Deploy ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

Table of Contents

Deploy ONTAP tools for VMware vSphere

Quick start for ONTAP tools for VMware vSphere

Set up ONTAP tools for VMware vSphere with this quick start section.

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. To expand your configuration for additional containers per service, enhanced resiliency, or to use vVols datastores and high availability (HA), complete this workflow first and then proceed with the expansion steps. For more information, refer to the HA deployment workflow.

1 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. Based on your security rules, you might need to set up firewalls or other security tools to allow network traffic.

Ensure the vCenter Server is installed and accessible.

- Interoperability Matrix Tool
- ONTAP tools for VMware vSphere requirements and configuration limits
- Before you get started

2 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 expand to an HA setup, make sure CPU hot-add and memory hot-plug are enabled.

- Deploy ONTAP tools for VMware vSphere

3 Add vCenter Server instances

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

- Add vCenter Server instances

4 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) Configure SRA protection**

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

- Enable ONTAP tools for VMware vSphere services
- 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. Perform the ONTAP cluster and SVM peering in ONTAP systems to use 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**

Backup is enabled by default in ONTAP tools for VMware vSphere 10.5 and occurs every 10 minutes. Schedule backups of your ONTAP tools for VMware vSphere setup that you can use to recover the setup in case of a failure.

- Edit the backup settings
- Recover the ONTAP tools setup

High availability deployment workflow for ONTAP tools

To increase resiliency and support more containers per service, expand your initial

ONTAP tools deployment to a high-availability (HA) configuration. Enabling the VASA Provider service is required for vVols datastores in an HA setup.

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 vVols datastores 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

ONTAP tools for VMware vSphere requirements and configuration limits

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 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** The table below shows the recommended memory for each deployment size. For high availability (HA) deployments, you need three times the appliance size listed.

Type of deployment	CPUs per node	Memory (GB) per node	Disk space (GB) thick provisioned per node

Small	9	18	350
Medium	13	26	350
Large NOTE: The large deployment is only for HA configuration.	17	34	350

When backup is enabled, each ONTAP tools cluster needs another 50 GB of space on the datastore where VMs are deployed. Therefore, non-HA requires 400 GB, and HA requires 1100 GB of space in total.

Minimum storage and application requirements

Storage, host, and applications	Version requirements
ONTAP	9.15.1, 9.16.1, and 9.17.0
ONTAP tools supported ESXi hosts	7.0.3 onwards
ONTAP tools supported vCenter Server	7.0U3 onwards
VASA Provider	3.0
OVA Application	10.5
ESXi host to deploy ONTAP tools virtual machine	7.0U3 and 8.0U3
vCenter Server to deploy ONTAP tools virtual machine	7.0 and 8.0

Beginning with ONTAP tools for VMware vSphere 10.4, the virtual machine hardware is changed from version 10 to 17.

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

Port requirements

The following table outlines the network ports that NetApp uses and their purposes. There are three different types of ports:

- External ports: These ports are accessible from outside the Kubernetes cluster or node. They allow services to communicate with external networks or users, enabling integration with systems outside the cluster environment.
- Inter-node ports: These ports enable communication between nodes within the Kubernetes cluster. They are needed for cluster tasks like sharing data and working together. For single-node deployments, inter-node ports are used only within the node and do not need external access. Inter-node ports can accept traffic from outside the cluster. Block inter-node ports from internet access with firewall rules.
- Internal ports: These ports communicate within the Kubernetes cluster using ClusterIP addresses. They are not exposed externally and do not need to be added to firewall rules.

Ensure that all ONTAP tools nodes reside on the same subnet to maintain uninterrupted communication with each other.

Click to expand or collapse the port requirements table.

Service/Component name	Port	Protocol	Port Type	Description
ntv-gateway-svc (LB)	443, 8443	TCP	External	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.
SSH	22	TCP	External	Secure Shell for remote server login and command execution.
rke2 server	9345	TCP	Inter-node	RKE2 supervisor API (Restrict to trusted networks).
kube-apiserver	6443	TCP	Inter-node	Kubernetes API server port (Restrict to trusted networks).
rpcbind/portmapper	111	TCP/UDP	Inter-node	Used for RPC communication between services.
coredns (DNS)	53	TCP/UDP	Inter-node	Domain Name System (DNS) service for name resolution within the cluster.
NTP	123	UDP	Inter-node	Network Time Protocol (NTP) for time synchronization.
etcd	2379, 2380, 2381	TCP	Inter-node	Key-value store for cluster data.
kube-vip	2112	TCP	Inter-node	Kubernetes API server port.
kubelet	10248, 10250	TCP	Inter-node	Kubernetes component
kube-controller	10257	TCP	Inter-node	Kubernetes component
cloud-controller	10258	TCP	Inter-node	Kubernetes component

Service/Component name	Port	Protocol	Port Type	Description
kube-scheduler	10259	TCP	Inter-node	Kubernetes component
kube-proxy	10249, 10256	TCP	Inter-node	Kubernetes component
calico-node	9091, 9099	TCP	Inter-node	Calico networking component.
containerd	10010	TCP	Inter-node	Container daemon service.
VXLAN (Flannel)	8472	UDP	Inter-node	Overlay network for pod communication.

For HA deployments, ensure UDP port 8472 is open between all nodes. This port enables pod-to-pod communication across nodes; blocking it will interrupt inter-node networking.

Configuration limits to deploy ONTAP tools for VMware vSphere for vVols datastores

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

Deployment	Type	Number of vVols	Number of hosts
Non-HA	Small (S)	up to 12K	32
Non-HA	Medium (M)	up to 24K	64
High-Availability	Small (S)	up to 24K	64
High-Availability	Medium (M)	up to 50k	128
High-Availability	Large (L)	up to 100k	256

The host counts in the table represent the combined total across all connected vCenters.

Configuration limits to deploy ONTAP tools for VMware vSphere for VMFS and NFS datastores

The configuration limits listed in this section are validated and supported by NetApp. Actual limits may vary depending on your environment and workload. Exceeding these limits may impact performance or supportability and is not recommended. Consider the following when reviewing the table:

- Virtual machine Disaster Recovery (DR) is configured using synchronous, asynchronous, or strict sync policies. DR is not supported for the NVMe protocol.
- ESXi host cluster protection uses SnapMirror Active Sync, which does not support multi-vCenter deployments.
- ONTAP tools restricts only the number of ESXi hosts and datastores based on deployment size. There are no restrictions on the number of vCenter Servers that can be connected to ONTAP tools.

- ONTAP tools performs parallel discovery of all storage objects. Configuration limits for ONTAP storage objects apply regardless of the number of objects actively in use.
- ONTAP tools does not impose a limit on the number of vCenter Servers that can be onboarded. Configuration limits are determined by the number of supported hosts and datastores, as detailed in the following table.

Deployment	Number of VMFS and NFS datastores	Number of DR enabled VMFS datastores	Number of hosts
Non-HA Small	200	80	32
Non-HA Medium	250	100	32
HA Small	350	200	64
HA Medium	600	200	128
HA Large	1024	250	256

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.

Pre-deployment requirements for ONTAP tools

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
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:

Requirement	Your value
IP address for the ONTAP tools application. This is the IP address for accessing the ONTAP tools web interface (load balancer)	
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.(The Kubernetes Control Plane)	
DNS hostname for the ONTAP tools management node	
Primary DNS server	
Secondary DNS server	

Requirement	Your value
DNS search domain	
IPv4 address for the ONTAP tools management 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

Ensure that the necessary firewall ports are open for all relevant IP addresses. ONTAP tools require access to the LIF via port 443. For a complete list of required ports, see the port requirements section at ONTAP tools for VMware vSphere requirements and configuration limits.

ONTAP storage settings

To ensure seamless integration of ONTAP storage with ONTAP tools for VMware vSphere, consider the following settings:

- If you're using the Fibre Channel (FC) for storage connectivity, configure the zoning on your FC switches to connect the ESXi hosts with the SVM's FC LIFs. Learn about FC and FCoE zoning with ONTAP systems
- To use ONTAP tools-managed SnapMirror replication, the ONTAP storage administrator should create ONTAP cluster peer relationships and ONTAP intercluster SVM peer relationships in ONTAP before using

SnapMirror.

Deploy ONTAP tools

The ONTAP tools for VMware vSphere appliance is deployed as a small-sized single node with core services to support NFS and VMFS datastores. The ONTAP tools deployment process might take up to 45 minutes.

Before you begin

If you're deploying a small single node, a content library is optional. For multi-node or HA deployments, a content library is required. In VMware, a content library stores VM templates, vApp templates, and other files. Deploying with a content library provides a seamless experience because it is not dependent on network connectivity.

Consider the following before creating a content library:

- Create the content library on a shared datastore so all hosts in the cluster can access it.
- Set up the content library before deploying the ONTAP tools for VMware vSphere OVA.
- Ensure the content library is created before configuring the appliance for HA.

Don't delete the OVA template in the content library after deployment.

To enable HA deployment in the future, avoid deploying the ONTAP tools virtual machine directly on an ESXi host. Instead, deploy it within a ESXi host cluster or resource pool.

Follow these steps to create a content library:

1. Download the file that contains the 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. Go 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 aren't migrated during the installation.

The 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 plug-in. You can perform this step as part of the deployment process or edit the VM settings after deployment.

Steps

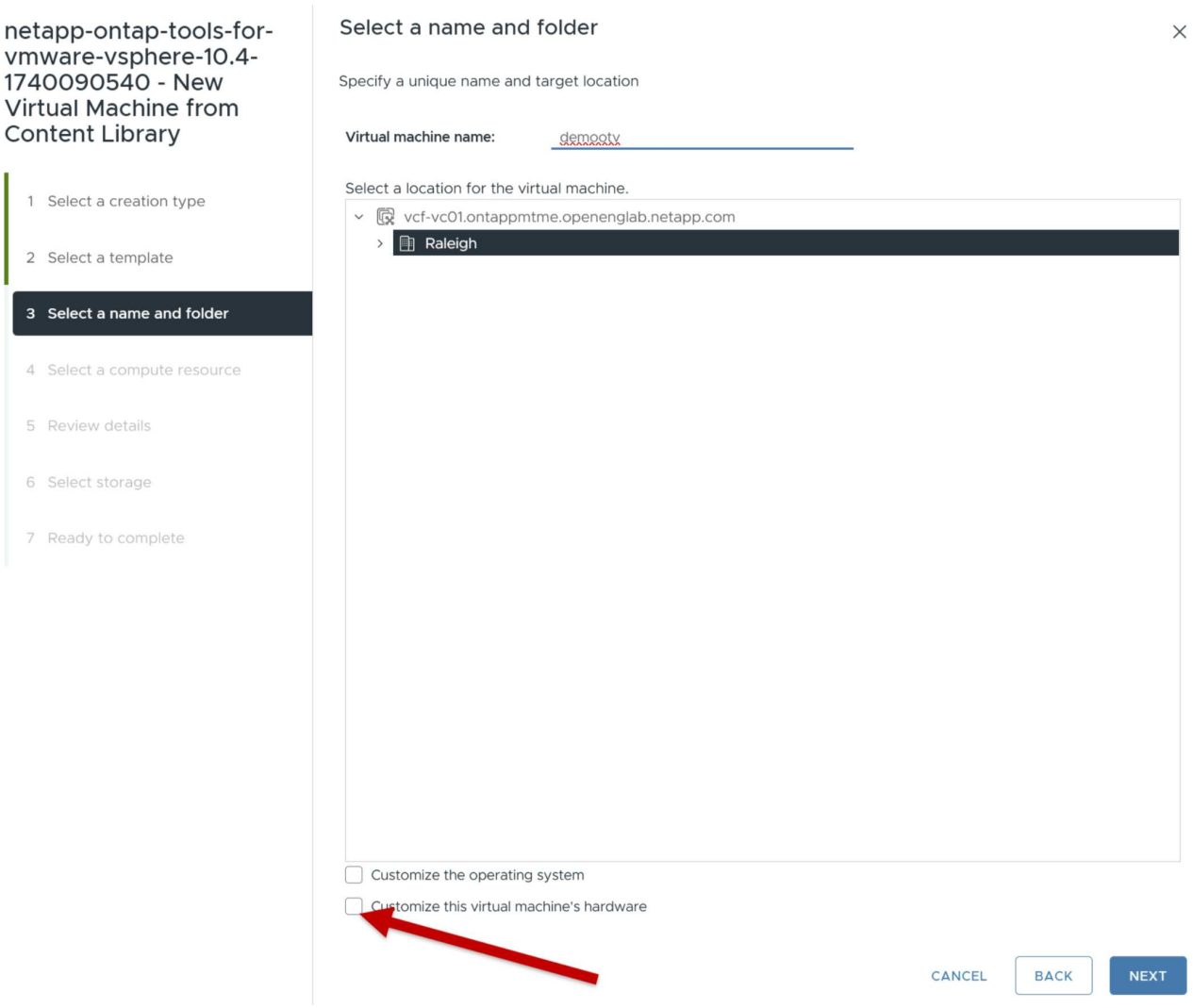
1. Download the file that contains the binaries (*.ova*) and signed certificates for the ONTAP tools for VMware vSphere from the NetApp Support Site. If you have imported the OVA into the content library, you can skip this step and proceed with the next step.
2. Log in to the vSphere server.
3. Go to 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.

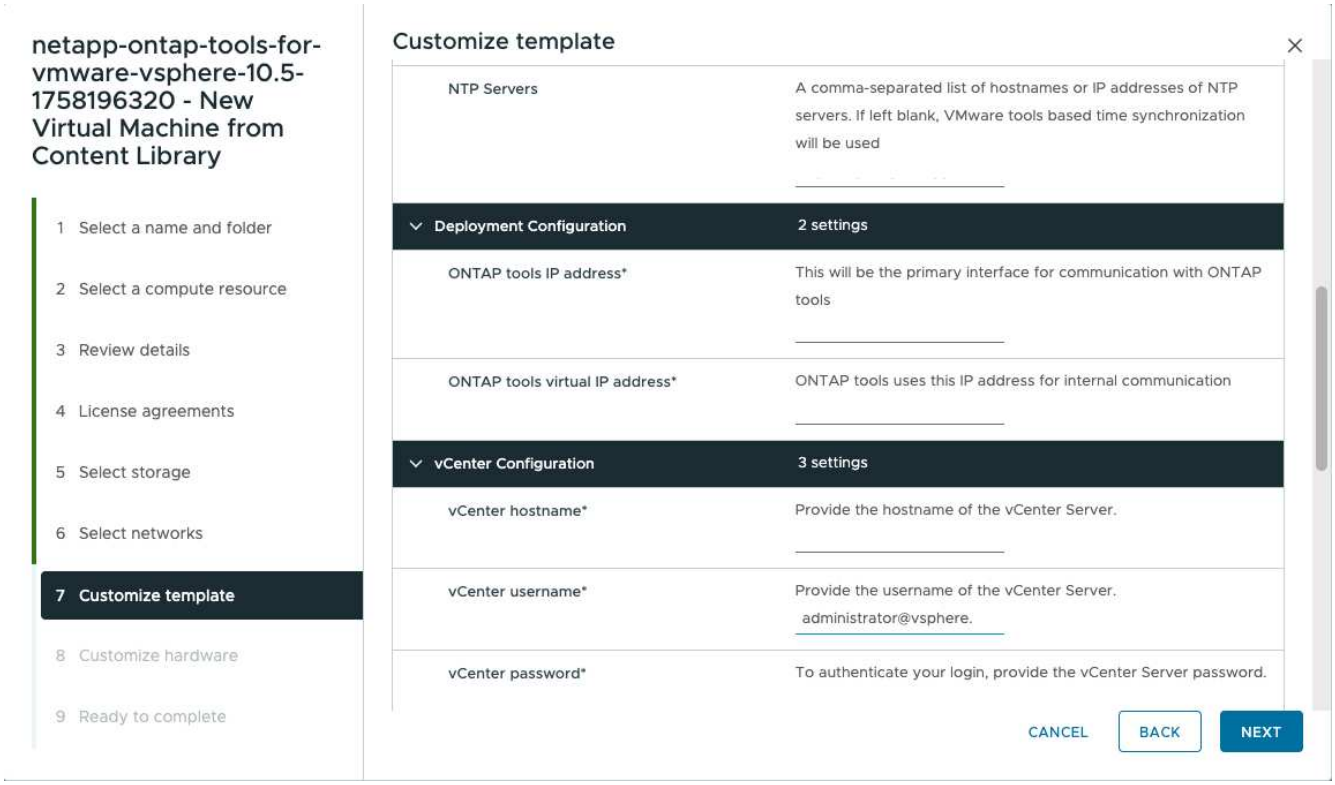
4. You can deploy the OVA from the content library or from the local system.

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.



The vCenter hostname is the name of the vCenter Server instance where the ONTAP tools appliance is deployed.

If you are deploying ONTAP tools in a two-vCenter Server topology—where the appliance is hosted in one vCenter instance and manages another, you can assign a restricted role for the vCenter instance hosting the ONTAP tools. You can create a dedicated vCenter user and role with only the permissions required for OVF template deployment. For details, see the roles listed in Roles included with ONTAP tools for VMware vSphere 10.

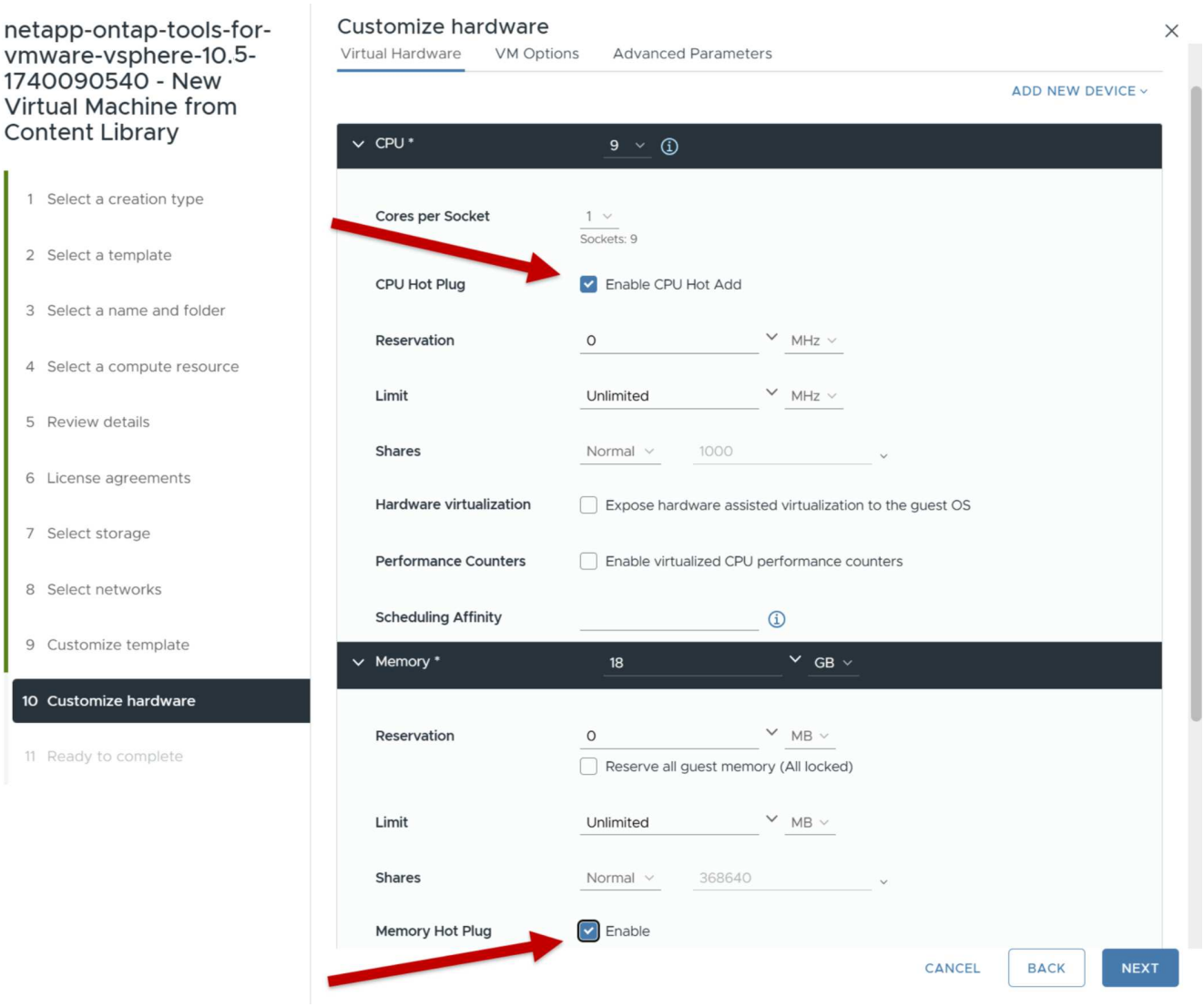
For the vCenter instance that will be managed by ONTAP tools, make sure the vCenter user account has administrator privileges.

- 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.

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 completing the task if the option to automatically power on the VM was not selected.

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. Go 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**.

Troubleshoot ONTAP tools deployment errors

If you experience deployment issues, review the logs and error codes to diagnose and resolve problems. Starting with ONTAP tools for VMware vSphere 10.5, log bundles collected from the pods include logs from MongoDB, RabbitMQ, and Vault, along with the status and descriptions of all pods. These are provided in addition to the existing ONTAP tools service logs, enhancing supportability and troubleshooting.

Collect the log files

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

> Generating logs from the ONTAP tools Manager includes all logs for all vCenter Server instances. Generating logs from the vCenter client user interface are scoped for the selected vCenter Server.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Log Bundles** from the sidebar.

   This operation can take several minutes.
4. Select **Generate** to generate the log files.
5. Enter the label for the Log Bundle and select **Generate**.

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

Follow the steps below to generate log bundle using the vCenter client user interface:

Steps

1. Log in to the vSphere client.
2. From the vSphere Client home page, go to **Support** > **Log bundle** > **Generate**.
3. Provide the log bundle label and generate the log bundle. You can see the download option when the files are generated. Downloading might take some time.

> The log bundle generated replaces the log bundle that was generated within the last 3 days or 72 hrs.

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 under the /var/log directory 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
049	For network and validation perl script will assign them as well shortly	-
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 ONTAP tools 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