NetApp

ONTAP tools for VMware vSphere 10.0 documentation

ONTAP tools for VMware vSphere 10

NetApp
September 30, 2025

Table of Contents

ONTAP tools for VMware vSphere 10.0 documentation

Release notes

Provides important information about this release of ONTAP tools for VMware vSphere, including fixed issues, known issues, cautions, and limitations.

For more information, see the ONTAP tools for VMware vSphere 10.0 Release Notes.

Concepts

ONTAP tools Overview

The ONTAP tools for VMware vSphere manages provisioning of datastores and virtual-machines in VMware environments that use NetApp storage backends. It enables the administrators to manage the storage within the vCenter Server directly and hence simplifies the storage and data management for VMware environments.

ONTAP tools for VMware vSphere 10.0 release is a collection of horizontally scalable, event driven, microservices deployed as an Open Virtual Appliance (OVA). It is packaged in various deployment form factors like Open Virtual Appliance (OVA) and Software as a service (SaaS) for on-prem.

ONTAP tools for VMware vSphere consists of:

- Virtual machine functionality
- VASA Provider for VM granular
- Storage policy-based management

ONTAP tools VASA Provider

ONTAP tools VASA provider supports high scale requirements for Virtual volumes (vVols). It supports NFS protocol, iSCSI protocol, and OVA deployment.
VASA Provider for VMware is a product that provides lifecycle management in a VMware deployment with ONTAP.

VASA Provider configurations for vVols

You can use VASA Provider for ONTAP to create and manage VMware Virtual Volumes (vVols). You can provision, edit, mount, and delete a vVols datastore. You can also add storage to the vVols datastore or remove storage from the vVols datastore to provide greater flexibility.

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

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

> ⓘ It is a good practice to include multiple FlexVol volumes in a vVols datastore for performance and flexibility. Because FlexVol volumes have LUN count restrictions that limit the number of virtual machines, including multiple FlexVol volumes allows you to store more virtual machines in your vVols datastore. Adding diverse volumes increases the datastore capabilities where there could be a mix of thin and thick volumes so that both kind of VMs can be created on the datastore.

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

- **Config**

VMware vSphere uses this vVols datastore to store configuration information.

In SAN (block) implementations, the storage is a 4 GB LUN.
vCenter 8 takes the capacity to 256GB LUN in Thin provisioning.

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

- **Data**

This vVols contains operating system information and user files.

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

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

- **Swap**

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

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

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

- **Memory**

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

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

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

Role based access control

Overview of role-based access control in ONTAP tools

vCenter Server provides role-based access control (RBAC) that enables you to control access to vSphere objects. vCenter Server provides centralized authentication and authorization services at many different levels within its inventory, using user and group rights with roles and privileges. vCenter Server features five main components for managing RBAC:

Components	Description
Privileges	A privilege enables or denies access to perform actions in vSphere.
Roles	A role contains one or more system privileges where each privilege defines an administrative right to a certain object or type of object in the system. By assigning a user a role, the user inherits the capabilities of the privileges defined in that role.

Users and groups	Users and groups are used in permissions to assign roles from Active Directory (AD) or potentially local windows users/groups as well (not recommended)
Permissions	Permissions allow you to assign privileges to users or groups to perform certain actions and make changes to objects inside vCenter Server. vCenter Server permissions affect only those users who log into vCenter Server rather than users who log into an ESXi host directly.
Object	An entity upon which actions are performed. VMware vCenter objects are data centers, folders, resource pools, clusters, hosts, and VMs

To successfully complete a task, you must have the appropriate vCenter Server RBAC roles. During a task, ONTAP tools checks a user's vCenter Server roles before checking the user's ONTAP privileges.

> ⓘ The vCenter Server roles apply to ONTAP tools vCenter users, not to administrators. By default, administrators have full access to the product and do not require roles assigned to them.

The users and groups gain access to a role by being part of a vCenter Server role.

Key points about assigning and modifying roles for vCenter Server

You only need to set up vCenter Server roles if you want to limit access to vSphere objects and tasks. Otherwise, you can log in as an administrator. This login automatically allows you to access all vSphere objects.

Where you assign a role determines the ONTAP tools tasks that a user can perform. You can modify one role at any time.
If you change the privileges within a role, the user associated with that role should log out and then log back in to enable the updated role.

Standard roles packaged with ONTAP tools

To simplify working with vCenter Server privileges and RBAC, ONTAP tools provide standard ONTAP tools roles that enable you to perform key ONTAP tools tasks. There is also a read-only role that enables you to view the information, but not perform any tasks.

You can view the ONTAP tools standard roles by clicking **Roles** on the vSphere Client Home page. The roles that ONTAP tools provides enable you to perform the following tasks:

Role	Description
NetApp ONTAP tools Administrator	Provides all of the native vCenter Server privileges and ONTAP tools-specific privileges that are required to perform some of the ONTAP tools tasks.
NetApp ONTAP tools Read Only	Provides read-only access to ONTAP tools. These users cannot perform any ONTAP tools actions that are access-controlled.

NetApp ONTAP tools Provision	Provides some of the native vCenter Server privileges and ONTAP tools-specific privileges that are required to provision storage. You can perform the following tasks: • Create new datastores • Manage datastores

The Manager UI admin role is not registered with vCenter. This role is specific to the manager UI.

If your company requires that you implement roles that are more restrictive than the standard ONTAP tools roles, you can use the ONTAP tools roles to create new roles.

In this case, you would clone the necessary ONTAP tools roles and then edit the cloned role so that it has only the privileges your user requires.

Permissions for ONTAP storage backends and vSphere objects

If the vCenter Server permission is sufficient, ONTAP tools then checks the ONTAP RBAC privileges (your ONTAP role) that are associated with the storage backends credentials (the user name and password) to determine whether you have sufficient privileges to perform the storage operations that are required by that ONTAP tools task on that storage backend. If you have the correct ONTAP privileges, you can access the storage backends and perform the ONTAP tools task. The ONTAP roles determine the ONTAP tools tasks that you can perform on the storage backend.

Recommended ONTAP roles when using ONTAP tools for VMware vSphere

You can set up several recommended ONTAP roles for working with ONTAP tools for VMware vSphere and role-based access control (RBAC). These roles contain the ONTAP privileges that are required to perform the required storage operations that are executed by the ONTAP tools tasks.

To create new user roles, you must log in as an administrator on storage systems running ONTAP. You can create ONTAP roles using ONTAP System Manager 9.8P1 or later. See List of minimum privileges required for non-admin global scoped cluster user for more information.

Each ONTAP role has an associated user name and password pair, which constitute the credentials of the role. If you do not log in by using these credentials, you cannot access the storage operations that are associated with the role.

As a security measure, the ONTAP tools-specific ONTAP roles are ordered hierarchically. This means that the first role is the most restrictive role and has only the privileges that are associated with the most basic set of ONTAP tools storage operations. The next role includes both its own privileges and all of the privileges that are associated with the previous role. Each additional role is less restrictive with regard to the supported storage operations.

The following are some of the recommended ONTAP RBAC roles when using ONTAP tools. After you create these roles, you can assign the roles to users who have to perform tasks related to storage, such as provisioning virtual machines.

1. Discovery

This role enables you to add storage systems.

2. Create Storage

   This role enables you to create storage. This role also includes all of the privileges that are associated with the Discovery role.

3. Modify Storage

   This role enables you to modify storage. This role also includes all of the privileges that are associated with the Discovery role and the Create Storage role.

4. Destroy Storage

   This role enables you to destroy storage. This role also includes all of the privileges that are associated with the Discovery role, the Create Storage role, and the Modify Storage role.

If you are using VASA Provider for ONTAP, you should also set up a policy-based management (PBM) role. This role enables you to manage storage by using storage policies. This role requires that you also set up the "Discovery" role.

Configure high availability for ONTAP tools

The ONTAP tools supports a high-availability (HA) configuration to help provide uninterrupted functionality of ONTAP tools during failure.

The ONTAP tools relies on the VMware vSphere High-availability (HA) feature and vSphere fault tolerance (FT) feature to provide high availability. High-availability (HA) solution provides for rapid recovery from outages caused by:

- Host failure

  (i) | Only single node failure is supported.

- Network failure
- Virtual machine failure (Guest OS failure)
- Application (ONTAP tools) crash

No additional configuration is required for ONTAP tools to provide high availability. Only the vCenter Server and ESXi hosts must be configured with the VMware vSphere HA feature or the vSphere FT feature based on their requirements. Both HA and FT require clustered hosts together with shared storage. FT has additional requirements and limitations.

In addition to the VMware vSphere HA solution and vSphere FT solution, ONTAP tools also helps keep the ONTAP tools services running at all times.

  (i) | vCenter HA is not supported by ONTAP tools.

AutoSupport

AutoSupport is a mechanism that proactively monitors the health of your system and

automatically sends messages to NetApp technical support, your internal support organization, and a support partner.

AutoSupport is enabled by default when you configure your storage system for the first time. AutoSupport begins sending messages to technical support 24 hours after AutoSupport is enabled.

You can enable or disable AutoSupport only at the time of deployment. It is recommended to leave it enabled. Enabling AutoSupport can significantly help speed problem determination and resolution should a problem occur on your storage system. By default, the system collects AutoSupport information and stores it locally, even if you disable AutoSupport.
You need to whitelist 216.240.21.18 // support.netapp.com URL in your network for successful transmission.

Deploy ONTAP tools

ONTAP tools for VMware vSphere Quick Start

ONTAP tools for VMware vSphere is a single vCenter Server plug-in that includes ONTAP tools and VASA Provider extensions. ONTAP tools are recommended for all ONTAP vSphere environments as it configures ESXi host settings and provisions ONTAP storage using best practices. The VASA Provider is required for virtual volumes (vVols)support.

Preparing for installation

You deploy the plug-in as a virtual appliance, which reduces your effort of installing and registering each product separately with the vCenter Server.

Deployment requirements

Before deploying the ONTAP tools for VMware vSphere, you should be familiar with the space requirements forthe deployment package and some basic host system requirements.

You can use the ONTAP tools with either a Windows vCenter Server or with a VMware vCenter Server VirtualAppliance (vCSA). You must deploy the ONTAP tools on a supported vSphere that includes ESXi system.

- **Installation package space requirements per node**

  - 10 GB for thin provisioned installations

  - 200 GB for thick provisioned installations

- **Host system sizing requirements per node**
  Recommended memory as per the size of deployment and per node is as shown in the table below:

Type of deployment	CPUs	Memory(GB)
Small (S)	8	16
Medium (M)	12	24
Large (L)	16	32

Minimum storage and application requirements:

Storage, host, and applications	Version requirements
ONTAP	ONTAP 9.10.1 , 9.11 , 9.12, and 9.13
VMware vSphere	Minimum supported VMware version is 7.0.3.
ESXi hosts	ESXi 7.0.3 or later version
vCenter server	vCenter 7.0.3
VASA provider	3.0

Storage, host, and applications	Version requirements
OVA Application	10.0

For more information, see Requirements for deploying the ONTAP tools

ONTAP tools requirements

- Configure and set up your vCenter Server environment.
- Download the .ova file.
- The login credentials for your vCenter Server instance.
- Delete the browser cache to avoid any browser cache issue during the deployment of the ONTAP tools.
- Configure the default gateway to be used by the virtual appliance to respond to ICMP pings.
- A valid DNS hostname for the virtual appliance.

Deploying ONTAP tools

Steps

1. Download `.zip` file that contains binaries and signed certificates from the NetApp Support Site to a vSphere Client system to deploy the ONTAP tools.
2. Extract the `.zip` file and deploy the `.ova` file.
3. Log in to the vSphere server.
4. Navigate to the resource pool or the host where you want to deploy the OVA.
5. Right-click the required datacenter, and select **Deploy OVF template…**.
6. You can either enter the URL for the .ova file or browse to the folder where the .ova file is saved, and then select **Next**.
7. Enter the required details to complete the deployment.

You can view the progress of the deployment from the Tasks tab, and wait for deployment to complete.

Requirements for deploying the ONTAP tools

Before deploying the ONTAP tools for VMware vSphere, you should be familiar with the space requirements for the deployment package and some basic host system requirements.

You can use the ONTAP tools with either a Windows vCenter Server or with a VMware vCenter Server Virtual Appliance (vCSA). You must deploy the ONTAP tools on a supported vSphere that includes ESXi system.

- **Installation package space requirements per node**
  - 10 GB for thin provisioned installations
  - 200 GB for thick provisioned installations

- **Host system sizing requirements per node**
  Recommended memory as per the size of deployment and per node is as shown in the table below:

Type of deployment	CPUs	Memory(GB)
Small (S)	8	16
Medium (M)	12	24
Large (L)	16	32

Minimum storage and application requirements:

Storage, host, and applications	Version requirements
ONTAP	ONTAP 9.10.1 , 9.11 , 9.12, and 9.13
VMware vSphere	Minimum supported VMware version is 7.0.3.
ESXi hosts	ESXi 7.0.3 or later version
vCenter server	vCenter 7.0.3
VASA provider	3.0
OVA Application	10.0

The Interoperability Matrix Tool (IMT) contains the latest information about the supported versions of ONTAP, vCenter Server, ESXi hosts, and plug-in applications.

Interoperability Matrix Tool

Additional deployment considerations

You must consider few requirements while customizing the deployment ONTAP tools.

Application user password

This is the password assigned to the administrator account. For security reasons, it is recommended that the password length is eight to thirty characters long and contains a minimum of one upper, one lower, one digit, and one special character. Password expires after 90 days.

Appliance maintenance console credentials

You must access the maintenance console by using the "maint" user name. You can set the password for the "maint" user during deployment. You can use the Application Configuration menu of the maintenance console of your ONTAP tools to change the password.

vCenter Server IP address

- You should provide the IP address (IPv4) of the vCenter Server instance to which you want to register ONTAP tools.

  The type of ONTAP tools and VASA certificates generated depends on the IP address (IPv4) that you have provided during deployment.

- The ONTAP tools IP address used to register with vCenter Server depends on the type of vCenter Server IP address (IPv4) entered in the deployment wizard.

  Both the ONTAP tools and VASA certificates will be generated using the same type of IP address used

during vCenter Server registration.

- Ensure that VM's are not migrated during installation.

ⓘ IPv6 is not supported in ONTAP tools for VMware vSphere 10.0 release.

Appliance network properties

Specify a valid DNS hostname (unqualified) as well as the static IP address for the ONTAP tools and the other network parameters. DHCP is not supported in ONTAP tools for VMware vSphere 10.0 release. All of these parameters are required for proper installation and operation.

How to download ONTAP tools

You can download the `.zip` file that contains binaries (*.ova*) and signed certificates for the ONTAP tools for VMware vSphere from the [NetApp Support Site](#).

The *.ova* file includes the ONTAP tools. When the deployment is complete, ONTAP tools and VASA products are installed in your environment. By default, ONTAP tools starts working as soon as you decide on the subsequent deployment model and choose whether to enable VASA Provider based on your requirements.

Content library

Content library in VMware is a container object which stores VM templates, vApp templates, and other types of files. Deployment with content library provides you a seamless experience as it is not depended on the network connectivity.
You need to create a content library to store the OVA before deploying them in HA configuration. Do not select any security policy or set any password for the content library.
Create the content library using the following steps:

Steps

1. Login to VSphere client.

2. Select the horizontal ellipsis next to vSphere client and select **Content library**.

3. Select **Create** button on the right side of the page.

4. Provide a name for the library and create the content library.

Deployment Checklist

The checklist here helps you to have all the information handy before you begin the deployment. Make sure to note down these values for your setup before deploying.

You should be aware of the basic storage backend requirements, application requirements, and license requirements before you begin deploying the ONTAP tools for VMware vSphere.
Before you deploy ONTAP tools for VMware vSphere, it is good practice to plan your deployment and decide how you want to configure ONTAP tools in your environment.

First Node and other common fields

☐ VASA Provider Username(*)

- ☐ Administrator Username(*)
- ☐ NTP Servers (provided to the vCenter for time synchronization)

Certificate Details

- ☐ Enable Custom CA Certificate
- ☐ Root and Intermediate certificates (ignore when self-signed is enabled)
- ☐ Leaf certificate and Private key (ignored when self-signed is enabled)
- ☐ Domain name(*) (ignored when self-signed is enabled)

Load balancer and API server details

- ☐ Load Balancer IP(*)
- ☐ Virtual IP for K8s Control Plane(*)

ONTAP Details

- ☐ ONTAP Management LIF(*) (Cluster management IP)
- ☐ ONTAP Data LIF(*)
- ☐ Storage VM(*)
- ☐ ONTAP Cluster Username(*)
- ☐ Enable Migration
- ☐ Primary VM
- ☐ Content Library Name(*)
- ☐ OVF Template Name(*)
- ☐ Hostname(*)
- ☐ Username(*)

First Node Network details

- ☐ HostName(*)
- ☐ IPAddress(*)
- ☐ Prefix length (Only for IPv6)
- ☐ Netmask (Only for IPv4)(*)
- ☐ Gateway(*)
- ☐ Primary DNS(*)
- ☐ Secondary DNS(*)
- ☐ Search Domains(*)

Second Node - Node Network details

- ☐ HostName(*)
- ☐ IPAddress(*)

Third Node - Node Network details

- ☐ HostName(*)
- ☐ IPAddress(*)

Prepare to deploy ONTAP tools

ONTAP tools for VMware vSphere supports multi vCenter Server that includes VASA Provider.

You should be aware of the basic storage backend requirements, application requirements, and license requirements before you begin deploying the ONTAP tools for VMware vSphere.
Before you deploy ONTAP tools for VMware vSphere, it is good practice to plan your deployment and decide how you want to configure ONTAP tools in your environment.

Preparing for deployment

Following are the ONTAP tools requirements before proceeding with the deployment:

- Configure and set up your vCenter Server environment.

- Download the *.ova* file.

- Make sure the host or the resource pool where the OVA is deployed has the minimum resources mentioned in the **Requirements for deploying the ONTAP tools** section.

- Delete the browser cache.

- You need two Virtual IPs for Load Balancer and Kubernetes API Server. Get two free IPs in the VLAN, used for deployment, which is used to access the services post deployment.

- Procure CA certificates (root , Leaf, and Intermediate certificates) from the commercial CA.

- In case of multi-vCenter deployment where Custom CA certificates are mandatory, map the **Domain Name** on which the certificate is issued to the **Virtual IP**. Perform a ping check on the domain name to check whether the domain is getting resolved to the intended IP.

- A storage VM on ONTAP with NFS enabled is required. Follow the below steps to configure the storage VM:

  - Have both your ONTAP System Manager and ONTAP CLI open.

  - If you prefer to create a new storage VM, login to your ONTAP System Manager and create a storage VM with NFS enabled.

  - Add an aggregate with at least 100GB.

  - To verify if the aggregate is added successfully:

    a) Login to your ONTAP CLI

    b) Run the command, vserver show -fields aggr-list

    c) If your aggregate has not been listed against your default storage VM, run the command: vserver modify <storage VM name> -aggr-list <aggregate name>

    To find the name of the aggregate you want to add to your default storage VM, you can use the following command in the ONTAP CLI: *aggr show*

    This command displays a list of aggregates on the storage system, and you can find the name of the aggregate you need to use in the **Aggregate** column.

◦ There are two options with deployment configuration, one is cluster credentials and the other is SVM credentials or direct SVM. For direct SVM, you need to configure the management LIF for the SVM before starting the deployment. Skip this for cluster credentials.

◦ Make sure network route exists, login to your ONTAP CLI and run the command, network route show -vserver <storage VM name>

   If it does not exist then login to your ONTAP CLI and run the following commands, net route create -vserver <vserver name> -destination <destination IP> -gateway <gateway IP> -metric 20

◦ Make sure that an Export Policy exists for the storage VM. On your ONTAP System Manager, go to **Storage** > **Storage VMs** > **[storage VM name]** > **Settings** > **Export Policies**. If there is no export policy follow the next step.

◦ Create an export policy rule using the following commands from ONTAP CLI

   vserver export-policy rule create -vserver <storage VM name> -policyname <export policy name> -clientmatch <ESXI-IP> -rorule any -rwrule any -superuser any

   (i)   Make sure that *superuser* value is not *none*.

How to deploy Non-HA single node configuration

You can configure Non-HA single node in either small, medium, or large configurations.

- Small Non-HA configuration contains 8 CPUs and 16 GB RAM.
- Medium Non-HA configuration contains 12 CPUs and 24 GB RAM.
- Large Non-HA configuration contains 16 CPUs and 32 GB RAM.

Make sure network route is present.
Example: C1_sti67-vsim-ucs154k_1679633108::> network route create -vserver <SVM> -destination 0.0.0.0/0 -gateway <gateway_ip>

About this task

This task gives you instructions on how to install Non-HA single node in small, medium, or high configurations.

Steps

1. Log in to the vSphere server.
2. Navigate to the resource pool or the host where you want to deploy the OVA.
3. Right-click the required datacenter, and select **Deploy OVF template…**.
4. You can either enter the URL for the *.ova* file or browse to the folder where the *.ova* file is saved, and then select **Next**.
5. Select a name and folder for the virtual machine and select **Next**.
6. Select the host and select **Next**
7. Review the summary of the template and select **Next**.
8. Read and accept the license agreement and select **Next**.
9. In the **Configuration window**, select **Non-HA single Node(small)**, **Non-HA single Node(Medium)**, or

Non-HA single Node(large) configuration.

10. In the Configuration window choose the required size of Non-HA single Node configuration and select **Next**.

11. Select the datastore where you need to deploy the OVA and select **Next**.

12. Select the source and destination network and select **Next**.

13. Select **Customize template** > **system configuration** window. Enter the following details:

    a. VASA provider username and password: This username and password is used for registering the VASA provider in the vCenter.

    b. The **Enable ASUP** checkbox is selected by default.

       The ASUP can be enabled or disabled only during deployment.

    c. Administrator Username and Administrator Password: This is the password used to login to **ONTAP Tools Manager** UI.

    d. Enter NTP server information in **NTP Servers** field.

    e. Maintenance user password: This is used to grant access to 'Maint Console Options'.

14. In the **Customize template** > **VASA Provider Certificates** window, enter the following details:

    a. Check Enable Custom CA certificate check box. This is required for multi-VC enablement. In case of non multi-VC environment, ignore the check box. There is no need to mention the certificates and domain name, you need to only provide the virtual IP details.

    b. Copy and paste the Root and Intermediate certificates.

    c. Copy and paste the Leaf certificates and Private key.

    d. Enter the Domain name with which you generated the certificate.

    e. Enter the Load Balance IP details..

15. In **Customize template** > **Deployment Configuration** window, enter the following details:

    a. Enter a free IP Address in Virtual IP for K8s Control Plane. You need this for K8s API Server.

    b. Select the checkbox against **Enable SVM scoping** option when you intend to use direct SVM. To use ONTAP cluster, do not select the checkbox.

       (i) When SVM scope is enabled you should have already enabled SVM support with management IP.

    c. Enter the details shown in the below image:

Enable SVM scoping	Ignore when cluster scoping is required
	☐
ONTAP/SVM Management LIF(*)	Specify the Management LIF for trident
	⚠
ONTAP/SVM Data LIF(*)	Specify the Data LIF for trident
	⚠
Storage VM	Specify the storage VM Name
	Ignored when SVM scop
ONTAP/SVM Username(*)	Specify the OnTap Cluster Username
	⚠
ONTAP/SVM Password(*)	Specify the OnTap Cluster Password
	Password 👁 ⚠
	Enter a password to enable authentication.

    d. Enter the ONTAP Cluster or the SVM Management IP in **ONTAP/SVM Management LIF**.

    e. Enter the ONTAP Cluster or the SVM **ONTAP/SVM Data LIF**.

    f. For Storage VM, you can choose to either provide your ONTAP's default storage VM details or you can create a new storage VM. Do not enter the value in **Storage VM** field when Enable SVM scoping is selected as this filed is ignored.

    g. Enter the ONTAP/SVM Username.

    h. Enter the ONTAP/SVM Password.

    i. Enable Migration is disabled by default. Do not alter this choice.

    j. Primary VM is enabled by default. Do not alter this choice.

16. In **Customize template** > **Node Configuration** window enter the network properties of the OVA.

> ℹ The information provided here will be validated for proper patterns during installation process. In case of discrepancy, an error message will be displayed on the web console and you will be prompted to correct any incorrect information provided.

    a. Enter the Host name.

    b. Enter the IP Address mapped to the host name.

    c. Prefix length (only for IPV6)

    d. Netmask (only for IPV4)

    e. Gateway

    f. Primary DNS

    g. Secondary DNS

    h. Search Domains

17. Review the details in the **Ready to complete** window, select **FINISH**.

As the task gets created, the progress is shown in the vSphere task bar.

18. Power on the VM after the completion of the task.

    The installation begins. You can track the the installation progress in VM's web console.
    As part of the installation, Node configurations are validated. The inputs provided under different sections under the **Customize template** in the OVF form are validated. In case of any discrepancies, a dialog prompts you to take corrective action.

19. To make necessary changes in the dialog prompt, follow the below steps:

    a. Double click on the web console to start interacting with the console.

    b. Use UP and DOWN arrow keys on your keyboard to navigate across the fields shown.

    c. Use RIGHT and LEFT arrow keys on your keyboard to navigate to the right or left end of the value provided to the field.

    d. Use TAB to navigate across the panel to enter your values, **OK** or **CANCEL**.

    e. Use ENTER to select either **OK** or **CANCEL**.

20. On selecting **OK** or **CANCEL**, the values provided would again be validated. You have the provision to correct any values for 3 times. If you fail to correct within the 3 attempts, the product installation stops and you are advised to try the installation on a fresh VM.

21. After successful installation, web console shows the message stating the ONTAP tools for VMware vSphere is in Healthy State.

How to deploy HA three node configuration

You can configure HA three node in either small, medium, or large configurations.

- Small HA three node contains 8 CPUs and 16 GB RAM per node.
- Medium HA three node contains 12 CPUs and 24 GB RAM per node.
- Large HA three node contains 16 CPUs and 32 GB RAM per node.

About this task

This task gives you instructions on how to install HA three node in small, medium, or high configurations.

> (i) Creating the content library is a mandatory step for deploying HA three node configuration. See How to download ONTAP tools for details.

> (i) Before proceeding with the deployment, set the cluster's Distributed Resource Scheduler (DRS) on the inventory to **Conservative** during the installation of ONTAP tools.

Steps

1. Log in to the vSphere server.

2. Navigate to the content library and select your content library.

3. Select **Actions** in the right side of the page and select **Import item** and import the OVA file.

4. Navigate to the resource pool or the host where you want to deploy the OVA.

5. Right-click the required datacenter, and select **Deploy OVF template…**.

6. Select the content library where the *.ova* file is saved, and then select **Next**.

7. Select a name and folder for the virtual machine and select **Next**.

8. Select the host and select **Next**

9. Review the summary of the template and select **Next**.

10. Read and accept the license agreement and select **Next**.

11. In the **Configuration window**, select **HA three Node(small)**, **HA three Node(Medium)**, or **HA three Node(large)** configuration, depending on your requirement.

12. Select the storage for the configuration and disk files, select **Next**.

13. Select the destination network for each source network, select **Next**.

14. Select **Customize template** > **system configuration** window. Enter the following details:

    a. VASA provider username and password: This username and password is used for registering the VASA provider in the vCenter.

    b. The **Enable ASUP** checkbox is selected by default.

       The ASUP can be enabled or disabled only during deployment.

    c. Administrator Username and Administrator Password: This is the password used to login to **ONTAP tools Manager** UI.

    d. Enter NTP server information in **NTP Servers** field.

    e. Maintenance user password: This is used to grant access to 'Maint Console Options'.

15. In the **Customize template** > **VASA Provider Certificates** window, enter the following details:

    a. Check Enable Custom CA certificate check box. This is required for multi-VC enablement. In case of non multi-VC environment, ignore the check box. There is no need to mention the certificates and domain name, you need to only provide the virtual IP details.

    b. Copy and paste the Root and Intermediate certificates.

    c. Copy and paste the Leaf certificates and Private key.

    d. Enter the Domain name with which you generated the certificate.

    e. Enter the Load Balance IP details.

16. In **Customize template** > **Deployment Configuration** window, enter the following details:

    a. Enter a free IP Address in Virtual IP for K8s Control Plane. You need this for K8s API Server.

    b. Select the checkbox against **Enable SVM scoping** option when you intend to use direct SVM. To use ONTAP cluster, do not select the checkbox.

       (i) When SVM scope is enabled you should have already enabled SVM support with management IP.

    c. Enter the details shown in the below image:

Enable SVM scoping	Ignore when cluster scoping is required ☐
ONTAP/SVM Management LIF(*)	Specify the Management LIF for trident ⓘ
ONTAP/SVM Data LIF(*)	Specify the Data LIF for trident ⓘ
Storage VM	Specify the storage VM Name Ignored when SVM scop
ONTAP/SVM Username(*)	Specify the OnTap Cluster Username ⓘ
ONTAP/SVM Password(*)	Specify the OnTap Cluster Password **Password** 👁 ⓘ Enter a password to enable authentication.

d. Enter the ONTAP Cluster or the SVM Management IP in **ONTAP/SVM Management LIF**.

e. Enter the ONTAP Cluster or the SVM **ONTAP/SVM Data LIF**.

f. For Storage VM, you can choose to either provide your ONTAP's default storage VM details or you can create a new storage VM. Do not enter the value in **Storage VM** field when Enable SVM scoping is selected as this filed is ignored.

g. Enter the ONTAP/SVM Username.

h. Enter the ONTAP/SVM Password.

i. Enable Migration is disabled by default. Do not alter this choice.

j. Primary VM is enabled by default. Do not alter this choice.

17. In **Customize template** > **Content Library Details** window, enter the **Content Library Name** and the **OVF Template Name**.

18. In **Customize template** > **vCenter Configuration** window, provide the details of the vCenter where the content library is hosted.

19. In **Customize template** > **Node Configuration** window, enter the network properties of the OVA for all the three nodes.

> ⓘ The information provided here will be validated for proper patterns during installation process. In case of discrepancy, an error message will be displayed on the web console and you will be prompted to correct any incorrect information provided.

Enter the following details:

a. Host name.

b. IP Address mapped to the host name.

c. Prefix length (only for IPV6)

d. Netmask (only for IPV4)

    e. Gateway

    f. Primary DNS

    g. Secondary DNS

    h. Search Domains

20. In **Customize template** > **Node 2 Configuration** and **Node 3 Configuration** window, enter the following details:

    a. HostName

    b. IP Address

21. Review the details in the **Ready to complete** window, select **FINISH**.

As the task gets created, the progress is shown in the vSphere task bar.

22. Power on the VM after the completion of the task.

The installation begins. You can track the the installation progress in VM's web console.
As part of the installation, Node configurations are validated. The inputs provided under different sections under the **Customize template** in the OVF form are validated. In case of any discrepancies, a dialog prompts you to take corrective action.

23. To make necessary changes in the dialog prompt, follow the below steps:

    a. Double click on the web console to start interacting with the console.

    b. Use UP and DOWN arrow keys on your keyboard to navigate across the fields shown.

    c. Use RIGHT and LEFT arrow keys on your keyboard to navigate to the right or left end of the value provided to the field.

    d. Use TAB to navigate across the panel to enter your values, **OK** or **CANCEL**.

    e. Use ENTER to select either **OK** or **CANCEL**.

24. On selecting **OK** or **CANCEL**, the values provided would again be validated. You have the provision to correct any values for 3 times. If you fail to correct within the 3 attempts, the product installation stops and you are advised to try the installation on a fresh VM.

25. After successful installation, web console shows the message stating the ONTAP tools for VMware vSphere is in Healthy State.

Configure ONTAP tools

Manage network access

This feature enables you to specify specific ESXi host address to be allowed for datastore mount operation.

When you have multiple IP addresses for ESXi hosts, all the discovered IP addresses from the host are added to an Export policy. If you do not want to add all IP addresses to export policy, provide a setting for whitelisted IP addresses in a comma separated list or range or CIDR, or combination of all three for each vCenter.

If the setting is not provided, export policy adds all IP addresses discovered in the pre-mount step. If the setting is provided, ONTAP tools adds only the ones which fall within the whitelisted IPs or range. If none of the IPs of a host belong to the whitelisted IPs, the mount on that host fails.

By default all host IP's are added to the export policy.

Use the following API to add IP addresses for whitelisting:

```
patch /api/v1/vcenters/{vcguid}/settings/ip-whitelist


{
    value: string
}


GET /api/v1/vcenters/{vcguid}/settings/ip-whitelist


{
    value: string
}
```

Configure user roles and privileges

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

What you'll need

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

> ℹ️ You can create users at cluster or direct 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://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip` file.

2. Access ONTAP System Manager. To access ONTAP system manager use the cluster management IP of the cluster.

3. Login as the cluster or SVM user.

4. Select **CLUSTER** > **Settings** > **Users and Roles** pane.

5. Select **Add** under Users.

6. In the **Add User** dialog box, select **Virtualization products**.

7. Select **Browse** to select and upload the ONTAP Privileges JSON file.

   The PRODUCT field is auto populated.

8. Select the required capability from the PRODUCT CAPABILITY drop-down menu.

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

9. Enter the required username and password.

10. Select the privileges (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) required for the user, and then click **Add**.

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

> ⓘ The uninstall operation does not remove ONTAP tool roles but removes the localized names for the ONTAP tool specific privileges and appends the prefix `XXX missing privilege` to them. When you reinstall ONTAP tools or upgrade to a newer version of the ONTAP tools, all of the standard ONTAP tools roles and ONTAP tools-specific privileges are restored.

SVM aggregate mapping requirements

To use direct SVM credentials for provisioning datastores, internally ONTAP tools create 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 direct SVM credentials. To resolve this, you need to map the SVMs with the aggregates using the 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. To access ONTAP system manager use the cluster management IP of the cluster.

2. Login as the cluster or SVM user.

3. Select **CLUSTER** > **Settings** > **Users and Roles** pane.

4. 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.

5. Create Users:

    a. Select **Add** under **Users** table.

    b. In the **Add User** dialog box, select **System Manager**.

    c. Enter the **USERNAME**.

    d. Select the **ROLE** from the options created in the **Create Roles** step above.

    e. Enter the applications to give access to and the authentication method. The ONTAPI and HTTP are the required application 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 is listed in this section.
If cluster is added in local scope, it is recommended to use the JSON file to create the users, as ONTAP tools require 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/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 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	Read-Only	Cluster user must have this privilege to get the correct storage backend status. Otherwise, ONTAP tools Manager UI shows "unknown" storage backend status.

ONTAP tools manager user interface

ONTAP tools for VMware vSphere 10.0 is a Multi-tenant system, which manages multiple vCenters. An administrator needs more control over the vCenters being managed and storage backends being onboarded.

ONTAP tools manager provides more control and power to ONTAP tools administrator, which helps in overall management of the appliance, tenants, and storage backends.

The ONTAP tools performs:

- vCenter management - Register and unregister vCenters to ONTAP tools

- Storage backend management - Register and unregister ONTAP Storage clusters to ONTAP tools and map them to onboarded vCenters globally.

  Storage backend is global when added from ONTAP tools manager or commons APIs and they are local when added from the vCenter APIs.
  Example: For multi-tenant setup, you can add storage backend (cluster) globally and SVM locally to use direct SVM credentials.

- Log bundle downloads

To access ONTAP tools UI, launch `https://loadBalanceIP:8443/virtualization/ui/` from the browser and login with ONTAP tools administrator credentials provided during deployment.
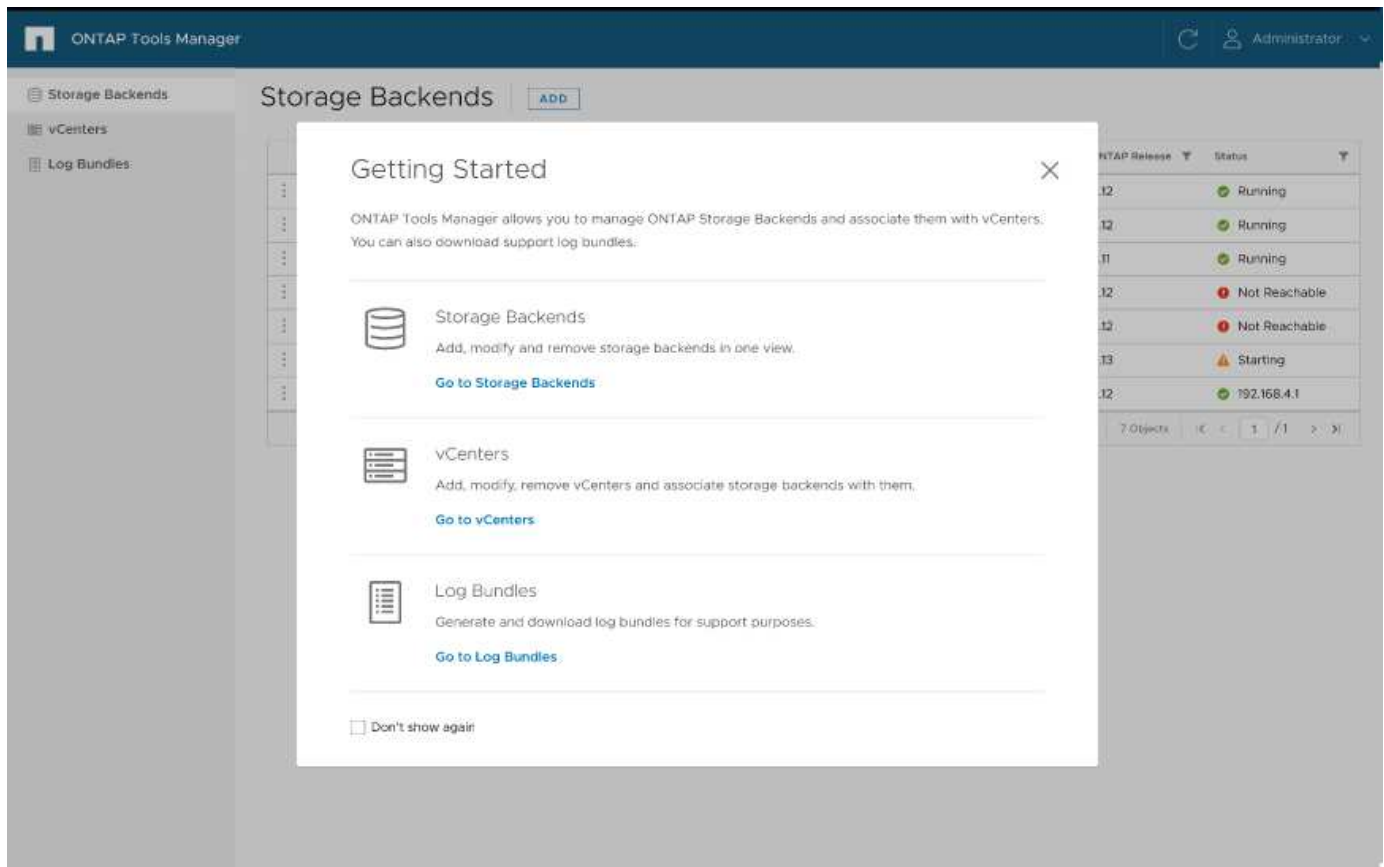
You can select **Don't show again** option to not see this pop up when you login again from the same browser.

Add vCenter

vCenters are the central management platforms that allow you to control hosts, virtual machines (VM), and storage backends.

About this task

You can add and manage multiple vCenters with one instance of ONTAP tools for VMware vCenter 10.0.

Steps

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.
2. Select vCenters from the sidebar
3. Select **ADD** to onboard vCenters with vCenter IP Address/Hostname, username, password, and port.

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

Add storage backend

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

About this task

This task helps you to onbord the ONTAP cluster.

Steps

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select **Storage Backends** from the sidebar.

3. Select **Add**.

4. Provide the Server IP Address or FQDN, Username, and Password details and select **Add**.

   > ℹ️ Only IPV4 management LIFs are supported.

Associate storage backend with vCenter

vCenter listing page shows the associated number of storage backends. Each vCenter has option to Associate a storage backend

About this task

This task help you to create mapping between storage backend and onboarded vCenter globally.

Steps

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select vCenters from the sidebar.

3. Click on the vertical ellipsis against the vCenter that you want to associate with storage backends.

4. Select storage backend from the dropdown in the pop up.

5. Select **Associate Storage Backend** option to associate vCenter with the required storage backend.

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

Onboard storage backend (SVM or Cluster) with vCenter

Use the following API to onboard the storage backends and map the SVM to vCenter locally. See Configure user roles and privileges section for the ONTAP SVM user privileges.

```
POST /virtualization/api/v1/vcenters/<vcguid>/storage-backends

{
    "hostname_or_ip": "172.21.103.107",
    "username": "svm11",
    "password": "xxxxxx"
}
```

	The ID from the above API response is used in discovery.

You need to pass x-auth for the API. You can generate this x-auth from the new API added under Auth in Swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

Register VASA Provider to vCenter

You can register VASA provide to vCenter by using either self signed certificate or CA signed certificate. Self signed certificate is generated using VMware CA handshake.

About this task

You need to have the CA signed certificate placed in vCenter when using the CA signed certificate method.

Steps

1. Navigate to vCenter server.
2. Select **Configure** > **Storage Providers**.
3. Click the **Add** icon.
4. Enter the connection information for the storage provider:

   a. Name: Any user-friendly name like "ScaleoutVP"

   b. URL: `https://<name>/virtualization/version.xml` - the name in the URL corresponds to Virtual IP provided during the OVA deployment for Single vCenter deployment (or) Domain name for Multi-vCenter deployments. Add the certificates to the URL. Same certificates are published to vCenter.

   c. Credentials: <VASA Provider username>/< VASA Provider password> provided during OVA deployment.

5. After the VASA is registered, click **OK**.
   Ensure that it is listed under Storage Provider and the status is Online.

   If you have placed CA signed certificate in vCenter, the VASA registration continues with CA signed certificate. Else, the handshaking fails and registration defaults to SSA certificate.

6. You can register multiple vCenters to a single scaleout vp instance.
   Repeat the steps mentioned above to register multiple vCenters.

Create vVols datastore

You can create vVols datastore with new volumes or with existing volumes. You can also create vVols datastore with the combination of existing volumes and new volumes.

	Check to ensure root aggregates are not mapped to SVM.

You need to pass x-auth for the API. You can generate this x-auth from the new API added under Auth in Swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

1. Create vVols datastore with new volume.
   Get Aggregate id, storage_id(SVM uuid) using ONTAP REST API.

```
POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores
```

Use the following URI to check the status:

```
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID
>?includeSubJobsAndTasks=true`
```

Request Body for NFS datastore

```
{
    "name":"nfsds1",
    "protocol":"nfs",
    "platform_type":"aff",
    "moref":"domain-c8",
    "volumes":[
        {
            "is_existing":false,
            "name":"vol_nfs_pvt",
            "size_in_mb":2048000,
            "space_efficiency":"thin",
            "aggregate":{
                "id":"d7078b3c-3827-4ac9-9273-0a32909455c2"
            },
            "qos":{
                "min_iops":200,
                "max_iops":5000
            }
        }
    ],
    "storage_backend":{
        "storage_id":"654c67bc-0f75-11ee-8a8c-00a09860a3ff"
    }
}
```

Request body for iSCSI datastore:

```
{
    "name" : "iscsi_custom",
    "protocol" : "iscsi",
    "platform_type": "aff",
    "moref" : "domain-c8",
    "volumes" : [
        {
            "is_existing" : false,
            "name" : "iscsi_custom",
            "size_in_mb" : 8034,
            "space_efficiency" : "thin",
            "aggregate" : {
                "id" : "54fe5dd4-e461-49c8-bb2d-6d62c5d75af2"
            }
        }
    ],
    "custom_igroup_name": "igroup1",
    "storage_backend": {
                        "storage_id": "eb9d33ab-1960-11ee-9506-
00a0985c6d9b"    }
}
```

1. Create vVols datastore with existing volumes.

   Get aggregate_id and volume_id using ONTAP REST API.

   ```
   POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
   691250bfe2df/vvols/datastores
   ```

   Request Body

```
    {
    "name" : "nfsds2",
    "protocol" : "nfs",
    "platform_type": "aff",
    "moref" : "domain-c8",
    "volumes" : [
        {
             "is_existing": true,
             "id": "e632a632-1412-11ee-8a8c-00a09860a3ff"
        }
    ],
    "storage_backend": {
                    "storage_id": "33a8b6b3-10cd-11ee-8a8c-
00a09860a3ff"    }

}
```

Verify registered SVM

Verify that the onboarded SVM is listed under VASA Provider from vCenter UI.

Steps

1. Navigate to vCenter Server.

2. Log in with the administrator credentials.

3. Select **Storage Providers**.

4. Select **Configure**.

5. Under Storage Provider/storage backends verify that the onboarded SVM is listed correctly.

Manage ONTAP tools

Manage datastores

Expand or shrink Storage of vVol Datastore

There are APIs to increase or decrease the available storage.

Steps

Use the following API to expand or shrink the vVols datastore:

```
PATCH
/virtualization/api/v1/vcenters/{vcguid}/vvols/datastores/{moref}/volumes
```

Examples

- Modify vVols datastore for add new volume

```
  PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/volumes

   Request Body
  {
   "operation": "grow",
   "volumes": [{
       "is_existing": false,
       "name": "exp3",
       "size_in_mb": 51200,
       "space_efficiency": "thin",
       "aggregate": {
           "id": "1466e4bf-c6d6-411a-91d5-c4f56210e1ab"
       },
       "storage_backend": {
           "storage_id": "13d86e4f-1fb1-11ee-9509-005056a75778"
       },
       "qos": {
           "max_iops": 5000
       }
   }]
 }
```

- Modify vVols datastore for add existing volume

```
  PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/volumes

    Request Body
    {
      "operation": "grow",
      "volumes": [{
        "is_existing": true,
        "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
      }]
    }
```

- Modify vVols datastore for remove volume and delete volume from storage

```
  PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/volumes?delete_volumes=true

    Request Body
    {
      "operation": "shrink",
      "volumes": [{
        "is_existing": true,
        "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
      }]
    }
```

- Modify vVols datastore for remove volume and do not delete volume from storage

```
  PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/volumes?delete_volumes=false

    Request Body
    {
      "operation": "shrink",
      "volumes": [{
        "is_existing": true,
        "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
      }]
    }
```

Delete vVols datastore

This API deletes the VMware Virtual Volumes (vVols) datastore from storage.

About this task

A vVols datastore exists as long as at least one FlexVol volume is available on the datastore. If you want to delete a vVols datastore in a HA cluster, you should first unmount the datastore from all hosts within the HA cluster, and then delete the residing *.vsphere-HA* folder manually using the vCenter server user interface.

Steps

Use the following API to delete vVols datastore.

```
DELETE
/virtualization/api/v1/vcenters/{vcguid}/vvols/datastores/{moref}
```

Examples

- Delete vVols datastore and delete volumes from storage

```
  DELETE /api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-28?delete_volumes=true
```

> (i) Delete vVols Datastore workflow deletes datastore-volumes if you have passed the delete_volume flag as true irrespective of if the datastore-volume is managed or not managed.

- Delete vVols datastore and do not delete volumes from storage

```
  DELETE /api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-28?delete_volumes=false
```

Response:

```
{

    "id": "1889"

}
```

Mount and unmount a vVols datastore

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

Use the following API to mount or unmount a vVols datastore.
You need to pass x-auth for the API. You can generate this x-auth from the new API added under Auth in Swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

```
PATCH
/virtualization/api/v1/vcenters/{vcguid}/vvols/datastores/{moref}/hosts
```

Get vVol datastore moref from vCenter.

Request Body

```
{
  "operation": "mount",
  "morefs": [
    "host-7044"
  ],
}
```

Examples:

- Mount on additional host

Use the following API to mount on additional host:

```
/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/hosts

    Request Body
    {
     "operation": "mount",
     "morefs": ["host-13"],
    }
```

- Unmount on additional host

Use the following API to unmount on additional host:

```
/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/hosts

    Request Body
    {
     "operation": "unmount",
     "morefs": ["host-13"],
    }
```

Manage storage backend

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

Add storage backend

Follow the steps below to add storage backends.

Steps

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select **Storage Backends** from the sidebar.

3. Select **Add**.

Modify storage backend

Follow the steps below to modify the existing storage backend.

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select storage backends from the sidebar.

3. Select the **Storage Backend** you want to modify

4. Click on the vertical ellipsis menu and select **Modify**.

5. Enter the **Username** and **Password** to modify the storage backend.

Remove storage backend

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

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select **Storage Backends** from the sidebar.

3. Select the storage backend you want to remove

4. Click on the vertical ellipsis menu and select **Remove**.

Manage vCenter

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

Add vCenter

You can add and manage multiple vCenters with one instance of ONTAP tools for VMware vCenter 10.0.

Steps

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select vCenters from the sidebar

3. Select **ADD** to onboard vCenters with vCenter IP Address/Hostname, username, password, and port.

4. Navigate to **Storage Backend** page and select **Add to onboard storage backend** (ONTAP Cluster) with Hostname, username, password, and port.

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

Associate or Dissociate storage backend with vCenter

vCenter listing page shows the associated number of storage backends. Each vCenter has option to Associate or Disassociate a storage backend
This task help you to create mapping between storage backend and onboarded vCenter globally.

Steps

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select vCenters from the sidebar.

3. Click on the vertical ellipsis against the vCenter that you want to associate or dissociate with storage backends.

4. Select **Associate or Dissociate storage backend** depending on what action you want to perform.

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

Modify vCenter

Follow the steps below to modify the vCenters.

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select vCenters from the sidebar

3. Click on the vertical ellipsis against the vCenter that you want modify and select **Modify**.

4. Modify the vCenter details and select **Modify**.

Remove vCenter

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

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.
2. Select vCenters from the sidebar
3. Click on the vertical ellipsis against the vCenter that you want remove and select **Remove**.

> ℹ️ Once you remove the vCenter, it will no longer be maintained by the application.

Manage Storage threshold

Use the following Get threshold API to retrieve the configured storage threshold limits for volume and aggregate.

```
GET/virtualization/api/v1/vcenters/{vcguid}/storage-thresholds
```

Examples:
Get the Storage thresholds per vcenter by vcenter guid

```
GET "/api/v1/vcenters/beded9ad-6bbb-4c9e-b4c6-691250bfe2da/storage-thresholds"
```

Use the following PATCH configure alarm for volume and aggregate to generate notification when configured threshold limits are reached.

```
PATCH/virtualization/api/v1/vcenters/{vcguid}/storage-thresholds
```

Examples:
Update the Storage thresholds per vcenter by vcenter guid. Default limits are 80% for nearly-full and 90% for full.
Modifying all threshold settings

```
{{{}PATCH "/api/v1/vcenters/beded9ad-6bbb-4c9e-b4c6-691250bfe2da/storage-
thresholds"
Request Body
{
"volume":

{ "nearly_full_percent": 80, "full_percent": 90 }
,
"aggregate": {
"nearly_full_percent": 80,
"full_percent": 90
}
}{}}}{}
```

Manage vVol Lifecycle

You can manage Virtual Volumes (vVols) using the VMWare vCenter user interface. For details, refer to VMware documentation.

Managed iGroup and Export policies

In ONTAP, export polices are used to provide volume data path access to hosts and initiator groups (igroups) are used to provide logical unit number (LUN) data path access to ESXi hosts.

When virtual volume datastores are created or mounted to hosts in vCenter, these hosts need to be given access to volumes (NFS) or LUNs (iSCSI) depending on the protocol type of the datastore.

The export policy is dynamic and the new export policy is created in format of trident-uuid. On your ONTAP System Manager, go to **Storage** > **Storage VMs** > **[storage VM name]** > **Settings** > **Export Policies** to see the export policy.

The igroups and export policies in ONTAP tools are managed in an efficient manner and provide the following benefits:

- Supports migrated export Policies and igroups.
- No interruption of Virtual Machine input and output operations.
- Supports mounting on additional hosts without manual intervention.
- Minimizes the need for managing number of igroups and export Policies.
- A garbage collector automatically deletes all the unused managed igroups and export Policies periodically.
- If datastore is provisioned at host cluster level then igroup is created with all host initiators under the host cluster that are added to the igroup.

Access ONTAP tools maintenance console

Overview of ONTAP tools maintenance console

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

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

> (i)   You must set a password for the `diag` user while enabling remote diagnostics.

You should use the **Summary** tab of your deployed ONTAP tools to access the maintenance console. When you click ▶, the maintenance console starts.

Console Menu	Options
Application Configuration	1. Display server status summary 2. Change LOG level for VASA Provider Services
System Configuration	1. Reboot virtual machine 2. Shutdown virtual machine 3. Change 'maint' user password 4. Change time zone 5. Add new NTP server 6. Increase jail disk size (/jail) 7. Upgrade 8. 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

Configure remote diagnostic access

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

What you will need

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

About this task

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

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

    The login session remains valid only until midnight the next day.

  - You log in as a diag user again using SSH.

Steps

1. From the vCenter Server, open a console to VASA Provider.
2. Log in as the maintenance user.
3. Enter 4 to select Support and Diagnostics.
4. Enter 3 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 the SSH on other nodes

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

What you will need

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

About this task

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

Steps

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

3. Enter `4` to select Support and Diagnostics.

4. Enter `1` to select Access diagnostic shell.

5. Enter `y` to proceed.

6. Run the command *sudo systemctl restart ssh*.

Update the vCenter and ONTAP credentials

You can update the vCenter and ONTAP credentials using the maintenance console.

What you will need

You need to have maint user login credentials.

About this task

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

Steps

1. From the vCenter Server, open a console to VASA Provider.

2. Log in as the maintenance user.

3. Enter `4` to select Support and Diagnostics.

4. Enter `1` to select Access diagnostic shell.

5. Enter `y` to proceed.

6. Update the credentials as required:

   a. For Updating the ONTAP credentials run the command:

      otv-update --ontapUsername <new username> --ontapPassword <new password>

   b. For Updating the vCenter credentials run the command:

      otv-update --vcenterUsername <new username> --vcenterPassword <new password>

   c. For Updating the datalif run the command:

      otv-update --dataLif <new Datalif IP>

Collect the log files

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

Steps

1. Launch `https://loadBalanceIP:8443/virtualization/ui/` from browser with ONTAP tools administrator credentials provided during deployment.

2. Select **Log Bundles** from the sidebar.

   This operation can take several minutes.

3. Select **GENERATE** to generate the log files.

4. Enter the label for the Log Bundle and select **GENERATE**.

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

Discovery

Discovery interval can be configured as part of the configuration map. Scheduled discovery runs for every 60 mins. The API given here is to run the discovery on demand for a given storage backend which is added in the local scope.

Use the following API to run discovery:

```
POST
/virtualization/api/v1/vcenters/{vcguid}/storage-backends/{id}/discovery-
jobs
```

ⓘ | See Onboard storage backend (SVM or Cluster) section and get ID from post storage backend API response.

Discovery from this API endpoint is supported only for local scoped storage backends and not for the global scoped storage backends.
If the storage backend type is cluster, discovery implicitly runs for the child svms.
If the storage backend type is svm, discovery only runs for the selected svm.

Example:

To run discovery on a storage backend specified by ID

```
POST
/api/v1/vcenters/3fa85f64-5717-4562-b3fc-2c963f66afa6/storage-
backends/74e85f64-5717-4562-b3fc-2c963f669dde/discovery-jobs
```

You need to pass x-auth for the API. You can generate this x-auth from the new API added under Auth in Swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

Migrate ONTAP tools

Migrate to the latest release of ONTAP tools

When migrating storage data, storage backends are onboarded manually using REST APIs. When migrating VASA provider data, data is exported from existing Derby database and imported into the MongoDB database.

> (i) It is recommended to migrate classic setup only if the setup is servicing the VASA provider feature alone. If you have features like traditional/NVMe datastores, vVol replication, and if SRA is enabled on classic, it is not recommended to migrate the setup to ONTAP tools for VMware vSphere 10.0.

About this task

Migration is supported from ONTAP tools for VMware vSphere 9.10D2 and 9.11D4 releases to 10.0 release. To migrate from:
* ONTAP tools for VMware vSphere 9.10 release, first upgrade to 9.10D2 release then migrate to 10.0 release.
* ONTAP tools for VMware vSphere 9.11 release, first upgrade to 9.11D4 release then migrate to 10.0 release.

> (i) As an existing user you need to take the OVA backup from 9.10/9.11 before upgrading to 9.10D patch or 9.11D patch

Steps

1. Enable Derby PORT 1527 on the existing ONTAP tools for VMware vSphere 9.10D2 and 9.11D4. To enable the port, login to CLI with root user and run the following command:

   ```
   iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
   ```

2. Deploy OVA for ONTAP tools for VMware vSphere 10.0 release. See ONTAP tools Quick start

3. Add the vCenter that you want to migrate to ONTAP tools for VMware vSphere 10.0 release. See Add vCenter.

4. Onboard storage backend locally from the remote plugin vCenter APIs. See Onboard storage backend. Add storage as local scoped for migration.

5. Use the following API to migrate:

```
/api/v1/vcenters/{vcguid}/migration-jobs

{
  "otv_ip": "10.10.10.10",
  "vasa_provider_credentials": {
    "username": "Administrator",
    "password": "password"
  }
}
```

Above API call gives the jobid, which can be used for status check.

6. Use the following URI to check the status:

```
https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?
includeSubJobsAndTasks=true
```

7. Once the job is completed, validate the migration report. You can see the report from the job-response as part of the jobData.

8. Add ONTAP tools storage provider 10.0 to the vCenter and Register VASA Provider to vCenter.

9. Stop the ONTAP tools storage provider 9.10 /9.11 VASA Provider service (STOP VASA provider from maint console).

   NetApp recommends you not to delete the VASA provider.

   Once the old VASA provider is stopped, vCenter fails over to ONTAP tools for VMware vSphere 10.0. All the datastores and VMs become accessible and are served from ONTAP tools for VMware vSphere 10.0.

10. Perform the patch migrate using the following API:

```
/virtualization/api/v1/vcenters/{vcguid}/migration-jobs/{migration_id}
```

Request body is empty for patch operation.

> (i) uuid is the migration uuid returned in the response of post migrate API.

Once the patch migrate API is successful, all the VMs will be compliant with the storage policy.

The delete API for migration is:

```
Delete /virtualization/api/v1/vcenters/{vcguid}/migration-
jobs/{migration_id}
```

This API deletes migration by Migration Id and deletes migration on the given vCenter.

After successful migration and after you register ONTAP tools 10.0 to the vCenter, do the following:

- Refresh the certificate on all the hosts.
- Wait for sometime before performing Datastore (DS) and Virtual Machine (VM) operations. The waiting time depends on the number of hosts, DS, and VMs that are present in the setup. When you don't wait, the operations may fail intermittently.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

https://www.netapp.com/company/legal/copyright/

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

https://www.netapp.com/company/legal/trademarks/

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Notice for ONTAP tools for VMware vSphere 10.0