Deploy ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

Table of Contents

Deploy ONTAP tools for VMware vSphere

Quick start for ONTAP tools for VMware vSphere

Getting started with ONTAP tools for VMware vSphere includes a few steps. This quick start takes you through the initial setup of ONTAP tools for VMware vSphere.

Initially, you'll deploy ONTAP tools for VMware vSphere as a small-sized single node configuration that provides core services to support NFS and VMFS datastores. If you need to expand your configuration to use vVols datastore and high availability (HA), you'll do so after you finish this workflow. For more information, refer to the HA deployment workflow.

Plan your deployment

Verify that your vSphere, ONTAP, and ESXi host versions are compatible with the ONTAP tools version. Allocate sufficient CPU, memory, and disk space. Depending on your security policies, you may need to configure firewalls or other security appliances to allow network traffic.

Ensure the vCenter Server is installed and accessible.

- Interoperability Matrix Tool
- Prerequisites for ONTAP tools for VMware vSphere deployment
- Before you get started

Deploy ONTAP tools for VMware vSphere

Initially, you'll deploy ONTAP tools for VMware vSphere as a small-sized single node configuration that provides core services to support NFS and VMFS datastores. If you plan to expand your configuration to use vVols datastores and high availability (HA), you'll do so after you finish this workflow. To successfully expand to an HA configuration, you must ensure that the CPU hot hot-add and memory hot-plug options are enabled.

- Deploy ONTAP tools for VMware vSphere

Add vCenter Server instances

Add one or more vCenter Server instances to ONTAP tools for VMware vSphere to configure, manage, and protect your virtual datastores in your vCenter Server environment.

- Add vCenter Server instances

Configure ONTAP user roles and privileges

Configure new user roles and privileges for managing storage backends using the JSON file provided with ONTAP tools for VMware vSphere.

- Configure ONTAP user roles and privileges

5 **Configure the storage backends**

Add a storage backend to an ONTAP cluster. For multitenancy setups where vCenter acts as the tenant with an associated SVM, use ONTAP tools Manager to add the cluster. Associate the storage backend with the vCenter Server to map it globally to the onboarded vCenter Server instance.

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

- Add a storage backend
- Associate the storage backend with a vCenter Server instance

6 **Upgrade the certificates if you're working with multiple vCenter Server instances**

When working with multiple vCenter Server instances, upgrade the self-signed certificate to a certificate authority (CA) signed certificate.

- Manage certificates

7 **(Optional) Enable SRA protection**

Enable the SRA capability to configure disaster recovery and protect NFS or VMFS datastores.

- Configure SRA on the VMware Live Site Recovery appliance

8 **(Optional) Enable SnapMirror active sync protection**

Configure ONTAP tools for VMware vSphere to manage host cluster protection for SnapMirror active sync. Pair the source and destination clusters and SVM for SnapMirror active sync. This applies only to VMFS datastores.

- Protect using host cluster protection

9 **Set up backup and recovery for your ONTAP tools for VMware vSphere deployment**

Schedule backups of your ONTAP tools for VMware vSphere setup that you can use to recover the setup in case of a failure.

- Create backup and recover the ONTAP tools setup

High availability (HA) deployment workflow

If you are using vVols datastores, you need to expand the initial deployment of ONTAP tools to a high-availability (HA) configuration and enable the VASA Provider services.

1 **Scale up the deployment**

You can scale up the ONTAP tools for VMware vSphere configuration to increase the number of nodes in the deployment and change the configuration to an HA setup.

- Change ONTAP tools for VMware vSphere configuration

2 **Enable services**

To configure the vVols datastore you must enable the VASA Provider service. Register the VASA provider with vCenter and ensure your storage policies meet the HA requirements, including proper network and storage configurations.

Enable the SRA services to use ONTAP tools Storage Replication Adapter (SRA) for VMware Site Recovery Manager (SRM) or VMware Live Site Recovery (VLSR).

- Enable VASA Provider and SRA services

3 **Upgrade the certificates**

If you're using vVol datastores with multiple vCenter Server instances, upgrade the self-signed certificate to a certificate authority (CA) signed certificate.

- Manage certificates

Prerequisites for ONTAP tools for VMware vSphere deployment

Before deploying 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 ONTAP tools for VMware vSphere with VMware vCenter Server Virtual Appliance (vCSA). You should deploy ONTAP tools for VMware vSphere on a supported vSphere client that includes ESXi system.

System requirements

- **Installation package space requirements per node**
  - 15 GB for thin provisioned installations
  - 348 GB for thick provisioned installations
- **Host system sizing requirements** Recommended memory as per the size of deployment is as shown in the table below:

Type of deployment	CPUs	Memory (GB)	Disk space (GB) thick provisioned
Non-HA small	9	18	350
Non-HA medium	13	26	350
HA small (cumulative of three nodes)	27	54	1050

HA medium (cumulative of three nodes)	39	78	1050
HA large (cumulative of three nodes)	51	102	1050

Minimum storage and application requirements

Storage, host, and applications	Minimum version requirements
ONTAP	9.14.1, 9.15.1, and 9.16.0. FAS, ASA A-Series, ASA C-Series, AFF A-Series, AFF C-Series, and ASA r2.
ESXi hosts	ESXi 7.0.3
vCenter server	vCenter 7.0U3
VASA Provider	3.0
OVA Application	10.3

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

Configuration limits to deploy ONTAP tools for VMware vSphere

You can use the following table as a guide to configure ONTAP tools for VMware vSphere.

Deployment	Type	Number of vVols	Number of hosts
Non-HA	Small (S)	~12K	32
Non-HA	Medium (M)	~24K	64
High-Availability	Small (S)	~24K	64
High-Availability	Medium (M)	~50k	128
High-Availability	Large (L)	~100k	256 [NOTE] The number of hosts in the table shows the total number of host from multiple vCenters.

ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA)

The following table shows the numbers supported per VMware Live Site Recovery instance using ONTAP tools for VMware vSphere.

vCenter Deployment size	Small	Medium
Total number of virtual machines configured for protection using array-based replication	2000	5000
Total number of array-based replication protection groups	250	250
Total number of protection groups per recovery plan	50	50
Number of replicated datastores	255	255
Number of VMs	4000	7000

The following table shows the number of VMware Live Site Recovery and the corresponding ONTAP tools for VMware vSphere deployment size.

Number of VMware Live Site Recovery instances	ONTAP tools deployment Size
Upto 4	Small
4 to 8	Medium
More than 8	Large

For more information, refer to Operational Limits of VMware Live Site Recovery.

Port requirements

The following table outlines the network ports that NetApp uses and their purposes. Ensure these ports are open and accessible to facilitate proper operation and communication within the system. Ensure that the necessary network configurations are in place to allow traffic on these ports for the associated services to function correctly. Depending on your security policies, you may need to configure firewalls or other security appliances to permit this traffic within your network.

Port	Description
22(TCP)	Ansible uses this SSH port for communication during cluster provisioning. This port is required for functionalities like changing maintenance user password, status messages, and to update values on all the three nodes in case of HA configuration.
443(TCP)	This is the pass through port for incoming communication for the VASA Provider service. VASA Provider self-signed certificate and custom CA certificate are hosted on this port.
8443(TCP)	This port hosts the API documentation through swagger and the Manager user interface application.
2379(TCP)	This is the default port for client requests such as get, put, delete, or watch for keys in the etcd key value store.

2380(TCP)	This is the default port for server-to-server communication for the etcd cluster used for the raft consensus algorithm that etcd relies on for data replication and consistency.
7472(TCP+UDP)	This is the prometheus metrics service port.
7946(TCP+UDP)	This port is used for docker's container network discovery.
9083(TCP)	This port is an internally used service port for VASA Provider service.
1162(UDP)	This is the SNMP trap packets port.
6443(TCP)	Source: RKE2 agents nodes. Destination: REK2 server nodes. Description: Kubernetes API
9345(TCP)	Source: RKE2 agents nodes. Destination: REK2 server nodes. Description: REK2 supervisor API
8472(TCP+UDP)	All nodes need to be able to reach other nodes over UDP port 8472 when flannel VXLAN is used. Source: all RKE2 nodes. Destination: all REK2 nodes. Description: Canal CNI with VXLAN
10250(TCP)	Source: all RKE2 nodes. Destination: all REK2 nodes. Description: Kubelet metrics
30000-32767(TCP)	Source: all RKE2 nodes. Destination: all REK2 nodes. Description: NodePort port range
123(TCP)	Ntpd uses this port to perform validation of the ntp server.

Before you get started…

Ensure the following requirements are met before you proceed with the deployment:

Requirements	**Your status**
vSphere version, ONTAP version, and ESXi host version are compatible with the ONTP tools version.	□ Yes □ No
vCenter Server environment is set up and configured	□ Yes □ No
Browser cache is deleted	□ Yes □ No
You have the parent vCenter Server credentials	□ Yes □ No
You have the login credentials for the vCenter Server instance, to which the ONTAP tools for VMware vSphere will connect post-deployment for registration	□ Yes □ No
The domain name on which the certificate is issued is mapped to the virtual IP address in a multi-vCenter deployment where custom CA certificates are mandatory.	□ Yes □ No

Requirements	Your status
You have run the nslookup check on the domain name to check if the domain is getting resolved to the intended IP address.	□ Yes □ No
The certificate is created with the domain name and the ONTAP tools IP address.	□ Yes □ No
ONTAP tools application and internal services are reachable from the vCenter Server.	□ Yes □ No
When using multi-tenant SVMs, you have an SVM management LIF on each SVM.	□ Yes □ No

Deployment worksheet

For single node deployment

Use the following worksheet to gather the required information for ONTAP tools for VMware vSphere initial deployment: For ONTAP tools for VMware vSphere initial deployment:

Requirement	Your value
IP address for the ONTAP tools application. This is the IP address for accessing the ONTAP tools web interface	
ONTAP tools virtual IP address for internal communication. This IP address is used for internal communication in a setup with multiple ONTAP tools instances. This IP address should not be same as the IP address for the ONTAP tools application.	
DNS hostname for the first node	
Primary DNS server	
Secondary DNS server	
DNS search domain	
IPv4 address for the first node. It is a unique IPv4 address for the node management interface on the management network.	
Subnet mask for the IPv4 address	
Default gateway for the IPv4 address	
IPv6 address (optional)	
IPv6 prefix length (optional)	
Gateway for the IPv6 address (optional)	

Create DNS records for all the above IP addresses. Before assigning hostnames, map them to the free IP addresses on the DNS. All IP addresses should be on the same VLAN selected for deployment.

For High availability (HA) deployment

In addition to the single node deployment requirements, you'll need the following information for HA deployment:

Requirement	Your value
Primary DNS server	
Secondary DNS server	
DNS search domain	
DNS hostname for the second node	
IP address for the second node	
DNS hostname for the third node	
IP address for the third node	

Network firewall configuration

Open the required ports for the IP addresses in your network firewall. ONTAP tools must be able to reach this LIF over port 443. Refer to Port requirements for latest updates.

Deploy ONTAP tools for VMware vSphere

The ONTAP tools for VMware vSphere appliance is deployed as small-sized single node with core services to support NFS and VMFS datastores.

Before you begin

A 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 with a seamless experience as it is not dependent on the network connectivity.

You should store the content library on a shared datastore so that all hosts within a cluster can access it. Create a content library to store the OVA before configuring the appliance to HA configuration. Do not delete the content library template after deployment.

To enable HA deployment later, do not deploy the virtual machine hosting the ONTAP tools directly on an ESXi host. Deploy it on a cluster or resource pool instead.

If you don't have a content library, follow these steps to create one:

Create content library In you plan to use only a small single node deployment, creating a content library is not necessary.

1. Download the `.zip` file that contains binaries (*.ova*) and signed certificates for ONTAP tools for VMware vSphere from the NetApp Support Site.
2. Log in to the vSphere client
3. Select the vSphere client menu and select **Content libraries**.

4. Select **Create** on the right of the page.
5. Provide a name for the library and create the content library.
6. Navigate to the content library you created.
7. Select **Actions** in the right of the page and select **Import item** and import the OVA file.

For more information, refer to Creating and Using Content Library blog.

Before proceeding with the deployment, set the cluster's Distributed Resource Scheduler (DRS) on the inventory to 'Conservative'. This ensures that VMs are not migrated during the installation.

ONTAP tools for VMware vSphere is initially deployed as a non-HA setup. To scale to HA deployment, you will need to enable the CPU hot plug and memory hot plugin. You can perform this step as part of the deployment process or edit the VM settings after deployment.

Steps

1. Download the `.zip` file that contains binaries (*.ova*) and signed certificates for ONTAP tools for VMware vSphere from the NetApp Support Site. If you have imported the OVA into the content library, you can skip this step and proceed with the next step.
2. Log in to the vSphere server.
3. Navigate to the resource pool, cluster, or host where you intend to deploy the OVA.

Never store ONTAP tools for VMware vSphere virtual machine on vVols datastores that it manages.

4. You can deploy the OVA from the content library or from the local system.

From the local system	From the content library
a. Right-click and select **Deploy OVF template…**. b. Choose the OVA file from the URL or browse to its location, then select **Next**.	a. Go to your content library and select the library item that you want to deploy. b. Select **Actions** > **New VM from this template**

5. In the **Select a name and folder** field, enter the virtual machine name and choose its location.
   - If you're using the vCenter Server 8.0.3 version, Select the option **Customize this virtual machine's hardware**, which will activate an additional step called **Customize hardware** before proceeding to the **Ready to complete** window.
   - If you're using the vCenter Server 7.0.3 version, follow the steps in the **what's next?** section at the end of deployment.
6. Select a computer resource and select **Next**. Optionally, check the box to **Automatically power on deployed VM**.
7. Review the details of the template and select **Next**.
8. Read and accept the license agreement and select **Next**.
9. Select the storage for the configuration and the disk format and select **Next**.
10. Select the destination network for each source network and select **Next**.

11. In the **Customize template** window, fill in the required fields and select **Next**.
    - The information is validated during installation. If there is a discrepancy, an error message appears on the web console, and you are prompted to correct it.
    - Host names must include letters (A-Z, a-z), digits (0-9), and hyphens (-). To configure dual stack, specify the host name mapped to the IPv6 address.

      Pure IPv6 is not supported. Mixed mode is supported with VLAN containing both IPv6 and IPv4 addresses.

    - ONTAP tools IP address is the primary interface for communicating with ONTAP tools.
    - IPv4 is the IP address component of the node configuration, which can be utilized to enable diagnostic shell and SSH access on the node for the purposes of debugging and maintenance.
    - Node interconnect IP address is used for internal communication.
12. When using the vCenter Server 8.0.3 version, in the **Customize hardware** window, enable the **CPU hot add** and **Memory hot plug** options to allow HA functionality.
13. Review the details in the **Ready to complete** window, select **Finish**.

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

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

You can track the progress of the installation within the VM's web console.

If there are discrepancies in the OVF form, a dialog box will prompt corrective action. Use the tab button to navigate, make the necessary changes, and select "OK.You have three attempts to resolve any issues. If problems continue after three attempts, the installation process will stop, and it is advised to retry the installation on a new virtual machine.

What's next?

If you have deployment ONTAP tools for VMware vSphere with vCenter Server 7.0.3, then follow these steps after the deployment.

1. Log in to the vCenter client
2. Power down the ONTAP tools node.
3. Navigate to the ONTAP tools for VMware vSphere virtual machine under **Inventories** and select the **Edit settings** option.
4. Under the **CPU** options, check the **Enable CPU hot add** checkbox
5. Under the **Memory** options, check the **Enable** checkbox against **Memory hot plug**.

Deployment error codes

You might encounter error codes during ONTAP tools for VMware vSphere deployment, reboot, and recovery operations. The error codes are five digits long, where the first two digits represent the script that encountered the issue, and the last three digits represent the specific workflow within that script.

All error logs are recorded in the ansible-perl-errors.log file to facilitate easy tracking and resolution of issues. This log file contains the error code and the failed Ansible task.

The error codes provided on this page are for reference only. Contact the support team if error persists or if there's no resolution mentioned.

The following table lists the error codes and the corresponding file names.

Error code	Script name
00	firstboot-network-config.pl, mode deploy
01	firstboot-network-config.pl, mode upgrade
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, deploy, HA
04	firstboot-deploy-otv-ng.pl, deploy, non-HA
05	firstboot-deploy-otv-ng.pl, reboot
06	firstboot-deploy-otv-ng.pl, upgrade, HA
07	firstboot-deploy-otv-ng.pl, upgrade, non-HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

The last three digits of the error code indicate the specific workflow error within the script:

Deployment error code	Workflow	Resolution
050	Ssh Key generation failed	Restart the primary virtual machine (VM).
053	Failed installing RKE2	Either run the following and restart the primary VM or redeploy: sudo rke2-killall.sh (all VMs) sudo rke2-uninstall.sh (all VMs).
054	Failed setting kubeconfig	Redeploy
055	Failed deploying registry	If the registry pod is present, wait for the pod to be ready then restart the primary VM or else redeploy.
059	KubeVip deployment has failed	Ensure virtual IP address for Kubernetes control plane and load balancer IP address provided during deployment belong to same VLAN and are free IP addresses. Restart if all the previous points are correct. Else, redeploy.
060	Operator deployment has failed	Restart

061	Services deployment has failed	Perform basic Kubernetes debugging like get pods, get rs, get svc, and so on in ntv-system namespace for more details and error logs at /var/log/ansible-perl-errors.log and /var/log/ansible-run.log and redeploy.
062	ONTAP tools Services deployment has failed	Refer to the error logs at /var/log/ansible-perl-errors.log for more details and redeploy.
065	Swagger page URL is not reachable	Redeploy
066	Post deployment steps for gateway certificate has failed	Do the following to recover/complete the upgrade: * Enable diagnostic shell. * Run 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy' command. * Check the logs at /var/log/post-deploy-upgrade.log.
088	Configuring log rotate for journald has failed	Check the VM network settings that is compatible with the host on which the VM is hosted. You can try to migrate to another host and restart the VM.
089	Changing ownership of summary log rotate config file has failed	Restart the primary VM.
096	Install dynamic storage provisioner	-
108	Seeding script failed	-

Reboot error code	**Workflow**	**Resolution**
067	Waiting for rke2-server timed out.	-
101	Failed to Reset Maint/Console user password.	-
102	Failed to Delete password file during reset Maint/Console user password.	-
103	Failed to Update New Maint/Console user password in vault.	-
088	Configuring log rotate for journald has failed.	Check the VM network settings that is compatible with the host on which the VM is hosted. You can try to migrate to another host and restart the VM.
089	Changing ownership of summary log rotate config file has failed.	Restart the VM.

Copyright information

Trademark information