Configure ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

Table of Contents

Configure ONTAP tools for VMware vSphere . . . 1

- Add vCenter Server instances to ONTAP tools . . . 1
- Register the VASA Provider with a vCenter Server instance in ONTAP tools . . . 2
- Install the NFS VAAI plug-in using ONTAP tools . . . 2
- Configure ESXi host settings in ONTAP tools . . . 3
  - Configure ESXi server multipath and timeout settings . . . 4
  - Set ESXi host values . . . 4
- Configure ONTAP user roles and privileges for ONTAP tools . . . 5
  - SVM aggregate mapping requirements . . . 6
  - Create ONTAP user and role manually . . . 6
  - Upgrade ONTAP tools for VMware vSphere 10.1 user to 10.3 user . . . 14
  - Upgrade ONTAP tools for VMware vSphere 10.3 user to 10.4 user . . . 16
- Add a storage backend to ONTAP tools . . . 16
- Associate a storage backend with a vCenter Server instance in ONTAP tools . . . 19
- Configure network access in ONTAP tools . . . 19
- Create a datastore in ONTAP tools . . . 20

Configure ONTAP tools for VMware vSphere

Add vCenter Server instances to ONTAP tools

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

ONTAP tools integrates with vCenter Server to perform storage tasks like provisioning, snapshots, and data protection directly from the vSphere client.

Before you begin

- Ensure the vCenter Server certificate includes a valid Subject Alternative Name (SAN) extension with both DNS and IP address entries. For example:

  ```
  X509v3 extensions:
      X509v3 Subject Alternative Name:
          DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
  ```

  If the certificate does not include a SAN extension, or if the SAN extension does not contain the correct DNS or IP address values, ONTAP tools operations may fail due to certificate validation errors.

- The Primary Network Identifier (PNID) of the vCenter Server must be included in the SAN details. The PNID and DNS name should be identical and resolvable in DNS.
- It is recommended to deploy vCenter Server using its fully qualified domain name (FQDN), and ensuring the SAN in the certificate includes DNS Name=machine_FQDN for optimal compatibility and support.
- For more information, refer to VMware documentation:
  - vSphere Certificate Requirements for Different Solution Paths
  - Replace vCenter Machine SSL certificate Custom Certificate Authority Signed Certificate
  - Error: Subject Alternate Name (SAN) field does not contain the PNID. Please provide a valid certificate

> If FQDN is not available, you can set the PNID to the IP address and include the IP address in the SAN. However, this is not recommended by VMware.

Steps

1. Open a web browser and go 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.
4. In advanced options, fetch the vCenter Server certificate automatically (authorize it) or upload it manually.

ⓘ 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:

- ONTAP tools registers the vCenter client plug-in 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 in ONTAP tools

Use ONTAP tools for VMware vSphere to register the VASA Provider with a vCenter Server instance. This enables storage policy-based management, vVols support, and integration with VMware Live Site Recovery appliances on ONTAP systems.

VASA Provider settings show the registration status for the selected vCenter Server.

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 ONTAP tools displays the VASA Provider registration status 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. Set the password length between 8 and 256 characters.
6. Select **Register**.
7. After a successful registration and page refresh, ONTAP tools display the registered VASA Provider’s status, name, and version.

What’s next

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

Steps

1. Go 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 using ONTAP tools

The NFS vStorage API for Array Integration (NFS VAAI) plug-in connects VMware vSphere to NFS storage arrays. Use ONTAP tools for VMware vSphere to install the VAAI plug-in. This allows the NFS storage array to handle certain storage operations instead of

ESXi hosts.

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. If you have already uploaded the VAAI plug-in to vCenter Server, select **Change** in **Existing version**. If you have not, select **Upload**.
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**.

   The vSphere Web Client shows only the ESXi hosts that can install the plug-in. You can monitor the installation progress in the recent tasks section.

7. Restart the ESXi host manually after installation.

   After you restart the ESXi host, ONTAP tools for VMware vSphere automatically detect and enable the NFS VAAI plug-in.

What’s next?

After you install the NFS VAAI plug-in and reboot your ESXi host, configure the NFS export policies for VAAI copy offload. Ensure the export policy rules meet these requirements:

- The relevant ONTAP volume allows NFSv4 calls.
- The root user remains as root and NFSv4 is allowed in all junction parent volumes.
- The option for VAAI support is set on the relevant NFS server.

For more information, 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 in ONTAP tools

Configuring ESXi server multipath and timeout settings helps maintain data availability and integrity. It enables automatic failover to a backup storage path if the primary path becomes unavailable.

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

This process might take time, depending on your setup and system load. You can view the progress in the Recent Tasks panel.

Steps

1. From the VMware vSphere Web client home page, select **Hosts and Clusters**.
2. On the shortcuts page of the VMware vSphere Web client, select **NetApp ONTAP tools** under the plug-ins section.
3. Go to the **ESXi Host compliance** card 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 you want to update to use NetApp recommended 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.

Set ESXi host values

Use ONTAP tools for VMware vSphere to set timeouts and other values on ESXi hosts for optimal performance and failover. It sets these values based on 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 pick the best paths for NetApp storage systems. MPIO settings select the best path and use it.

For high-performance environments or when testing with a single LUN datastore, adjust the load balance setting of the round-robin (VMW_PSP_RR) path selection policy (PSP) to improve performance. Set the default IOPS value from 1000 to 1.

ⓘ The MPIO settings don’t 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 for ONTAP tools

Use this section to configure ONTAP user roles and privileges for storage backends with ONTAP tools for VMware vSphere and ONTAP System Manager. You can assign roles using the provided JSON files, manually create users and roles, and apply the minimum required privileges for non-admin accounts.

Before you begin

- Download the ONTAP Privileges file from ONTAP tools for VMware vSphere using *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*. After downloading the zip file, you find two JSON files. Use the ASA r2-specific JSON file when configuring an ASA r2 system.

  ⓘ You can create users at the cluster level or directly at the storage virtual machines (SVMs) level. If you do not use the user_roles.json file, ensure the user has the minimum required SVM permissions.

- Log in with administrator privileges for the storage backend.

Steps

1. Extract the *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* file that you downloaded.
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:
   a. To configure a cluster ONTAP tools user, select **Cluster** > **Settings** > **Users and Roles** pane.
   b. To configure an 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. For non-ASA r2 systems, select users_roles.json file and for ASA r2 systems, select users_roles_ASAr2.json file.

ONTAP tools automatically populates the Product field.

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

   ONTAP tools automatically populates the **Role** field based on the product capability you select.

g. Enter the required username and password.

h. Select the privileges (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) the user needs, and then select **Add**.

ONTAP tools adds the new role and user. You can view privileges under the role you configured.

SVM aggregate mapping requirements

When provisioning datastores using SVM user credentials, ONTAP tools for VMware vSphere creates volumes on the aggregate specified in the datastores POST API. ONTAP prevents SVM users from creating volumes on aggregates not mapped to the SVM. Map the SVM to the required aggregates using the ONTAP REST API or CLI before creating volumes.

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

Create users and roles manually without 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**.
   b. To configure cluster SVM ONTAP tools roles, select **Storage SVM** > **Settings** > **Users and Roles**.
3. Create roles:
   a. Select **Add** under **Roles** table.
   b. Enter the **Role name** and **Role Attributes** details.

      Add the **REST API Path** and choose the access from the drop-down list.

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

This page lists the minimum privileges required for a non-admin global-scoped cluster user without a JSON file. If a cluster is in local scope, use the JSON file to create users because ONTAP tools for VMware vSphere needs more than just the Read privileges for provisioning on ONTAP.

You can access functionality by 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 when 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.
/api/cluster/metrocluster	Read-Only	Gets MetroCluster status and configuration details.

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

> Discovery, create, modify, and destroy privileges are required for PATCH operations and automatic rollback on datastores. Missing permissions might cause workflow and cleanup issues.

An ONTAP API-based user with discovery, create, modify, and destroy privileges can 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

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

Run the following commands to create an SVM scoped user with all privileges:

```
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_
```

Run the following command to unlock the account and enable management interface access:

```
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>

To enable the following commands, add the commands *vserver nvme namespace show* and *vserver nvme subsystem show* to the existing role.

```
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 to ONTAP tools

Use ONTAP tools for VMware vSphere to add and manage storage backends for your ESXi hosts. You can onboard clusters or SVMs, enable MetroCluster support, and validate certificates for secure connectivity. You can configure storage backends using ONTAP tools Manager or the vSphere client, monitor certificate status, and manually rediscover resources after cluster changes.

To add a storage backend locally, use cluster or SVM credentials in the ONTAP tools interface. Local storage backends are available only to the selected vCenter Server. ONTAP tools maps SVMs to the vCenter Server for vVols or VMFS datastore management. For VMFS datastores and SRA workflows, you can use SVM credentials without mapping a cluster globally.

To add a global storage backend, use ONTAP cluster credentials in ONTAP tools Manager. Global storage backends enable discovery workflows to identify cluster resources required for vVol management. In multitenant environments, you can add an SVM user locally to manage vVols datastores.

If MetroCluster support is enabled in ONTAP, onboard both source and destination clusters as local or global storage backends.

Before you begin

Verify that the certificate includes a valid Subject Alternative Name (SAN) field. ONTAP systems use the SAN field to identify cluster and SVM management LIFs.

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.

5. Fetch the ONTAP cluster certificates automatically and authorize the certificate, or manually upload it by browsing to its location.

   ⓘ If needed, you can disable Subject Alternative Name (SAN) validation from the maintenance console. For instructions, see Change certificate validation flag.

6. If the storage backend you add is part of a MetroCluster configuration, ONTAP tools Manager shows a pop-up message to add the peered cluster. Select **Add** and provide the details for the MetroCluster peer storage backend.

   ⓘ After the ONTAP system performs a switchover and switchback, run the ONTAP tools discovery manually.

Using vSphere client user interface

ⓘ vVols datastores do not support direct addition of an SVM user through the vSphere client user interface.

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.

   ⓘ You can add a storage backend using cluster-based credentials with either IPv4 or IPv6 management LIFs. To add an SVM user directly, provide SVM-based credentials along with an SVM management LIF. If a cluster is already onboarded, you cannot onboard an SVM user from that cluster again.

5. Fetch the ONTAP cluster certificates automatically and authorize the certificate, or manually upload it by browsing to its location.
6. If the added storage backend is part of the MetroCluster configuration, ONTAP tools displays the **Add MetroCluster peer** screen. Select **Add peer** to add the peer storage backend.

ⓘ After the ONTAP system performs a switchover and switchback, run the ONTAP tools discovery manually.

What’s next?

ONTAP tools updates the list to show the new storage backend.

ONTAP tools list the newly added storage backend on the **Storage backends** page. If a certificate expires in 30 days or less, ONTAP tools shows a warning in the certificate expiry date column. After expiry, ONTAP tools marks the storage backend as unknown because it cannot connect to the storage system.

Related information

Configuring the clusters into a MetroCluster configuration

Associate a storage backend with a vCenter Server instance in ONTAP tools

Associate a storage backend with a vCenter Server instance to enable access for all vCenter Server instances. For MetroCluster configuration, when you associate a storage backend cluster, ensure you also associate its peer cluster with the vCenter Server.

Steps

1. Launch ONTAP tools Manager from a web browser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select vCenter from the sidebar.
4. Select the vertical ellipses next to the vCenter Server instance that you want to connect to the storage backends.
5. From the dropdown menu, choose the storage backend you want to associate with the selected vCenter Server instance.

Configure network access in ONTAP tools

By default, all IP addresses discovered from the ESXi host are automatically added to the export policy unless you configure network access. You can modify the export policy to allow access only from specific IP addresses. If an excluded ESXi host attempts a mount operation, 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, go 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 in ONTAP tools

When you create a datastore at the host cluster level, ONTAP tools mounts it on all destination hosts and enables the action only if you have the required privileges.

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

Beginning with ONTAP tools for VMware vSphere 10.4, ONTAP tools 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.

After you onboard the storage and run datastore discovery, ONTAP tools changes flat igroups in VMFS datastores to nested igroups. You cannot use earlier flat igroups to create new datastores. Use the ONTAP tools interface or REST API to reuse 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. The VASA Provider does not assign any backing volumes to this container.

Before you begin

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

Steps

1. Log in to the vSphere client.
2. Right-click on 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 don’t 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. Skip this step for vVols datastores on ASA r2 storage systems.

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

Create an NFS datastore

An NFS datastore connects ESXi hosts to shared storage using the NFS protocol. They are simple and flexible and are used in VMware vSphere environments.

Steps

1. Log in to the vSphere client.
2. Right-click on 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 don't use this option.

   ⓘ You cannot create an NFS datastore using the SVM's default or 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 all SVMs in the vCenter. Platform and asymmetric flag do not affect visibility.
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**.

ONTAP tools creates the NFS datastore and mounts it on all hosts.

Create a VMFS datastore

VMFS is a clustered file system for storing virtual machine files. Multiple ESXi hosts can access the same VM files simultaneously for vMotion and High Availability features.

On a protected cluster:

- You can create only VMFS datastores. Adding a VMFS datastore to a protected cluster automatically protects it.
- You cannot create a datastore on a data center with one or more protected host clusters.
- You cannot create a datastore on an ESXi host if the parent host cluster is protected by an "Automated Failover Duplex policy" (uniform or non-uniform configuration).
- 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. Check if the Network Interface Card (NIC) vendor supports ESXi NIC with the NVMe/TCP protocol.

3. Set up 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're 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 on 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. To add the new datastore to an existing VMFS cluster, select the datastore cluster in 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. ONTAP tools creates the namespace subsystem 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 storage is disaggregated. When you choose an ASA r2 storage system type SVM, the storage attributes page shows the options for enabling QoS.

b. ONTAP tools creates a storage unit (LUN/Namespace) with a thin space reserve based on the selected protocol.

> ⓘ 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 doesn’t apply to storage unit creation(LUN/Namespace). Therefore, these options aren’t shown.

> ⓘ You cannot use the existing volume to create a VMFS datastore with NVMe/FC or NVMe/TCP protocol. Create a new volume for the VMFS datastore.

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

ONTAP tools creates the VMFS datastore and mounts it on all the hosts.

Copyright information

Trademark information