Configure ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 12, 2025

Table of Contents

Configure ONTAP tools for VMware vSphere

Add vCenter Server instances

Add vCenter Server instances to ONTAP tools for VMware vSphere to configure, manage, and protect your virtual datastores in your vCenter Server environment. When you add multiple vCenter Server instances, Custom CA certificates are required for secure communication between ONTAP tools and each vCenter Server.

About this task

By integrating with vCenter, ONTAP tools enables you to perform storage tasks like provisioning, snapshots, and data protection directly from the vSphere client, eliminating the need to switch to separate storage management consoles.

Steps

1. Open a web browser and navigate to the URL:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **vCenters** > **Add** to onboard the vCenter Server instances. Provide your vCenter IP address or hostname, username, password, and port details.

> You don't need an admin account to add vCenter instances to ONTAP tools. You can create a custom role without the admin account with limited permissions. Refer to Use vCenter Server RBAC with ONTAP tools for VMware vSphere 10 for details.

Adding a vCenter Server instance to ONTAP tools automatically triggers the following actions:

- The vCenter client plug-in is registered as a remote plug-in.
- Custom privileges for the plug-ins and APIs are applied to the vCenter Server instance.
- Custom roles are created to manage the users.
- The plug-in appears as a shortcut on the vSphere user interface.

Register the VASA Provider with a vCenter Server instance

You can register the VASA Provider with a vCenter Server instance using ONTAP tools for VMware vSphere. The VASA Provider settings section displays the VASA Provider registration status for the selected vCenter Server. In a multi-vCenter deployment ensure that you have custom CA certificates for each vCenter Server instance.

Steps

1. Log in to the vSphere client.
2. Select **Shortcuts** > **NetApp ONTAP tools** under the plug-ins section.
3. Select **Settings** > **VASA Provider settings**. The VASA Provider registration status will be displayed as not registered.

4. Select the **Register** button to register the VASA Provider.
5. Enter a name and credentials for the VASA Provider. The username can only contain letters, numbers, and underscores. Password length should be between 8 and 256 characters.
6. Select **Register**.
7. After a successful registration and page refresh, the registered VASA Provider's status, name, and version is displayed. After registration, the unregister action is activated.

What's next

Verify that the onboarded VASA Provider is listed under VASA Provider from the vCenter client:

Steps

1. Navigate to the vCenter Server instance.
2. Log in with the administrator credentials.
3. Select **Storage Providers** > **Configure**. Verify that the onboarded VASA Provider is listed correctly.

Install the NFS VAAI plug-in

The NFS vStorage API for Array Integration (NFS VAAI) plug-in is a software component that integrates VMware vSphere and NFS storage arrays. Install the NFS VAAI plug-in using ONTAP tools for VMware vSphere to leverage the advanced capabilities of your NFS storage array to offload certain storage-related operations from the ESXi hosts to the storage array itself.

Before you begin

- Download the NetApp NFS Plug-in for VMware VAAI installation package.
- Make sure you have the ESXi host and vSphere 7.0U3 latest patch or later versions and ONTAP 9.14.1 or later versions.
- Mount an NFS datastore.

Steps

1. Log in to the vSphere client.
2. Select **Shortcuts** > **NetApp ONTAP tools** under the plug-ins section.
3. Select **Settings** > **NFS VAAI Tools**.
4. When the VAAI plug-in is uploaded to vCenter Server, select **Change** in the **Existing version** section. If a VAAI plug-in is not uploaded to the vCenter Server, select **Upload** button.
5. Browse and select the `.vib` file and select **Upload** to upload the file to ONTAP tools.
6. Select **Install on ESXI host**, select the ESXi host on which you want to install the NFS VAAI plug-in, and then select **Install**.

   Only the ESXi hosts eligible for the plug-in installation are displayed. You can monitor the installation progress in the recent tasks section of the vSphere Web Client.

7. Restart the ESXi host manually after installation.

   When the VMware admin restarts the ESXi host, ONTAP tools for VMware vSphere automatically detects and enables the NFS VAAI plug-in.

What's next?

After you've installed the NFS VAAI plug-in and rebooted your ESXi host, you need to configure the correct NFS export policies for VAAI copy offload. When configuring VAAI in a NFS environment, configure the export policy rules with the following requirements in mind:

- The relevant ONTAP volume needs to allow NFSv4 calls.
- The root user should remain as root and NFSv4 should be allowed in all junction parent volumes.
- The option for VAAI support needs to be set on the relevant NFS server.

For more information on the procedure, refer to Configure the correct NFS export policies for VAAI copy offload KB article.

Related information

Support for VMware vStorage over NFS

Enable or disable NFSv4.0

ONTAP support for NFSv4.2

Configure ESXi host settings

Configuring ESXi server multipath and timeout settings ensures high availability and data integrity by allowing to seamlessly switch to a backup storage path if a primary path fails.

Configure ESXi server multipath and timeout settings

ONTAP tools for VMware vSphere checks and sets the ESXi host multipath settings and HBA timeout settings that work best with NetApp storage systems.

About this task

Depending on your configuration and system load, this process might take a long time. The task progress is displayed in the Recent Tasks panel.

Steps

1. From the VMware vSphere Web client home page, select **Hosts and Clusters**.
2. Right-click a host and select **NetApp ONTAP tools** > **Update host data**.
3. On the shortcuts page of the VMware vSphere Web client, select **NetApp ONTAP tools** under the plug-ins section.
4. Go to the **ESXi Host compliance** card in the overview (dashboard) of the ONTAP tools for VMware vSphere plug-in.
5. Select **Apply Recommended Settings** link.
6. In the **Apply recommended host settings** window, select the hosts you want to update to comply with NetApp recommended settings and select **Next**.

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

7. In the settings page, select the recommended values as required.

8. In the summary pane, check the values and select **Finish**. You can track the progress in the recent task panel.

Set ESXi host values

Using ONTAP tools for VMware vSphere, you can set timeouts and other values on the ESXi hosts to ensure the best performance and successful failover. The values that ONTAP tools for VMware vSphere sets are based on internal NetApp testing.

You can set the following values on an ESXi host:

HBA/CNA Adapter Settings

Sets the following parameters to default values:

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBA timeouts
- QLogic FC HBA timeouts

MPIO Settings

MPIO settings define the preferred paths for NetApp storage systems. They determine which of the available paths are optimized (as opposed to non-optimized paths that traverse the interconnect cable) and set the preferred path to one of those paths.

In high-performance environments, or when you are testing performance with a single LUN datastore, consider changing the load balance setting of the round-robin (VMW_PSP_RR) path selection policy (PSP) from the default IOPS setting of 1000 to a value of 1.

The MPIO settings do not apply to NVMe, NVMe/FC, and NVMe/TCP protocols.

NFS settings

Parameter	Set this value to…
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 or higher
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

Configure ONTAP user roles and privileges

You can configure new user roles and privileges for managing storage backends using the JSON file provided with ONTAP tools for VMware vSphere and ONTAP System Manager.

Before you begin

- You should have downloaded the ONTAP privileges file from ONTAP tools for VMware vSphere using *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*.
- You should have downloaded the ONTAP Privileges file from ONTAP tools using `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip`.

> ⓘ You can create users at cluster or directly at storage virtual machines (SVMs) level. You can also create users without using the user_roles.json file and if done so, you need to have a minimum set of privileges at SVM level.

- You should have logged in with administrator privileges for the storage backend.

Steps

1. Extract the downloaded *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* file.
2. Access ONTAP System Manager using the cluster management IP address of the cluster.
3. Log in to the cluster with admin privileges. To configure a user, perform the following steps:
   a. To configure cluster ONTAP tools user, select **Cluster** > **Settings** > **Users and Roles** pane.
   b. To configure SVM ONTAP tools user, select **Storage SVM** > **Settings** > **Users and Roles** pane.
   c. Select **Add** under Users.
   d. In the **Add User** dialog box, select **Virtualization products**.
   e. **Browse** to select and upload the ONTAP Privileges JSON file.

      The Product field is auto populated.

   f. Select the product capability as **VSC, VASA Provider and SRA** from the drop-down.

      The **Role** field is auto populated based on the product capability selected.

   g. Enter the required username and password.
   h. Select the privileges (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) required for the user, and then select **Add**.

The new role and user are added, and you can see the detailed privileges under the role that you have configured.

SVM aggregate mapping requirements

To use SVM user credentials for provisioning datastores, internally ONTAP tools for VMware vSphere creates volumes on the aggregate specified in the datastores POST API. The ONTAP does not allow the creation of volumes on unmapped aggregates on an SVM using SVM user credentials. To resolve this, you need to map the SVMs with the aggregates using the ONTAP REST API or CLI as described here.

REST API:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI:

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

Create ONTAP user and role manually

Follow the instructions in this section to create the user and roles manually without using the JSON file.

1. Access ONTAP System Manager using the cluster management IP address of the cluster.
2. Log in to the cluster with admin privileges.
   a. To configure cluster ONTAP tools roles, select **Cluster** > **Settings** > **Users and Roles** pane.
   b. To configure cluster SVM ONTAP tools roles, select **Storage SVM** > **Settings** > **Users and Roles** pane
3. Create Roles:
   a. Select **Add** under **Roles** table.
   b. Enter the **Role name** and **Role Attributes** details.

      Add the **REST API Path** and the respective access from the drop down.

   c. Add all the needed APIs and save the changes.
4. Create Users:
   a. Select **Add** under **Users** table.
   b. In the **Add User** dialog box, select **System Manager**.
   c. Enter the **Username**.
   d. Select **Role** from the options created in the **Create Roles** step above.
   e. Enter the applications to give access to and the authentication method. ONTAPI and HTTP are the required applications, and the authentication type is **Password**.
   f. Set the **Password for the User** and **Save** the user.

List of minimum privileges required for non-admin global scoped cluster user

The minimum privileges required for non-admin global scoped cluster user created without using the users JSON file are listed in this section. If a cluster is added in local scope, it is recommended to use the JSON file to create the users, because ONTAP tools for VMware vSphere requires more than just the Read privileges for provisioning on ONTAP.

Using APIs:

API	Access level	Used for
/api/cluster	Read-Only	Cluster Configuration Discovery
/api/cluster/licensing/licenses	Read-Only	License Check for Protocol specific licenses
/api/cluster/nodes	Read-Only	Platform type discovery
/api/security/accounts	Read-Only	Privilege Discovery
/api/security/roles	Read-Only	Privilege Discovery
/api/storage/aggregates	Read-Only	Aggregate space check during Datastore/Volume provisioning
/api/storage/cluster	Read-Only	To get the Cluster level Space and Efficiency Data
/api/storage/disks	Read-Only	To get the Disks associated in an Aggregate
/api/storage/qos/policies	Read/Create/Modify	QoS and VM Policy management
/api/svm/svms	Read-Only	To get SVM configuration in the case the Cluster is added locally.
/api/network/ip/interfaces	Read-Only	Add Storage Backend - To identify the management LIF scope is Cluster/SVM
/api/storage/availability-zones	Read-Only	SAZ Discovery. Applicable to ONTAP 9.16.1 release onwards and ASA r2 systems.

Create ONTAP tools for VMware vSphere ONTAP API based cluster scoped user

You need discovery, create, modify, and destroy Privileges to perform PATCH operations and automatic rollback in case of failure on datastores. Lack of these all these privileges together leads to workflow disruptions and cleanup issues.

Creating ONTAP tools for VMware vSphere ONTAP API based user with discovery, create storage, modify storage, destroy storage privileges enables initiating discoveries and manage ONTAP tools workflows.

To create a cluster scoped user with all privileges mentioned above, run the following commands:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all
```

```
security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
```

```
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly
```

```
security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly
```

Additionally, for ONTAP Versions 9.16.0 and above run the following command:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

For ASA r2 systems on ONTAP Versions 9.16.1 and above run the following command:

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

Create ONTAP tools for VMware vSphere ONTAP API based SVM scoped user

To create a SVM scoped user with all the privileges, run the following commands:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
```

```
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
```

```
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

Additionally, for ONTAP Versions 9.16.0 and above run the following command:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

To create a new API based user using the above created API based roles, run the following command:

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

Example:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

To unlock the account, to enable access to the management interface run the following command:

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Example:

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

Upgrade ONTAP tools for VMware vSphere 10.1 user to 10.3 user

For ONTAP tools for VMware vSphere 10.1 users with a cluster-scoped user created using the JSON file, use the following ONTAP CLI commands with user admin privileges to upgrade to the 10.3 release.

For product capabilities:

- VSC
- VSC and VASA Provider
- VSC and SRA
- VSC, VASA Provider, and SRA.

Cluster privileges:

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all

For ONTAP tools for VMware vSphere 10.1 user with a SVM scoped user created using the json file, use the ONTAP CLI commands with admin user privileges to upgrade to the 10.3 release.

SVM privileges:

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>

Adding command *vserver nvme namespace show* and *vserver nvme subsystem show* to the existing role adds the following commands.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Upgrade ONTAP tools for VMware vSphere 10.3 user to 10.4 user

Beginning with ONTAP 9.16.1 upgrade the ONTAP tools for VMware vSphere 10.3 user to 10.4 user.

For ONTAP tools for VMware vSphere 10.3 user with a cluster-scoped user created using the JSON file and ONTAP version 9.16.1 or above, use the ONTAP CLI command with admin user privileges to upgrade to the 10.4 release.

For product capabilities:

- VSC
- VSC and VASA Provider
- VSC and SRA
- VSC, VASA Provider, and SRA.

Cluster privileges:

```
security login role create -role <existing-role-name> -cmddirname "storage
availability-zone show" -access all
```

Add a storage backend

Adding a storage backend enables you to onboard an ONTAP cluster.

About this task

In case of multitenancy setups where vCenter acts as the tenant with an associated SVM, use ONTAP tools Manager to add the cluster. Associate the storage backend with the vCenter Server to map it globally to the onboarded vCenter Server instance. The vCenter tenant must onboard the desired Storage Virtual Machines (SVMs). This enables an SVM user to provision vVols datastores. You can add storage in vCenter using the SVM.

Add the local storage backends with cluster or SVM credentials using the ONTAP tools user interface. These storage backends are limited to a single vCenter. When using cluster credentials locally, the associated SVMs automatically map to the vCenter to manage vVols or VMFS. For VMFS management, including SRA, ONTAP tools supports SVM credentials without needing a global cluster.

Using ONTAP tools Manager

In a multi-tenant setup, you can add a storage backend cluster globally and SVM locally to use SVM user credentials.

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. Add the storage backend and provide the server IP address or FQDN, username, and password details.

   IPv4 and IPv6 address management LIFs are supported.

Using vSphere client user interface

When configuring a storage backend through the vSphere client user interface, it is important to note that the vVols datastores do not support the direct addition of an SVM user.

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. Select **Storage Backends** from the sidebar.
4. Add the storage backend and provide the server IP address, username, password, and port details.

   To add an SVM user directly, you can add cluster-based credentials and IPv4 and IPv6 address management LIFs or provide SVM-based credentials with an SVM management LIF.

What's next?

The list gets refreshed, and you can see the newly added storage backend in the list.

Associate a storage backend with a vCenter Server instance

Associate a storage backend with the vCenter Server to create a mapping between the storage backend and the onboarded vCenter Server instance globally.

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 vCenter from the sidebar.

4. Select the vertical ellipses against the vCenter Server instance that you want to associate with the storage backends.
5. Select the storage backend from the dropdown to associate the vCenter Server instance with the required storage backend.

Configure network access

If you've not configured the network access, all the discovered IP addresses from the ESXi host are added to the export policy by default. You can configure it to add a few specific IP addresses to the export policy and exclude the rest. However, when you perform a mount operation on the excluded ESXi hosts, the operation fails.

Steps

1. Log in to the vSphere client.
2. Select **NetApp ONTAP tools** in the shortcuts page under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Settings** > **Manage Network Access** > **Edit**.

   To add multiple IP addresses, separate the list with commas, range, Classless Inter-Domain Routing (CIDR), or a combination of all three.

4. Select **Save**.

Create a datastore

When you create a datastore at the host cluster level, the datastore is created and mounted on all the hosts of the destination, and the action is enabled only if the current user has the privilege to execute.

Interoperability between native datastores with vCenter Server and ONTAP tools managed datastores

ONTAP tools for VMware vSphere 10 creates nested igroups for datastores, with parent igroups specific to datastores and child igroups mapped to the hosts. You can create flat igroups from ONTAP system manager and use them to create VMFS datastores without using ONTAP tools. Refer to Manage SAN initiators and igroups for more information.

When the storage is onboarded to ONTAP tools and datastore discovery is run, flat igroups and VMFS datastores become ONTAP tools-managed and are converted to nested igroups. You cannot use the earlier flat igroups to create new datastores; you must use the ONTAP tools user interface or REST API to reuse the nested igroups.

Create a vVols datastore

Beginning with ONTAP tools for VMware vSphere 10.3, you can create a vVols datastore on ASA r2 systems with space-efficiency as thin.vVol. The VASA Provider creates a container and the desired protocol endpoints while creating the vVol datastore. This container will not have any backing volumes.

Before you begin

- Ensure that root aggregates aren't mapped to SVM.
- Ensure that the VASA Provider is registered with the selected vCenter.
- In the ASA r2 storage system, SVM should be mapped to aggregate for SVM user.

Steps

1. Log in to the vSphere client.
2. Right-click a host system, host cluster, or data center and select **NetApp ONTAP tools** > **Create Datastore**.
3. Select vVols **Datastore type**.
4. Enter the **Datastore name** and **Protocol** information.

   The ASA r2 system supports the iSCSI and FC protocols for vVols.

5. Select the storage VM where you want to create the datastore.
6. Under advanced options:
   - If you select the **Custom export policy**, ensure you run discovery in vCenter for all objects. It's recommended that you do not use this option.
   - You can select **Custom initiator group** name for the iSCSI and FC protocols.

   In ASA r2 storage system type SVM, storage units (LUN/namespace) aren't created because the datastore is only a logical container.

7. In the **Storage attributes** pane, you can create new volumes or use the existing volumes. However, you cannot combine these two types of volumes to create a vVols datastore.

   When creating a new volume, you can enable QoS on the datastore. By default, one volume is created for every LUN-created request. This step is not applicable for vVols datastores using the ASA r2 storage systems.

8. Review your selection in the **Summary** pane and select **Finish**.

Create an NFS datastore

A VMware Network File System (NFS) datastore uses the NFS protocol to connect ESXi hosts to a shared storage device over a network. NFS datastores are commonly used in VMware vSphere environments and offer several advantages, such as simplicity and flexibility.

Steps

1. Log in to the vSphere client.
2. Right-click a host system, host cluster, or data center and select **NetApp ONTAP tools** > **Create datastore**.
3. Select NFS in the **Datastore type** field.

4. Enter the datastore name, size, and protocol information in the **Name and protocol** pane. Select **Datastore cluster** and **Kerberos authentication** in the advanced options.

   Kerberos authentication is available only when the NFS 4.1 protocol is selected.

5. Select **Platform** and **Storage VM** in the **Storage** pane.
6. If you select **Custom export policy** under the advanced options, run the discovery in vCenter for all objects. It's recommended that you do not use this option.

   You cannot create an NFS datastore using the SVM's default/root volume policy.

   - In the advanced options, the **Asymmetric** toggle button is visible only if performance or capacity is selected in the platform drop-down.
   - When you choose the **Any** option in the platform dropdown, you can see the SVMs that are part of the vCenter irrespective of the platform or asymmetric flag.

7. Select the aggregate for volume creation in the **Storage Attributes** pane. In the advanced options, choose **Space Reserve** and **Enable QoS** as required.
8. Review the selections in the **Summary** pane and select **Finish**.

The NFS datastore is created and mounted on all the hosts.

Create a VMFS datastore

Virtual Machine File System (VMFS) is a clustered file system that stores virtual machine files in VMware vSphere environments. VMFS allows multiple ESXi hosts to access the same virtual machine files concurrently, enabling features like vMotion and High Availability.

On a protected cluster:

- You can create only a VMFS datastores. When you add a VMFS datastore to a protected cluster, the datastore becomes protected automatically.
- You cannot create a datastore on a data center with one or more protected host clusters.
- You cannot create a datastore at the ESXi host if the parent host cluster is protected with a relationship of "Automated Failover Duplex policy" type (uniform/non-uniform config).
- You can create a VMFS datastore only on an ESXi host protected by an asynchronous relationship. You cannot create and mount a datastore on an ESXi host that is part of a host cluster protected by the "Automated Failover Duplex" policy.

Before you begin

- Enable services and LIFs for each protocol on the ONTAP storage side.
- Map SVM to aggregate for SVM user in the ASA r2 storage system.
- Configure the ESXi host if you're using the NVMe/TCP protocol:
  1. Review the VMware Compatibility Guide

     VMware vSphere 7.0 U3 and later versions support the NVMe/TCP protocol. However, VMware vSphere 8.0 and later versions are recommended.

  2. Validate whether the Network Interface Card (NIC) vendor supports ESXi NIC with the NVMe/TCP protocol.

3. Configure the ESXi NIC for NVMe/TCP according to the NIC vendor specifications.
4. When using VMware vSphere 7 release, follow the instructions on the VMware site Configure VMkernel Binding for the NVMe over TCP Adapter to configure NVMe/TCP port binding. When using VMware vSphere 8 release, follow Configuring NVMe over TCP on ESXi, to configure the NVMe/TCP port binding.
5. For VMware vSphere 7 release, follow the instructions on page Enable NVMe over RDMA or NVMe over TCP Software Adapters to configure NVMe/TCP software adapters. For the VMware vSphere 8 release, follow Add Software NVMe over RDMA or NVMe over TCP Adapters to configure the NVMe/TCP software adapters.
6. Run Discover storage systems and hosts action on the ESXi host. For more information, refer to How to Configure NVMe/TCP with vSphere 8.0 Update 1 and ONTAP 9.13.1 for VMFS Datastores.

- If you are using the NVME/FC protocol, perform the following steps to configure the ESXi host:
  1. If not already enabled, enable NVMe over Fabrics(NVMe-oF) on your ESXi host(s).
  2. Complete SCSI zoning.
  3. Ensure that ESXi hosts and the ONTAP system are connected at a physical and logical layer.

To configure an ONTAP SVM for FC protocol, refer to Configure an SVM for FC.

For more information on using NVMe/FC protocol with VMware vSphere 8.0, refer to NVMe-oF Host Configuration for ESXi 8.x with ONTAP.

For more information on using NVMe/FC with VMware vSphere 7.0, refer to ONTAP NVMe/FC Host Configuration guide and TR-4684.

Steps

1. Log in to the vSphere client.
2. Right-click a host system, host cluster, or data center and select **NetApp ONTAP tools** > **Create Datastore**.
3. Select VMFS datastore type.
4. Enter the datastore name, size, and protocol information in the **Name and Protocol** pane. If you choose to add the new datastore to an existing VMFS datastore cluster, select the datastore cluster selector under Advanced Options.
5. Select storage VM in the **Storage** pane. Provide the **Custom initiator group name** in the **Advanced options** section as required. You can choose an existing igroup for the datastore or create a new igroup with a custom name.

   When NVMe/FC or NVMe/TCP protocol is selected, a new namespace subsystem is created and is used for namespace mapping. The namespace subsystem is created using the auto-generated name that includes the datastore name. You can rename the namespace subsystem in the **custom namespace subsystem name** field in the advanced options of the **Storage** pane.

6. From the **storage attributes** pane:
   a. Select **Aggregate** from the drop-down options.

   For ASA r2 storage systems, the **Aggregate** option is not shown because the ASA r2 storage is a disaggregated storage. When you choose an ASA r2 storage system type SVM, the storage attributes page shows the options for enabling QoS.

b. As per the selected protocol, a storage unit(LUN/Namespace) is created with a space reserve of type thin.

> Beginning in ONTAP 9.16.1, ASA r2 storage systems support up to 12 nodes per cluster.

c. Select the **Performance service level** for ASA r2 storage systems with 12 nodes SVM that is a heterogeneous cluster. This option is unavailable if the selected SVM is a homogeneous cluster or uses an SVM user.

   'Any' is the default performance service level (PSL) value. This setting creates the storage unit using the ONTAP balanced placement algorithm. However, you can select the performance or extreme option as required.

d. Select **Use existing volume**, **Enable QoS** options as required, and provide the details.

> In the ASA r2 storage type, volume creation or selection does not apply to storage unit creation(LUN/Namespace). Therefore, these options are not shown.

> You cannot use the existing volume to create a VMFS datastore with NVMe/FC or NVMe/TCP protocol; you should create a new volume.

7. Review the datastore details in the **Summary** pane and select **Finish**.

> If you create the datastore on a protected cluster, you can see a read-only message: "The datastore is being mounted on a protected Cluster."

Result

The VMFS datastore is created and mounted on all the hosts.

Copyright information

Trademark information