Deploy ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10.1

NetApp
June 21, 2024

Table of Contents

Deploy ONTAP tools for VMware vSphere

Prerequisites for deploying ONTAP tools for VMware vSphere

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.

- **Installation package space requirements per node**
  - 10 GB for thin provisioned installations
  - 248 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	Minimum version requirements
ONTAP	Latest patch release of ONTAP 9.12.1, 9.13.1, or 9.14.1
ESXi hosts	ESXi 7.0.3
vCenter server	vCenter 7.0U3
VASA provider	3.0
OVA Application	10.1

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 should consider a few requirements while customizing the deployment of 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.

Appliance maintenance console credentials

You should access the maintenance console by using the “maint” username. You can set the password for the “maint” user during deployment. You can use the Restart guest OS option available during VM restart in vCenter Server to change the password.

Appliance network properties

Specify a valid DNS hostname (unqualified) as well as the static IP address for ONTAP tools for VMware vSphere and the other network parameters. The IP addresses provided should be accessible from the VLAN network that you select during the deployment. DHCP is not supported for ONTAP tools for VMware vSphere 10.1 release. All these parameters are required for proper installation and operation.

Download ONTAP tools for VMware vSphere

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

When the deployment is complete, ONTAP tools for VMware vSphere and VASA products are installed in your environment. By default, ONTAP tools for VMware vSphere starts working as soon as you decide on the subsequent deployment model and choose whether to enable VASA Provider based on your requirements. See Register the VASA Provider with a vCenter Server instance for details.

Content library

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, such that all hosts in a cluster can access it. You need to create a content library to store the OVA before deploying the OVA in HA configuration. Create the content library using the following steps:

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. Select the horizontal ellipses next to vSphere client and select **Content library**.
3. Select **Create** on the right side of the page.
4. Provide a name for the library and create the content library.
5. Navigate to the content library you created.
6. Select **Actions** in the right side of the page and select **Import item** and import the OVA file.

Prepare to deploy ONTAP tools for VMware vSphere

You should be aware of the basic storage backend requirements, application requirements, and license requirements before you begin deploying ONTAP tools for VMware vSphere. Plan your deployment in advance and decide how you want to configure ONTAP tools for VMware vSphere in your environment.

Preparing for deployment

Following are ONTAP tools for VMware vSphere requirements before proceeding with the deployment:

1. Configure and set up your vCenter Server environment.
2. Download the *.ova* file.
3. (Optional) Used for automation user - Gather the Postman collections JSON file provided by NetApp.
4. Parent vCenter Server Credentials to deploy the OVA. Parent vCenter Server password should not contain these special characters($, ', ")
5. Make sure the host or the resource pool where the OVA is deployed has the minimum resources mentioned in the Prerequisites for deploying ONTAP tools for VMware vSphere section.
6. The login credentials for your vCenter Server instance to which the ONTAP tools for VMware vSphere will connect to post deployment for registration.
7. Delete the browser cache.
8. For non-HA deployment, you need three free IP addresses - one free IP address for load balancer and one free IP address for the Kubernetes control plane and one IP address for node. For HA deployment, along with these three IP addresses you'll need two more IP addresses for second and third nodes. Host names should be mapped to the free IP addresses on the DNS before assigning. All the five IP addresses should be on the same VLAN that is selected for deployment.
9. Content library template once uploaded should not be deleted post deployment as it will be used during reboots.
10. In a multi-vCenter deployment where Custom CA certificates are mandatory, map the Domain Name on which the certificate is issued to the Virtual IP address. Perform a *nslookup* check on the domain name to check whether the domain is getting resolved to the intended IP address. The certificates should be created with domain name and IP address of the load balancer IP address.
11. IPv4/IPv6 supported VLAN - Pure IPV6 is not supported. Mixed mode is supported with VLAN having both IPv6 and IPv4 addresses.
12. NTP Server which is provided to the vCenter Server for time Sync.
13. Static IP address Configuration details for the Node or VM where the OVA is being deployed (Mandatory) and other details.
    a. vCenter Server hostname (vCenter where the OVA is deployed)
    b. vCenter Server username (vCenter where the OVA is deployed)
    c. vCenter Server password (vCenter where the OVA is deployed)
    d. Resource pool
    e. Data LIF (IPv4/IPv6)
    f. Management LIF
    g. ONTAP username

h. ONTAP password
i. SVM name
j. Protocol
k. Virtual IP addresses for the Kubernetes control plane.
l. HA / NON-HA drop down
m. List of hostnames
n. IP addresses (string)
o. Content library name
p. OVF template name
q. IPv6 gateway (optional)

Deploy non-HA single-node configuration

You can deploy a non-HA single-node configuration in either a small or medium configuration.

- The small non-HA configuration contains 8 CPUs and 16 GB RAM.
- Medium non-HA configuration contains 12 CPUs and 24 GB RAM.

Before you begin

Make sure the network route is present. Storage data network needs to be accessible from VM management network. Example: C1_sti67-vsim-ucs154k_1679633108::> network route create -vserver <SVM> -destination 0.0.0.0/0 -gateway <gateway_ip>

Steps

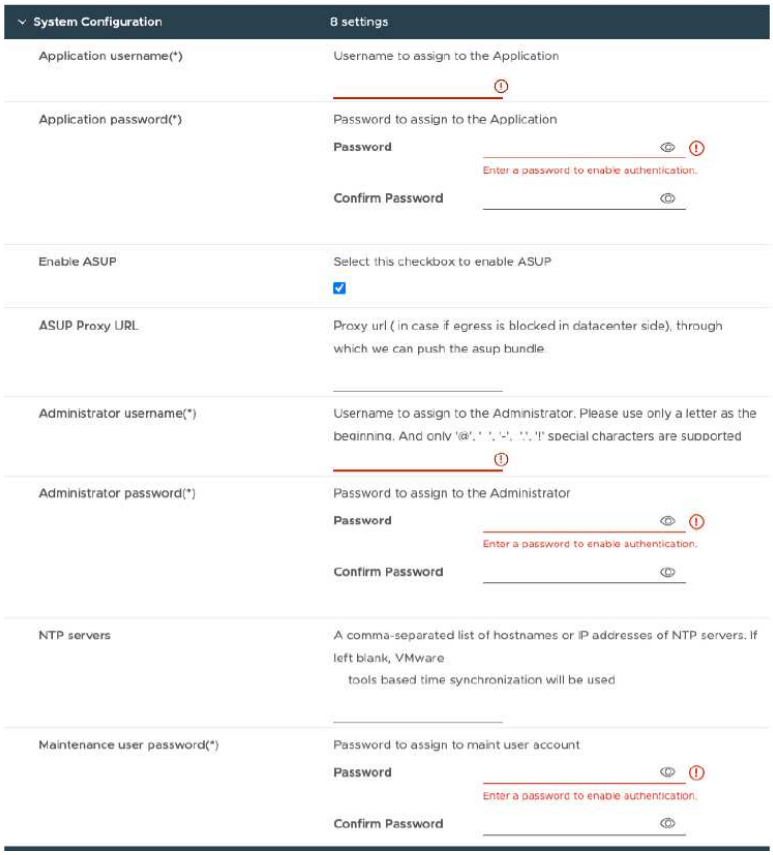
1. Log in to the vSphere server.
2. Navigate to the resource pool or the cluster or the host where you want to deploy the OVA.
3. Right-click the required location and select **Deploy OVF template…**.

   Do not deploy ONTAP tools VMware vSphere virtual machine on a vVols datastore that it manages.

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 **Easy deployment(S)**, **Easy deployment(M)**, or **Advanced deployment(S)** or **Advanced deployment(M)** configuration.

   The advanced deployment option uses Trident as a dynamic storage provisioner for ONTAP to create volumes and the easy deployment uses local storage to create volumes.

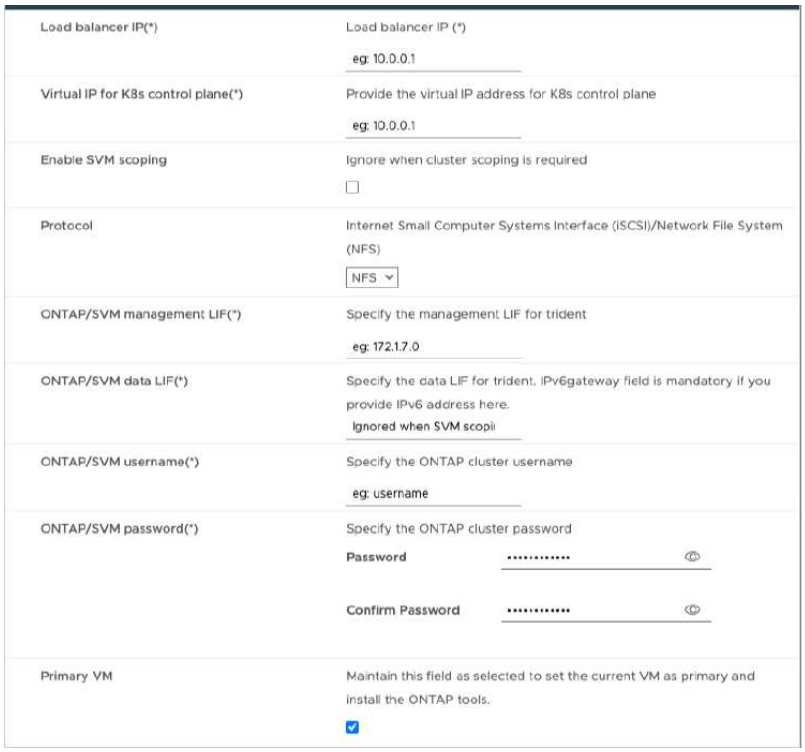
10. Select the datastore where you need to deploy the OVA and select **Next**.
11. Select the source and destination network and select **Next**.
12. Select **Customize template** > **system configuration** window.



Enter the following details: .. Application username and password: This username and password is used for registering both VASA provider and SRA in the vCenter Server. .. The **Enable ASUP** checkbox is selected by default.

AutoSupport can be enabled or disabled only during deployment. .. In the **ASUP Proxy URL** field, provide this URL to avoid firewall blockage for AutoSupport data transmission. .. Administrator Username and Administrator Password: This is the password used to log in to ONTAP Tools Manager. .. Enter your NTP server information in the **NTP Servers** field. .. Maintenance user password: This is used to grant access to 'Maint Console Options'. . In **Customize template** > **Deployment Configuration** window, enter the following details:

+



a. Enter an available IP address in the Virtual IP address for the Kubernetes control plane. You need this for the Kubernetes API Server.

b. Select **Enable SVM scoping** option when you intend to use the directly added SVM user account. To use ONTAP cluster, do not select the checkbox.

> When SVM scope is enabled, you should have already enabled SVM support with management IP address.

c. Select either NFS or iSCSI in the **Protocol** field.

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

e. Enter the ONTAP Cluster or the SVM ONTAP/SVM Data LIF. The data LIF should belong to the protocol selected. For example, if iSCSI protocol selected, then an iSCSI data LIF should be provided.

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

g. Enter the ONTAP/SVM Username. ONTAP/SVM username and Password is required for Trident to create volumes for storing the data of services in case of advanced or HA deployment and to recover the data from volumes during node failure.

h. Enter the ONTAP/SVM Password. The ONTAP/SVM login password for this storage VM should not contain these special characters($,',").

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

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

> 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.

j. Enter the Host name. Host names that consist of uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), and the hyphen (-) special character only are supported. If you want to configure dual stack, specify the host name mapped to IPv6 address.

k. Enter IP address (IPV4) mapped to the host name. In case of dual stack, provide any available IPv4 IP address that is in the same VLAN as the IPv6 address.

l. Enter the IPV6 Address on the deployed network only when you need dual stalk.

m. Specify the prefix length only for IPV6.

n. Specify the subnet to use on the deployed network in Netmask (only for IPV4) field.

o. Specify the Gateway on the deployed network.

p. Specify the Primary DNS server IP address.

q. Specify the Secondary DNS server IP address.

r. Specify the Search Domain name to use when resolving the hostname.

s. Specify the IPV6 gateway on the deployed network only when you need dual stack.

1. 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.

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

   The installation begins. You can track 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.

3. Make necessary changes in the dialog prompt. Use tab button to navigate across the panel to enter your values, **OK** or **Cancel**.
4. On selecting **OK**, the values provided would again be validated. You have the provision to correct any values up to three 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.
5. After successful installation, the web console shows the state of ONTAP tools for VMware vSphere.

Deploy HA configuration

You can configure HA three nodes in either small, medium, or large configurations. HA deployment uses Trident to store the services data.

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

Before you begin

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

Creating the content library is a mandatory step for deploying HA three nodes configuration. See Download ONTAP tools for details. Learn more Creating and Using Content Library.

Make sure you have imported your OVA into your content library. Keep the name of the content library and the library item name that you have given to your OVA item handy.

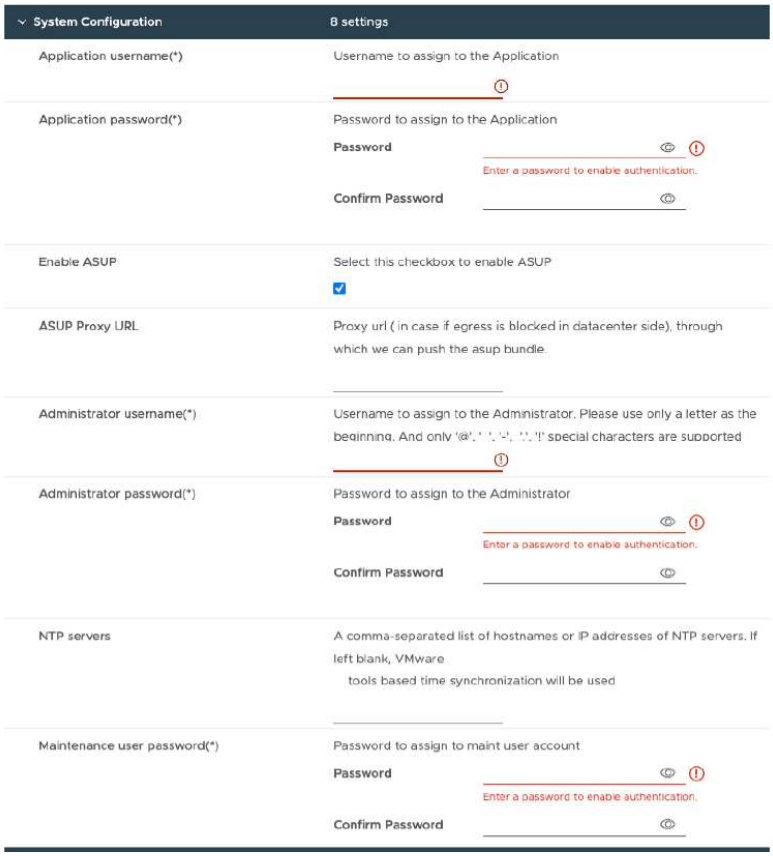
> Before proceeding with the deployment, set the cluster's Distributed Resource Scheduler (DRS) on the inventory to 'Conservative' during the installation of ONTAP tools. This ensures that VM's do not migrate during the installation.

Steps

1. To deploy from vSphere server:
   a. Log in to the vSphere server.
   b. Navigate to the resource pool or the host where you want to deploy the OVA and right-click the required location where you want to deploy the VM, and select **Deploy OVF template…**

      > Do not deploy ONTAP tools VMware vSphere virtual machine on a vVols datastore that it manages.

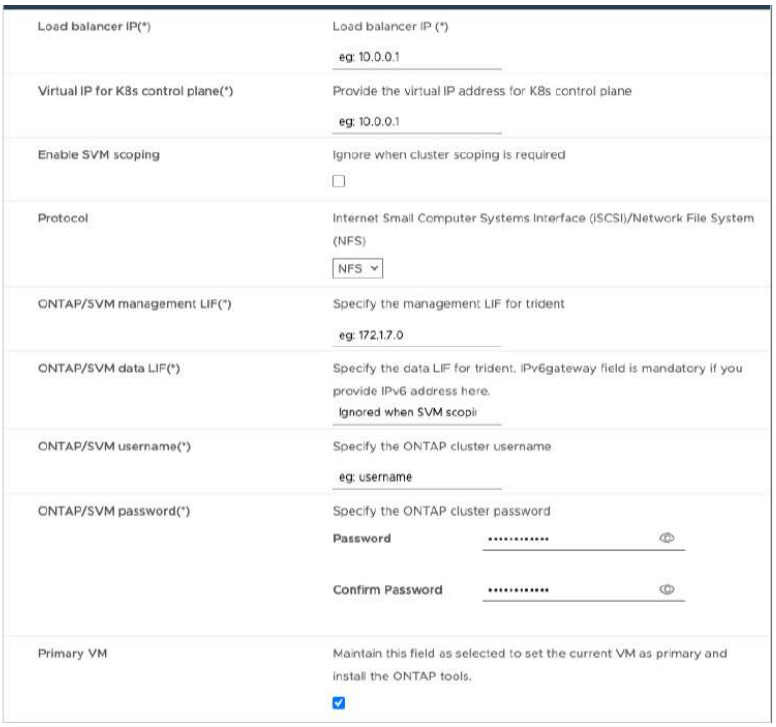
   c. You can either enter the URL for the *.ova* file or browse to the folder where the *.ova* file is saved, and then select **Next**
2. To deploy from content library:
   a. Go to your content library and click on the library item that you want to deploy.
   b. Click on **Actions** > **New VM from This Template**
3. Select a name and folder for the virtual machine and select **Next**.
4. Select the host and select **Next**
5. Review the summary of the template and select **Next**.
6. Read and accept the license agreement and select **Next**.
7. In the **Configuration window**, select **High-Availability Deployment(S)**, **High-Availability Deployment(M)**, or **High-Availability Deployment(L)** configuration, depending on your requirement.
8. Select the storage for the configuration and disk files, select **Next**.
9. Select the destination network for each source network, select **Next**.
10. Select **Customize template** > **system configuration** window.



Enter the following details:

a. Application username and password: This username and password is used for registering both VASA provider and SRA in the vCenter Server.
b. The **Enable AutoSupport** checkbox is selected by default. AutoSupport can be enabled or disabled only during deployment.
c. In the **ASUP Proxy URL** field, provide this URL to avoid firewall blockage for AutoSupport data transmission.
d. Administrator Username and Administrator Password: This is the password used to log in to ONTAP tools Manager.
e. Enter your NTP server information in the **NTP Servers** field.
f. Maintenance user password: This is used to grant access to ‘Maint Console Options’.

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



a. Enter an available IP address in the Virtual IP address for the Kubernetes control plane. You need this for the Kubernetes API Server.

b. In the advanced deployment option, select **Enable SVM scoping** option when you intend to use the directly added SVM user account. To use ONTAP cluster, do not select the checkbox.

> When SVM scope is enabled you should have already enabled SVM support with management IP address.

c. Select either NFS or iSCSI in the **Protocol** field.

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

e. Enter the ONTAP Cluster or the SVM ONTAP/SVM Data LIF. The data LIF should belong to the protocol selected. For example, if iSCSI protocol selected, then an iSCSI data LIF should be provided.

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

g. Enter the ONTAP/SVM Username. ONTAP/SVM username and Password is required for Trident to create volumes for storing the data of services in case of advanced or HA deployment and to recover the data from volumes during node failure.

h. Enter the ONTAP/SVM Password. The ONTAP/SVM login password for this storage VM should not contain these special characters($,',").

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

12. In **Customize template** > **Content Library Details** window, enter the **Content Library Name** and the **OVF Template Name**.
13. In **Customize template** > **vCenter Configuration** window, provide the details of the vCenter Server where the content library is hosted.
14. 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 the 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. Host names that consist of uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), and the hyphen (-) special character only are supported. If you want to configure dual stack, specify the host name mapped to IPv6 address.
b. Enter IP address (IPV4) mapped to the host name. In case of dual stack, provide any available IPv4 IP address that is in the same VLAN as the IPv6 address.
c. Enter the IPV6 Address on the deployed network only when you need dual stack.
d. Specify the prefix length only for IPV6.
e. Specify the subnet to use on the deployed network in Netmask (only for IPV4) field.
f. Specify the Gateway on the deployed network.
g. Specify the Primary DNS server IP address.
h. Specify the Secondary DNS server IP address.
i. Specify the Search Domain name to use when resolving the hostname.
j. Specify the IPV6 gateway on the deployed network only when you need dual stack.

15. In **Customize template** > **Node 2 Configuration** and **Node 3 Configuration** window, enter the following details:
    a. Host name 2 and 3 - Host names that consist of uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), and the hyphen (-) special character only are supported. If you want to configure dual stack, specify the host name mapped to IPv6 address.
    b. IP address
    c. IPV6 address
16. 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.
17. Power on the VM after the completion of the task.

    The installation begins. You can track 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 the case of any discrepancies, a dialog prompts you to take corrective action.
18. Make necessary changes in the dialog prompt. Use tab button to navigate across the panel to enter your values, **OK** or **Cancel**.
19. On selecting **OK**, the values provided would again be validated. You have the provision to correct any values up to 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.
20. After successful installation, the web console shows the state of ONTAP tools for VMware vSphere.

Recover your ONTAP tools for VMware vSphere setup

If you lose your ONTAP tools for VMware vSphere setup, you can recover the ONTAP tools for VMware vSphere setup using the data available in the ONTAP volume data. When you lose the setup, bring down the setup gracefully. You can recover both the single-node deployment and the HA three nodes deployment configurations.

> You cannot recover your ONTAP tools for VMware vSphere setup if there are issues with vCenter Server or ONTAP data management software.

Steps

1. Log in to the vSphere server.
2. Navigate to the resource pool or the node cluster or the host where you want to deploy the OVA.
3. Right-click the required location 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**.

   > You should use the same OVA build that you used for installing the recovery setup.

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 **Recovery** option.
10. In the **Select storage** window, select the storage for the configurations and disk files.
11. In the **Select networks** window, select a destination network for each source network.

    > You need to retain the load balancer IP address and the Kubernetes API Server IP address. You can change the node IP address or you can retain the same IP address.

12. Select **Customize template** > **system configuration** window. Enter the following details:
    a. Application username and password: This username and password is used for registering both VASA provider and SRA in the vCenter Server. This can be different from the username and password provided during initial deployment.
    b. The **Enable ASUP** checkbox is selected by default.

AutoSupport can be enabled or disabled only during deployment. .. In the **ASUP Proxy URL** field, provide this URL to avoid firewall blockage for AutoSupport data transmission. .. Administrator Username and Administrator Password: This is the password used to log in to ONTAP Tools Manager. This can be different from the username and password provided during initial deployment. .. Enter your NTP server information in the **NTP Servers** field. .. Maintenance user password: This is used to grant access to maintenance console options. . In **Customize template** > **Deployment Configuration** window, enter the details provided during deployment. All the values in this section should be the same as the ones provided during initial deployment with the exception of data LIF value.

The storage SVM name should not be changed as that is where the recovery data is stored. This applies to directly added SVM user account as well. . In the case of HA-deployment recovery, provide the following details: .. Content library details. .. vCenter configuration details. . In **Customize template** > **Node Configuration** window enter the details as per the set up you're trying to recover, non-HA or HA setup. . 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. . Power on the VM after the completion of the task.

+ The installation begins. You can track 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. . Make necessary changes in the dialog prompt. Use tab button to navigate across the panel to enter your values, **OK** or **Cancel**. . 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. . After successful installation, the web console shows the state of ONTAP tools for VMware vSphere. After successful installation, you should manually edit the hardware requirements as per the guidelines in the Prerequisites for deploying ONTAP tools for VMware vSphere page.

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

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).
051	Failed deploying secondary VMs	* If the second and third VMs are created, then ensure that enough CPU/memory resources are available before you power on the secondary VMs and restart the primary VM. * If the second and third VMs are in deploy ONTAP tools for VMware vSphere template task, wait for the task to be completed, power on the VMs and reboot the primary VM. * Redeploy.
052	Copy SSH Keys failed	Restart the primary 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.
056	Login ISCSI has failed	Make sure that iSCSI protocol is enabled and configured properly on ONTAP. Ensure that the iSCSI Data LIF IP address provided is correct and online. Restart the VM if previous points are correct. Else, redeploy.

057	Trident deployment has failed	*Ensure Management LIF and Data LIF IP addresses are reachable from VM. *Ensure NFS or iSCSI protocol is enabled and configured properly on ONTAP. *Ensure that the NFS/iSCSI Data LIF IP address provided is correct and online. *Ensure that the user name and password provided are correct and the user has sufficient privileges to create volume. * Restart if all the above points are correct. Else, redeploy.
058	Trident import has failed	*Ensure that the user name and password provided are correct and the user has sufficient privileges to create, mount, clone, and delete volumes. *Ensure that the same ONTAP setup is used to recover the setup and retry recovery.
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	VASA Provider and SRA deployment has failed	Refer to the error logs at /var/log/ansible-perl-errors.log for more details and redeploy.
064	version.xml verification failed	Redeploy
065	Swagger page URL is not reachable	Redeploy

066	Post deployment steps failed	-
088	Configuring log rotate for journald has failed	Restart the primary VM.
089	Changing ownership of summary log rotate config file has failed	Restart the primary VM.

Reboot error code	Workflow
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

Recovery error code	Workflow	Resolution
104	Post recovery steps have failed.	-
105	Copying contents to recovery volume has failed.	-
106	Failed to mount recovery volume.	* Ensure that the same SVM is used and recovery volume is present in the SVM. (Recovery volume name starts with otvng_trident_recovery) * Ensure Management LIF and Data LIF IP addresses are reachable from VM. * Ensure NFS/iSCSI protocol is enabled and configured properly on ONTAP. * Ensure that the NFS/iSCSI Dat LIF IP address provided is correct and online. * Ensure that the username, password, protocol provided are correct and the user has sufficient privileges to create, mount, clone, delete. * Retry the recovery

Copyright information

Trademark information