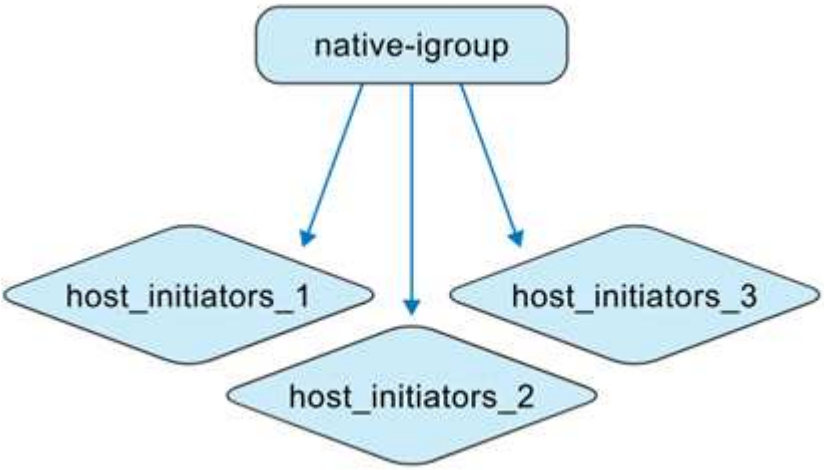
If you manage both ONTAP tools VMs and ONTAP storage systems, it is important to understand how igroups behave, especially when moving datastores from environments not managed by ONTAP tools to those that are. This page explains how igroups are updated during this process.

ONTAP tools for VMware vSphere 10.4 and later version automatically creates and maintains ONTAP and vCenter objects to simplify datastore management in VMware datacenter environments.

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

Non-ONTAP tools managed igroups

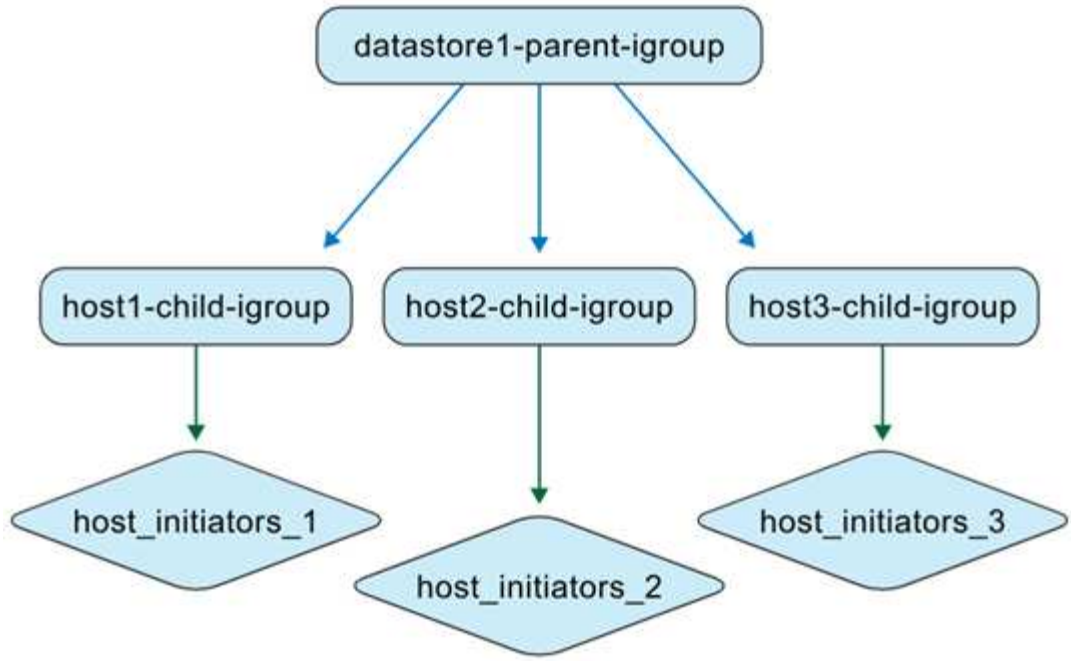
As a storage administrator, you can create igroups on the ONTAP system as flat or nested structures. The illustration shows a flat igroup created in the ONTAP system.

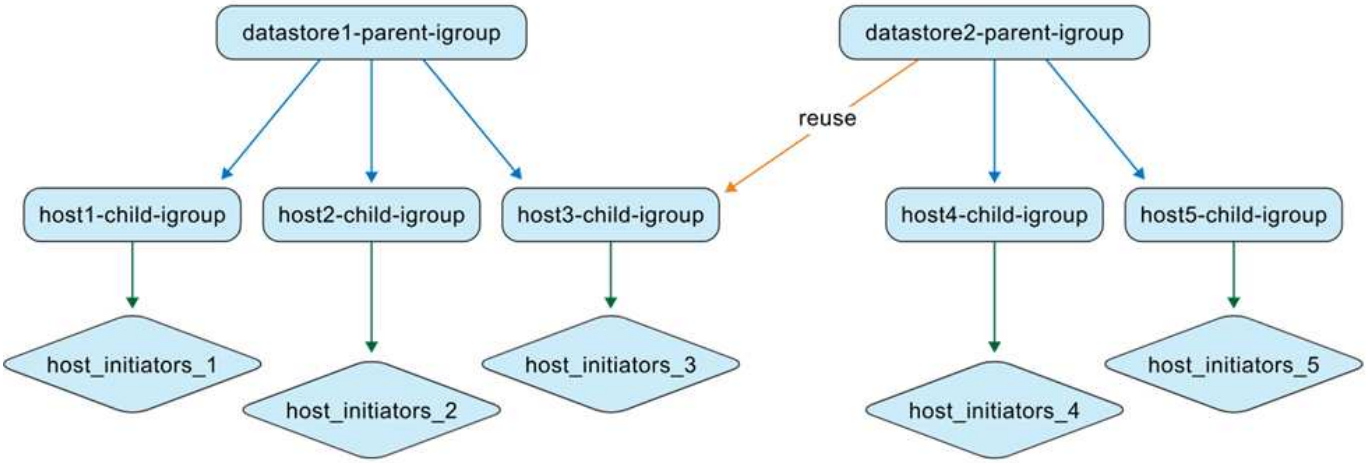


ONTAP tools managed igroups

When you create datastores, ONTAP tools for VMware vSphere 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). You can see the new datastore with the custom igroup name in the vCenter Server interface.

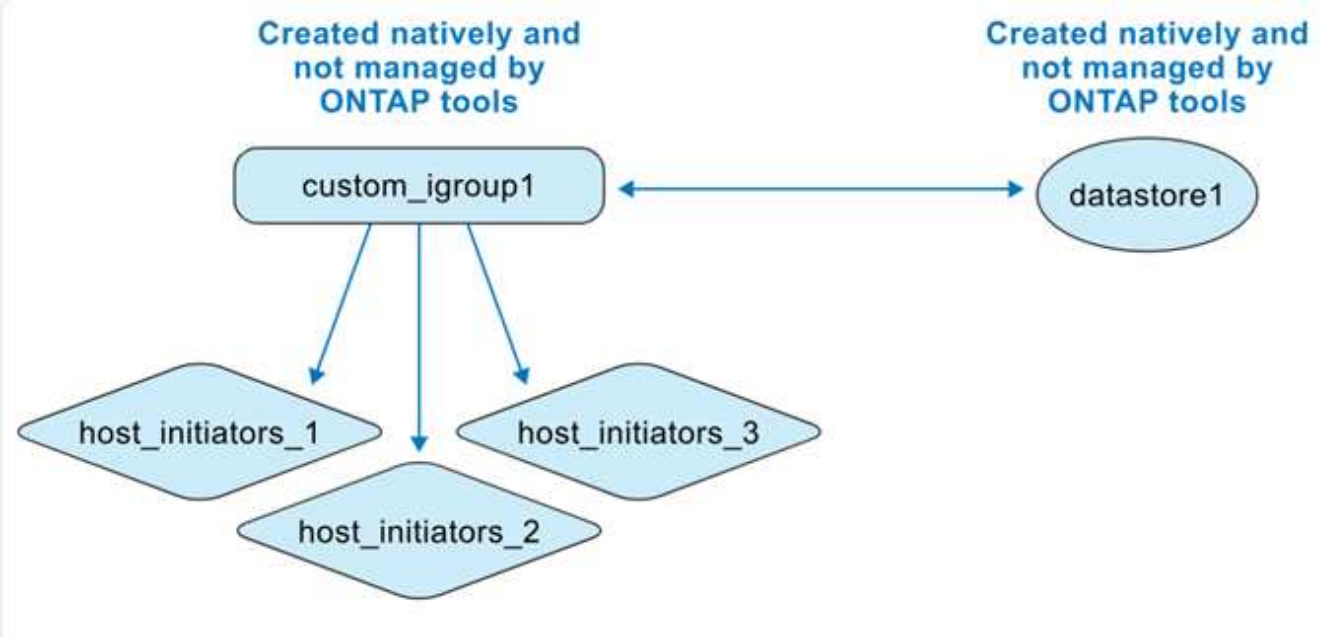
When you reuse the igroup name during datastore creation

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.

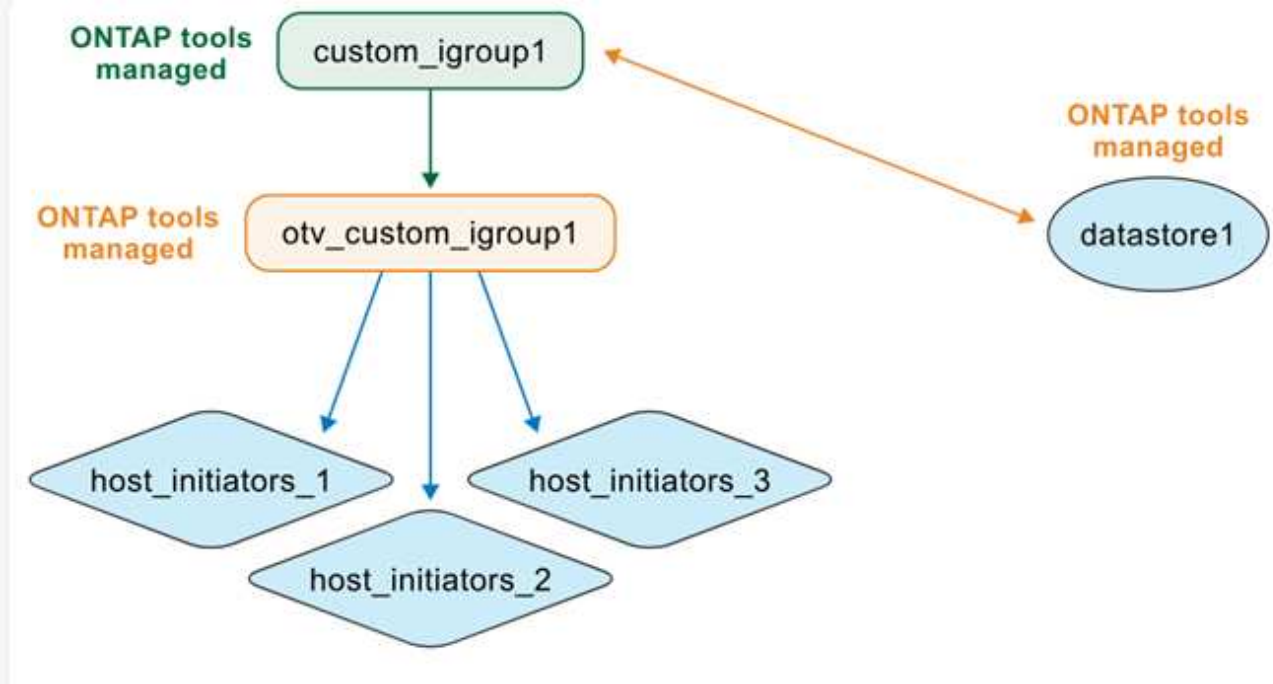
This operation can also be performed using the API. To reuse an existing igroup during datastore creation, specify the igroup UUID in the API request payload.

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.



After you run datastore discovery in ONTAP tools, ONTAP tools converts the flat igroup 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 create a datastore in ONTAP tools using an igroup that was first created in ONTAP systems, after ONTAP tools manages it. 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.

Learn about the ONTAP tools Manager user interface

ONTAP tools for VMware vSphere supports multi-tenancy, enabling management of multiple vCenter Server instances.

ONTAP tools Manager is a web-based console for managing ONTAP tools for VMware vSphere, vCenter Server instances, storage backends, and appliance configuration such as High Availability (HA) and node scaling.

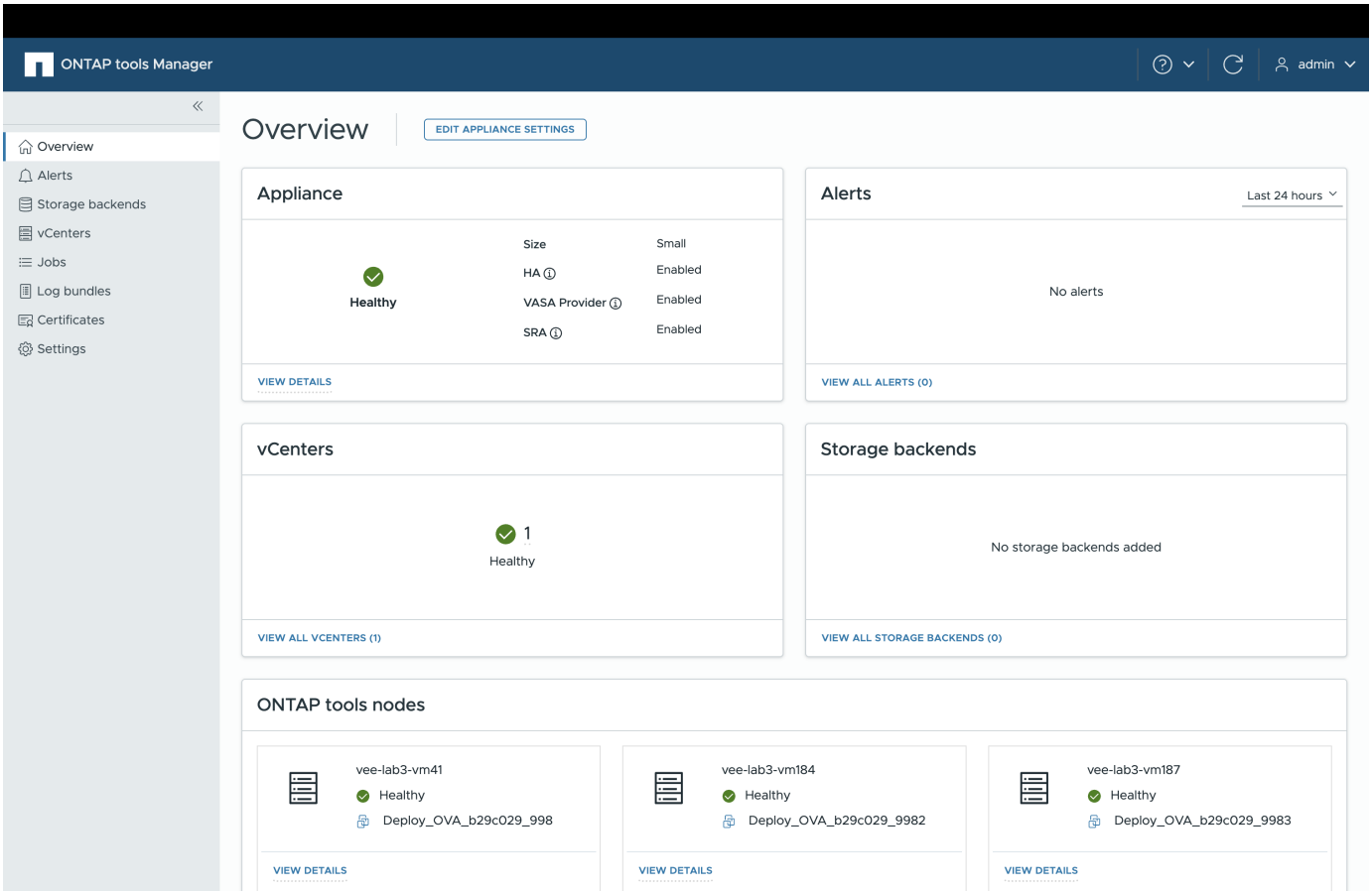
ONTAP tools Manager provides the following capabilities:

- Manage alerts - View and filter alerts generated by ONTAP tools for VMware vSphere.
- Manage storage backends - Add and manage ONTAP storage clusters, and map them to vCenter Server instances globally.
- Manage vCenter Server instances - Add and manage vCenter Server instances within ONTAP tools.
- Monitor jobs - Monitor and debug asynchronous jobs initiated from both the ONTAP tools plug-in interface and ONTAP tools Manager interface. You can filter jobs by time period, adjust page size, and view job

details, including errors and sub-tasks. Click a failed status for error details. For jobs with sub-tasks, expand the row to view descriptions and statuses. For sub-jobs use the job's drilldown to view the details.

- Download log bundles - Collect log files to troubleshoot ONTAP tools for VMware vSphere.
- Manage certificates - Replace the self-signed certificate with a custom CA certificate, and renew or refresh certificates for VASA Provider and ONTAP tools.
- Reset passwords - Change the password for the VASA Provider and SRA.
- Manage appliance settings - Configure the ONTAP tools appliance, including enabling HA and scaling up node sizes.

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.



Card	Description
Appliance card	The Appliance card shows the overall status of the ONTAP tools appliance, configuration details, and the status of enabled services. To view more information, select the **View details** link. If you change an appliance setting, the card shows the job status and details until the change is complete.

Card	Description
Alerts card	The Alerts card shows ONTAP tools alerts categorized by type, including HA node-level alerts. You can view detailed alerts by clicking the count hyperlink, which takes you to the alerts page filtered by the selected alert type.
vCenters card	The vCenters card shows the health status of all vCenter Server instances managed by ONTAP tools. You can view details for each vCenter by selecting the corresponding link, which navigates to a page with more information about the selected instance.
Storage backends card	The Storage backends card shows the health and connectivity status of all ONTAP storage clusters configured in ONTAP tools. You can view details for each storage backend by selecting the corresponding link, which navigates to a page with more information about the selected cluster.
ONTAP tools nodes card	The ONTAP tools nodes card shows all nodes in the appliance, including node name, VM name, status, and network information. Select **View details** to see more details for a specific node. [NOTE] In a non-HA configuration, only a single node appears. In an HA configuration, three nodes are displayed.

Manage ONTAP tools Manager settings

Edit ONTAP tools AutoSupport settings

When configuring ONTAP tools for VMware vSphere for the first time, AutoSupport is enabled by default. It sends messages to technical support 24 hours after it is enabled.

Disable AutoSupport

When you disable AutoSupport, you no longer receive proactive support and monitoring.

> It is recommended to keep AutoSupport enabled, as it helps accelerate problem detection and resolution. Even when AutoSupport is disabled, the system continues to collect and store information locally, but it doesn't send reports over the 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 so the AutoSupport feature routes data through the proxy server for secure transmission.

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 to ONTAP tools

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.

Reset VASA Provider and SRA credentials in ONTAP tools

If you forget your VASA Provider or SRA credentials, you can reset them to a new password using the ONTAP tools Manager interface. The new password must be between 8 and 256 characters long.

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** > **VASA Provider / SRA credentials** > **Reset Password** option.
4. Enter the new password and confirm it.

5. Select **Save** to apply the changes.

Edit ONTAP tools backup settings

Beginning with ONTAP tools for VMware vSphere 10.5, the backup feature is enabled by default and a backup is created every 10 minutes. You can disable the backup or edit the frequency of the backup.

Do not disable the backup because it prevents ONTAP tools from maintaining low RPO. Disabling the backup doesn't delete the existing backup files. You can change the frequency of the backup to a value between 10 and 60 minutes.

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** > **Backup** > **Edit** option.
4. In the edit window, you can disable the backup or edit the backup frequency.

Enable ONTAP tools 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 needed.

   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 don't use them.

   The **Allow import of vVols configuration** option is shown only when the VASA Provider service is enabled. This option enables vVols data migration from ONTAP tools 9.xx to ONTAP tools 10.5.

Change ONTAP tools appliance settings

Use ONTAP tools Manager to scale up the ONTAP tools for VMware vSphere configuration, either by increasing the number of nodes or by enabling High Availability (HA). By default, the ONTAP tools for VMware vSphere appliance is deployed as a single-node, non-HA configuration.

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, scale up the node size and enable HA configuration. Use vCenter Server credentials to make changes.

   In HA configuration, you can change content library details. Provide the password for each edit.

   > In ONTAP tools for VMware vSphere, you're 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 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.

   > ONTAP tools pre-fill most input options with Node 1 network details to simplify the workflow. You can edit the input data before going to the wizard's last 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. You can also track the edit appliance settings job status from the jobs view by using the job ID.

If HA deployment fails and the new node status is 'New,' delete the new VM in vCenter before trying to enable HA again.

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

Add VMware vSphere hosts to ONTAP tools

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 in ONTAP tools

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.

- vSphere disables the mount datastore option 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 a host or a 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 in ONTAP tools

The Unmount datastore action removes an NFS or VMFS datastore from ESXi hosts. It is available for datastores discovered or managed by ONTAP tools for VMware vSphere.

Steps

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

   The vSphere client opens a dialog box and lists the ESXi hosts that mount the datastore. 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 in ONTAP tools

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**.

The recent task panel displays the progress.

Related topic

Add new VMware vSphere hosts

Resize NFS and VMFS datastores in ONTAP tools

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 increase the size of NFS and VMFS datastores. A FlexVol volume in these datastores cannot shrink below its current size but can grow up to 120%.

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, enter a new size for the datastore and select **OK**.

Expand vVols datastores in ONTAP tools

When you right-click on the datastore object in the vCenter object view, the plug-in section shows the supported actions for ONTAP tools for VMware vSphere. 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. Follow the on-screen instructions to make your selection.

5. In the **Summary** window, review the selections and select **Expand**. You can track the progress in the recent tasks panel.

Shrink a vVols datastore in ONTAP tools

This page explains how to remove volumes from a vVols datastore.

Use the remove storage from datastore action on any vVols datastore managed by ONTAP tools in vCenter Server.

You cannot remove storage from a volume if it contains vVols; the remove option will be disabled for such volumes. When removing volumes from the datastore, you also have the option to delete the selected volumes from ONTAP storage.

The shrink vVols datastore operation is not supported for vVols datastores based on ASA r2 systems.

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 that don't have vVols and select **Remove**.

   The option to select the volume on which 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 in ONTAP tools

This page describes how to delete NFS, VMFS, or vVols datastores using ONTAP tools in the vCenter Server.

When you delete a datastore, the following actions are performed depending on the datastore type:

- The vVol container is unmounted.
- If the igroup is not in use, iqn is removed from the igroup.
- The vVol container is deleted.
- Flex volumes are left on the storage array.

You can delete the datastore only if no vVols are present on the selected datastore.

Steps

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

You cannot delete a datastore used by virtual machines. Move virtual machines to another datastore before deleting. You cannot delete the volume if it is part of a protected host cluster.

a. In the case of an NFS or VMFS datastore, a dialog box appears with the list of VMs using the datastore.
b. If no virtual machines are associated with a VMFS datastore, you see a confirmation dialog. If host cluster protection is enabled and an AFD relationship exists, you can clean up secondary storage elements.
c. For protected VMFS datastores on ASA r2 systems, remove protection before deleting. Beginning with ONTAP 9.17.1 and ONTAP tools for VMware vSphere 10.5, you can delete a protected datastore. If it is the only datastore in the protection group, host cluster protection removes automatically.
d. For vVols datastores, you can delete the datastore only if there are no vVols present. The **Delete datastore** dialog box includes an option to remove volumes from the ONTAP cluster.
e. For vVols datastores on ASA r2 systems, you cannot delete the backing volumes from ONTAP using the **Delete datastore** option.

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

For VMFS datastores on unified ONTAP storage that are part of a protected host cluster, you cannot delete the volume from the ONTAP cluster.

When you delete an NFS, VMFS, or vVols datastore, parent igroups remain on the ONTAP system. Child igroups that are not mapped to any LUNs are deleted automatically. ONTAP tools perform a daily cleanup to remove unmapped default parent igroups. Delete the custom parent igroups manually in ONTAP. ONTAP tools cannot reuse stale parent igroups.

ONTAP storage views for datastores in ONTAP tools

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, go to the datastore.
2. Select the **Configure** tab in the right pane.
3. Select **NetApp ONTAP tools** > **ONTAP Storage**. The view changes by datastore type. See the table below:

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. ONTAP tools do not support this view for ASA r2 system-based vVols datastores.

Virtual machine storage view in ONTAP tools

The storage view shows the list of vVols that the virtual machine creates.

> This view applies to VMs with at least one disk from an ONTAP tools for VMware vSphere managed vVols datastore.

Steps

1. From the vSphere Client go 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 in ONTAP tools

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, go 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 restore the threshold values to the recommended defaults: 80 for Nearly Full and 90 for Full.

Manage storage backends in ONTAP tools

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 immediately. For MetroCluster configurations, run ONTAP tools discovery manually after a switchover.

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, go 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

You can modify the storage backend credentials or the port name. You can also modify the storage backend for global ONTAP clusters using ONTAP tools Manager. If the certificate will expire in 30 days or less, ONTAP tools shows a warning. Modify the storage backend and upload the new certificate from the ONTAP administrator.

When you modify the storage backend, ONTAP tools for VMware vSphere performs a discovery of the storage backend to update the storage details.

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, go 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.

Modify global ONTAP clusters with ONTAP tools Manager as follows.

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 must remove all datastores attached to the storage backend before you remove it. 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, go to **Storage Backends** and select a storage backend.
4. Select the vertical ellipses menu and select **Remove**. Ensure that the storage backend doesn't 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 that you added, but not on the individual child SVM under the cluster.

Select the parent cluster or child to view the component summary. For the parent cluster, use the actions dropdown to discover storage, modify, or remove the storage backend.

The summary page provides the following details:

- Status of the storage backend
- Capacity information
- Basic information about the VM
- Certificate details such as the certificate status and the expiry date.
- Network information like the IP address and port of the network. For the child SVM, the information is the same as the parent storage backend.
- Privileges allowed and restricted for the storage backend. For the child SVM, the information is the same as the parent storage backend. ONTAP tools show privileges only on the cluster-based storage backends. If you add SVM as the storage backend, privileges information is not shown.
- The ASA r2 system cluster drill-down view doesn't 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 in ONTAP tools

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. In the **Modify vCenter** window, enter the username, password, and port details.
6. Upload the certificate and select **Modify**.

Remove a vCenter Server instance

Remove all storage backends from 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 to 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.

Renew vCenter Server certificate

ONTAP tools notifies you when the vCenter certificate is nearing expiration or has expired. After renewing the vCenter certificate, upload the new certificate to ONTAP tools using the following steps:

1. Log in to the ONTAP tools remote diagnostics shell.
2. Obtain the renewed vCenter certificate from the diagnostics shell:

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p'
```

3. Ensure the certificate is in Base 64 ASCII format and includes the beginning and ending lines, for example:

```
---{}BEGIN CERTIFICATE{}---
MIIFUzCCA7ugAwIBAgIJANOgLapcl5oSMA0GCSqGSIb3DQEBCwUAMIGJMQwwCgYD
VQQDDAN2YzExFDASBgoJkiaJk/IsZAEZFgRkZW1vMRUwEwYKCZImiZPyLGQBGRYF
bG9jYWwxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRwwGgYDVQQK
DBN2YzEuZGVtby5uZXRhcHAuY29tMQwwCgYDVQQLDANMT0QwHhcNMjQwNDA1MTgw
NTE4WhcNMjYwNDA1MTgwNTE4WjBzMRwwGgYDVQQDDBN2YzEuZGVtby5uZXRhcHAu
Y29tMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJ
UGFsbyBBbHRvMQ8wDQYDVQQKDAZOZXRBcHAxDDAKBgNVBAsMA0xPRDCCAaIwDQYJ
KoZIhvcNAQEBBQADggGPADCCAYoCggGBALU8OCWMtA2gvIC/OTw/7xucvPVuM+b8
DhzvNpQ2phjfr6ctEhbntPpqPdu+t2CKK7l0mzg3D9cJ/rvMvdDDXr0tgaD1oi2u
ZDW0CaF0QhLOpNfRXMoogBZ66csEhViAy3CHTcOse770mA/PyoHgrCPZngVlZIiQ
TIWpdQMbEEzFIkrLfC70UW2MzfublrsH7Dn/kOu/iCSlVJWixKf7SmZtVQ5ZxBTD
UlJSiqoX1eRXGyunArEvrIpOY9kkKXUElm3hGnk/ZmiuBJ+HqUYqYW+H+7vE3lKa
6NEqDX+tZotxTx2bXMjeiIWU30ZbshgeXlIG9qc49clBoC9iGjavhctOcaXg/W3h
dLKK5ds3rpRERgMg6VMkrfiqAJuiq+b3sTvXMAul/3hL7hz5QABAE/hP4ZvIHV02
WWDQRLiuVFAcDAyvCrO9Irx0Gk1RyRShKYakdWxZ3hhMdLuGq0yvRXqo1Ib94zwO
JfBJHjFToA/GqwromZgiTzJkKq5xbN8MFwIDAQABo4HSMIHPMAsGA1UdDwQEAwIF
4DA7BgNVHREENDAygRVlbWFpbEBkZW1vLm5ldGFwcC5jb22HBMCoAB+CE3ZjMS5k
ZW1vLm5ldGFwcC5jb20wHQYDVR0OBBYEFJ0V0zY+JRpFrEt31ovAY4BLFXmAMB8G
A1UdIwQYMBaAFENf6fRxWF3OJQNTPIdUpK6kjA78MEMGCCsGAQUFBwEBBDcwNTAz
BggrBgEFBQcwAoYnaHR0cHM6Ly92YzEuZGVtby5uZXRhcHAuY29tL2FmZC92ZWNz
L2NhMA0GCSqGSIb3DQEBCwUAA4IBgQBaDfk7GBM4vmhzYCqGrr6KB+h3qeTJ+Y0Y
5nIPRP1HucawDQ8QTay605ddJ8gFGoxkOQDn9tdXWXGjnTRFOT8R+Hw/nUfVSiDP
sYienb16copzUNwtqh+m9Ifow74Gf+ulRzEC0EAVO1X/nTEYH6NKM6Wy7y7F8g5J
lrpM3JY90ZChMqHO3Av/88rbErfQ/gU1brJ3u9Gks4e20Z7Ff312ZKhWRuJDlN2Z
0tc/gp90N9GxaVvELovq/pdjaZ8xiXCxa6piicrJd9WnqMH1gmxP2PIBDxMDBWBG
gwsfs5H7VG9MJYks6lViNsGclo0EwEdF0MfoB3JtsWpPWq6+jBua0Jm7/aFCU+Ht
mykr0gaV7muegoiBQuDma4EkAI31D7ZlUgJQaw157NTk4RW3TFcbtViBHJkM54Hr
iVm0cl+2BZNi/QTMh/MkWV2dYXJ3NuNlqqfzFY+bUfkzkR4SneMk0HX3joNNYDJv
siO7bL+k/Pxql27NVIhuCoVJAlcI7ak=
---{}END CERTIFICATE{}---
```

4. Copy the output and save it as a text file with a `.pem` extension on your desktop.
5. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
6. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
7. Select the applicable vCenter Server instance from the sidebar
8. Select the vertical ellipses against the vCenter Server that you want to modify and select **Modify**.
9. In the **Modify vCenter** window, enter the username, password, and port details.
10. Upload the certificate and select **Modify**.

Related information

Configure remote diagnostic access

Manage ONTAP tools certificates

A self-signed certificate is generated for ONTAP tools and VASA Provider by default during deployment. You can use the ONTAP tools Manager interface to renew this certificate or replace it with a custom CA certificate. In multi-vCenter deployments, using custom CA certificates is required.

Before you begin

You should have the following before you begin:

- The domain name mapped to the virtual IP address.
- Successful nslookup of the domain name, confirming it resolves to the correct IP address.
- Certificates 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 FQDN of the Load Balancer IP 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 FQDN of the Load Balancer IP 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

Learn about the ONTAP tools maintenance console

The maintenance console for ONTAP tools for VMware vSphere enables you to manage application, system, and network settings. You can update administrator and maintenance passwords, generate support bundles, configure log levels, manage TLS settings, and enable remote diagnostics.

After deploying ONTAP tools for VMware vSphere, if the maintenance console is not accessible, install the VMware tools from the vCenter Server. Log in using the `maint` username and the password set during deployment. Use **nano** to edit files in the 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 ONTAP tools services 3. Change cert validation flag
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 for ONTAP tools

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

Before you begin

Enable the VASA Provider extension for your vCenter Server instance.

About this task

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

- you’re 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 expires at 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 ONTAP tools nodes

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

Before you begin

Enable the VASA Provider extension for your vCenter Server instance.

About this task

Repeat this procedure on each node before upgrading.

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 vCenter Server credentials in ONTAP tools

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 changed vCenter Server credentials after deployment, update them 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.

Change certificate validation flag in ONTAP tools

By default, the certificate validation flag is enabled (set to true). You can set the ONTAP storage backend certificate validation flag to false if you need to bypass SAN certificate checks. This setting is not applicable to vCenter Server certificates.

Before you begin

You need to have maintenance user login credentials.

Steps

1. From the vCenter Server, open a console to ONTAP tools.
2. Log in as the maintenance user.

3. Enter `1` to select **Application Configuration** menu.
4. Enter `3` to change cert validation flag.

   The maintenance console shows the certificate validation flag status and prompts you to change it.

5. Enter 'y' to toggle the flag or 'n' to cancel.

When you enable the certificate validation flag (set to true), ONTAP tools checks that all storage backends use certificates with a Subject Alternative Name (SAN). If any backend uses a certificate without a SAN, you cannot enable certificate validation. Before enabling this flag, verify that all storage backends use SAN-based certificates. If you disable the certificate validation flag (set to false), ONTAP tools bypasses certificate validation for all configured storage backends.

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, the interface displays all the disk-related datastore information.

The datastores report lists ONTAP tools for VMware vSphere discovered or recognized datastores that use any ONTAP storage, with performance metrics.

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

Manage virtual machines

Virtual machine migration and cloning considerations for ONTAP tools

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 you migrate the virtual machine to a different FlexVol volume, the system updates the metadata file for that volume 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 doesn't 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're expected to delete memory snapshot before enabling protection for the virtual machine.

For a Windows VM with the ASA r2 storage type, a snapshot of the virtual machine is read-only. When you power on the VM, VASA Provider creates a LUN from the read-only snapshot and enables IOPS. When you power off the VM, VASA Provider deletes the LUN and disables IOPS.

Migrate virtual machines to vVols datastores in ONTAP tools

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're migrating.
4. Review the settings and select **Finish**.

Clean up VASA configurations in ONTAP tools

To complete the VASA cleanup process, follow these steps.

> It is recommended to remove any vVols datastores before starting 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 VM in ONTAP tools

Follow these steps to attach or detach data disks from virtual machines in vSphere and manage their storage resources.

Attach a data disk to a virtual machine

Attach a data disk to a virtual machine to add more storage.

Steps

1. Log in to the vSphere client.
2. Right-click on 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 the **OK** button.

Result

The hard disk appears in the Virtual Hardware devices list.

Detach a data disk from the virtual machine

Detach a data disk from a virtual machine when you don't need it anymore. The disk is not deleted; it stays on the ONTAP storage system.

Steps

1. Log in to the vSphere client.
2. Right-click on 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 in ONTAP tools

When ONTAP tools for VMware vSphere is launched in the vSphere Client for the first time, it automatically discovers ESXi hosts, their associated LUNs and NFS exports, as well as the NetApp storage systems that own these resources.

Before you begin

- Ensure all ESXi hosts are powered on and connected.
- Ensure all storage virtual machines (SVMs) to be discovered are running, and each cluster node has 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 existing ones to get the latest capacity and setup details. You can also change ONTAP tools for VMware vSphere credentials for storage system access.

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 on 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

Use the ONTAP tools dashboard in VMware vSphere to identify configuration issues, select ESXi hosts, review NetApp recommended settings, and apply them.

Before you begin

The ESXi host systems portlet displays issues with ESXi host settings. Select an issue to view the host name or IP address.

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 use 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 your ONTAP tools for VMware vSphere administrator credentials.
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 and new passwords. The user interface screen shows the password requirements.
5. Select **Change** to apply the changes.

Reset ONTAP tools Manager password

If you forget the ONTAP tools Manager password, you can restore administrator access by using a reset token generated from the ONTAP tools for VMware vSphere maintenance console.

Steps

1. Open a web browser and navigate to `https://<ONTAPtoolsIP>:8443/virtualization/ui/` to access ONTAP tools Manager.

2. On the login page, select **Reset password**.
3. Generate a password reset token using the ONTAP tools for VMware vSphere maintenance console:
   a. Log in to the vCenter Server and open the maintenance console.
   b. Enter `2` to select **System Configuration**.
   c. Enter `3` to select **Change 'maint' user password**.
4. In the password reset dialog, enter the reset token, username, and new password.
5. Select **Reset** to update the credentials.
6. Log in to ONTAP tools Manager with the new password.

Reset application user password in ONTAP tools

Follow these steps to reset the application user password needed for SRA and VASA Provider registration with vCenter Server using ONTAP tools for VMware vSphere.

Steps

1. Open a web browser and navigate to: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in using the administrator credentials configured during ONTAP tools deployment.
3. From the sidebar, select **Settings**.
4. On the **VASA/SRA credentials** page, select **Reset password**.
5. Enter and confirm the new password.
6. Select **Reset** to apply the new password.

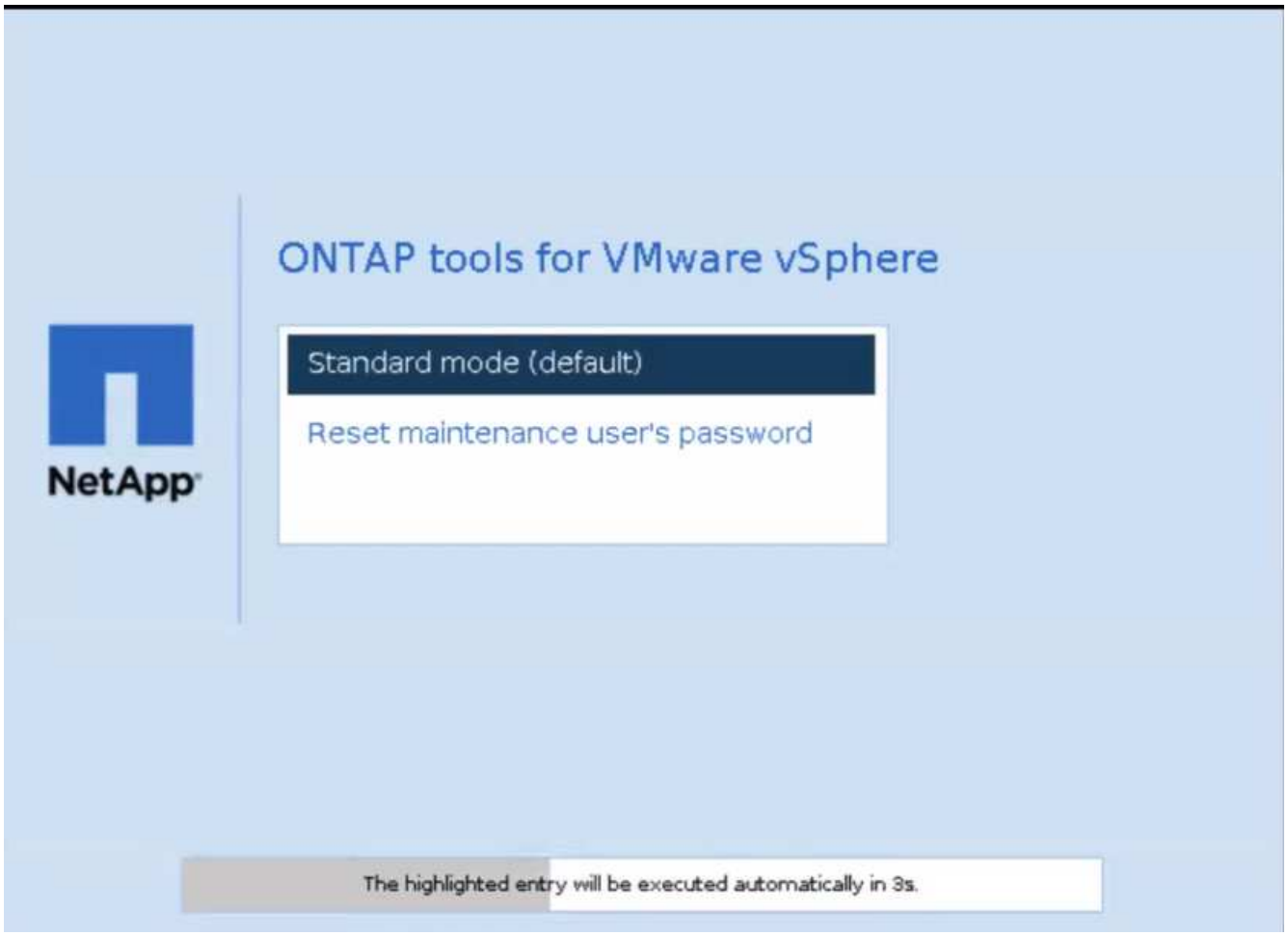
Reset the ONTAP tools maintenance console password

During guest OS restart operation, GRUB menu displays an option to reset maintenance console user password. Use this option to update the maintenance console user password on the VM. After you reset the password, 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 and confirm the new password. You have three attempts. The system restarts after you successfully enter the new password.
5. Press **Enter** to continue. The system updates the password 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 the **Restart Guest OS** option.

Manage host cluster protection

Modify a protected host cluster in ONTAP tools

You can change protection settings for a host cluster in a single workflow. The following changes are supported:

- 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.

> You need to perform storage discovery after you create, edit, or delete protection for a host cluster to reflect the changes. If you do not perform the storage discovery, the changes are reflected after the periodic storage discovery is triggered.

Monitor host cluster protection

Monitor the protection status, SnapMirror relationships, datastores, and SnapMirror status for each protected host cluster.

Steps

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

   The protection column displays an icon that shows the protection status.

3. Hover over the icon to see more details.

Add new datastores or hosts

Add hosts or create datastores on the protected cluster using the vCenter user interface.

Steps

1. Log in to the vSphere client.
2. To edit the properties of a protected cluster, you can either
   a. Go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu next to the cluster and select **Edit** or
   b. Right-click on a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. If you create a datastore in the vCenter user interface, it appears as unprotected. You can view all datastores in the cluster and their protection status in a dialog box. Select the **Protect** button to enable protection.

   > After creating a datastore in the vCenter Server user interface, select **Discover** on the overview page to show the datastore as a candidate for protection in the host cluster. The protection status updates to protected after the next periodic protection discovery.

4. If you add a new ESXi host, the protection status is shown as partially protected. Select the ellipsis menu under the SnapMirror settings and select **Edit** to set the proximity of the newly added ESXi host.

   > For Asynchronous relationships, editing is not supported in ONTAP tools because the target SVM for a tertiary site cannot be added to the same instance. To modify the relationship configuration, use System Manager or the CLI on the target SVM.

5. After making changes, select **Save**.
6. You can see the changes in the **Protect Cluster** window.

ONTAP tools creates a vCenter task, and you can track its 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. Go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu against the cluster and select **Edit** or
   b. Right-click on 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.

ONTAP tools creates a vCenter task, and you can track its progress in the **Recent task** panel.

Delete an existing SnapMirror relationship

To delete an SnapMirror asynchronous relationship, ensure that the secondary site SVM or cluster is added as a storage backend in ONTAP tools for VMware vSphere. You cannot delete all SnapMirror relationships at once. Deleting a relationship also removes the corresponding relationship from the ONTAP cluster. When you delete an Automated Failover Duplex SnapMirror relationship, the system unmaps the destination datastores and deletes the consistency group, LUNs, volumes, and igroups from the destination ONTAP cluster.

When you delete the relationship, the system rescans the secondary site to remove the unmapped LUN as an 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. Go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu against the cluster and select **Edit** or
   b. Right-click on a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. Select the ellipsis menu under the SnapMirror settings and select **Delete**.
   - If you delete an asynchronous policy type-based relationship of a protected host cluster, you must manually remove the storage elements from the tertiary storage cluster. Storage elements include consistency groups, volumes (for ONTAP systems), storage units (LUNs/Namespaces), and snapshots.
   - If you delete an Automated Failover Duplex (AFD) policy-based relationship of a protected host cluster, you can choose to remove the associated storage elements on the secondary storage directly from the interface.
   - If you delete an Automated Failover Duplex (AFD) policy-based relationship and the consistency group is now hierarchical for application-level backups, a warning appears about backup impact. Confirm to proceed. After confirmation, delete the associated storage elements on the secondary storage. If you do not remove them, they remain on the secondary site.

ONTAP tools creates a vCenter task, and you can track its progress in the **Recent task** panel.

Modify an existing SnapMirror relationship

To modify an SnapMirror asynchronous relationship, ensure the secondary site SVM or cluster is added as a storage backend in ONTAP tools for VMware vSphere. For Automated Failover Duplex SnapMirror relationships, you can update host proximity for uniform configurations or host access for non-uniform configurations. Changing between Asynchronous and Automated Failover Duplex policy types is not supported. You can configure proximity or access settings for newly discovered hosts in the cluster.

You cannot edit an existing SnapMirror asynchronous relationship.

Steps

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

ONTAP tools create a vCenter task. Track its progress in the **Recent task** panel.

Remove host cluster protection in ONTAP tools

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

Steps

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

   On this page, monitor protected host clusters, protection state, SnapMirror relationship, and status. Select consistency groups to view capacity, associated datastores, and child groups.

2. In the **Host cluster protection** window, select the ellipsis menu next to the cluster, and select **Remove protection**.
   - If you remove protection from a host cluster with only a SnapMirror asynchronous relationship, you must manually delete the storage elements. Storage elements include consistency groups, volumes (for ONTAP system), storage units (LUNs), and snapshots.
   - If you remove protection from a host cluster with only an automated failover duplex-based SnapMirror policy relationship and a non-hierarchical consistency group, you can delete the associated storage elements on the secondary storage directly from the same screen.
   - If you remove protection from a host cluster with both SnapMirror policies and a hierarchical consistency group for backups, a warning appears about backup impacts. Confirm to proceed. After confirmation, delete the associated storage elements on the secondary storage. If you do not clean up, the storage elements remain on the secondary site.

Recover the ONTAP tools setup

Beginning with ONTAP tools for VMware vSphere 10.5, the backup feature is enabled by default.

The datastore where you deploy ONTAP tools for VMware vSphere virtual machines stores the backup files. A folder named after the ONTAP tools IP address (dots replaced by underscores and suffixed with *OTV_backup*) keeps the two most recent backup files (*OTV_backup_1.tar.enc* and *OTV_backup_2.tar.enc*) and an info file (*OTV_backup_info.txt*) that contains the name of the latest backup.

Ensure that the new virtual machine uses the same ONTAP tools IP address and matches the initial system configuration, including enabled services, node size, and HA mode.

Steps

1. Download the backup files from the datastore of the original virtual machine to your local system.
   a. Go to the storage section and choose the datastore that contains the backup files for the virtual machine.
   b. Select the **Files** section.
   c. Download the required backup directory.
2. Power off the existing virtual machine. Then, deploy a new virtual machine using the same OVA file as the original deployment.
3. From the vCenter Server, open the maintenance console.
4. Log in as the maintenance user.
5. Enter `4` to select **Support and Diagnostics**.
6. Enter `2` to select **Enable remote diagnostic access** option and create a new password for the diagnostic access.
7. Choose a backup file from the downloaded directory. Refer to the *OTV_backup_info.txt* file to identify the latest backup.
8. Use the following command to transfer the backup file to the new virtual machine. When prompted, enter the diagnostic password.

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

   don’t alter the destination path and file name (/home/diag/system_recovery.tar.enc) mentioned in the command.

9. After the backup file is transferred, log in to the 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.

After you complete the recovery, ONTAP tools restores services and vCenter objects.

Uninstall ONTAP tools

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 after uninstalling ONTAP tools

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. Find out the ONTAP tools for VMware vSphere deployment type from the ONTAP tools management node VM. Run the following command to check the deployment type: *cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol*

   If it is an iSCSI deployment, 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. Enter the exact FlexVol volume name in the CLI command to delete a volume.
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