Deploy and upgrade ONTAP tools

ONTAP tools for VMware vSphere 9.13

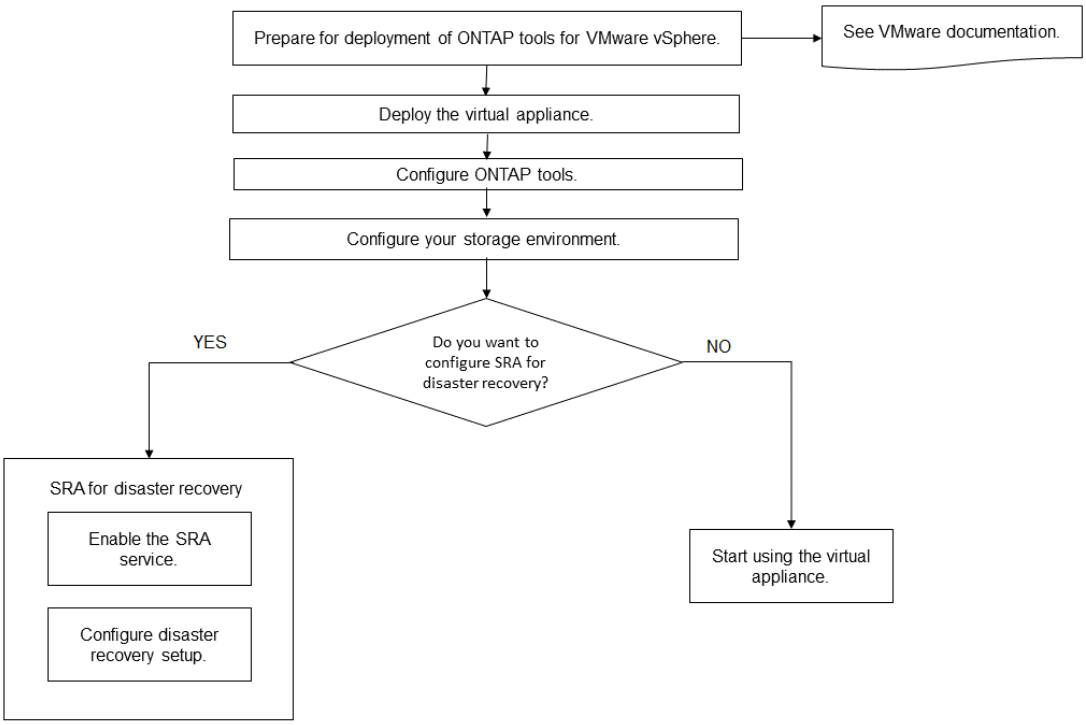
NetApp
June 19, 2024

Table of Contents

Deploy and upgrade ONTAP tools

Deployment workflow for new users of ONTAP tools for VMware vSphere

If you are new to VMware and have never used a NetApp ONTAP tools product, you need to configure your vCenter Server and setup an ESXi host, before you deploy and configure the ONTAP tools.



Deployment workflow for existing users of ONTAP tools

The 9.x releases of ONTAP tools for VMware vSphere support in-place upgrade to the latest version.

The earlier releases of individual applications like Virtual Storage Console 6.x, Storage Replication Adapter 2.x, 3.x, 4.x and VASA Provider 6.x use a different upgrade process. If you have these legacy versions of VSC or VASA Provider or SRA installed in your setup, then contact the technical support to perform the following operations:

1. Deploy the latest release of ONTAP tools.
2. Migrate any existing configuration data.

   The configuration data includes storage system credentials, as well as preferences found in the `kaminoprefs.xml` and `vscPreferences.xml` files.

Set IPv4 or IPv6 using the preferences file

In many cases, you might not need to migrate configuration data. However, if you have customized the preferences files earlier, you might want to review them and make similar changes to the newly deployed ONTAP tools. You can add the storage systems to the newly deployed ONTAP tools for VMware vSphere and specify the credentials as you add them.

If you are upgrading from VASA Provider 6.X, you should unregister VASA Provider before upgrading. See the documentation for your current release for more details.

If you are upgrading from SRA 4.0 or earlier:

- If you are using SRA 4.0P1, then you must first upgrade to SRA9.6, and then perform an in-place upgrade of the SRA 9.6 release. You can later upgrade to the latest release of ONTAP tools.

  Upgrade to the latest release of ONTAP tools

- If you are using SRA 2.1 or 3.0, you should first make note of existing site configuration details. Contact technical support for new deployment and migration.

  The Storage Replication Adapter (SRA) 4.0 for ONTAP releases also use the VASA Provider, so you must unregister VASA Provider and then deploy the latest version of ONTAP tools. The previous release of the server (`.ova`) can be removed when the upgrade is complete.

If you have the VASA Provider deployment, then after the upgrade from existing setup, you must configure the memory size for your ONTAP tools to be 12GB using the `Edit Settings` option. You must also modify the virtual memory reservation. The virtual machine must be powered off to modify the memory size.

If you are having 7.2 or 7.2.1 release of the virtual appliance for VSC, VASA Provider, and SRA, then you cannot directly upgrade to 9.7P1 or later release of the unified appliance. You must first upgrade your existing setup to the 9.7 release of the virtual appliance, and then upgrade to the latest release.

To upgrade to ONTAP tools 9.10 and later you should be running virtual appliance 9.7P1 or later. Upgrading from an earlier version prior to 9.7P1 of the virtual appliance is not supported.

If you are going to deploy the latest release of ONTAP tools, you must see the topic Space and sizing requirements for the ONTAP tools. The topic Upgrade to the latest release of ONTAP tools has information on performing an in-place upgrade.

Related information

https://mysupport.netapp.com/site/tools

VMware Cloud Foundation mode of deployment for ONTAP tools

ONTAP tools for VMware vSphere can be deployed in VMware Cloud Foundation (VCF) environment. The main objective of VCF deployment is to use ONTAP tools in a cloud setup and create containers without vCenter Server.

The VCF mode enables you to create containers for your storage without the need for a vCenter Server. VASA Provider is enabled by default after the deployment of ONTAP tools in VCF mode. After the deployment is complete, you can add, delete, or modify storage systems, and create containers using REST APIs.

Modify and delete storage system is supported from ONTAP tools for VMware vSphere 9.13P1 release onwards.

The following article has the procedure for adding storage to ONTAP tools when VCF is enabled, Add Storage to ONTAP tools from Swagger-UI.

A new API is introduced to generate the *appliance-api-token* that authenticates API calls. Some of the existing APIs are modified to include the *appliance-api-token* header. From ONTAP tools 9.12 release onwards, swagger does not support 1.0 APIs. The pointers that were previously on 1.0 are moved to 2.0 or 3.0 APIs.

From ONTAP tools for VMware vSphere 9.13 release, 2.0 Storage capability profile APIs are no longer available.

The APIs available for VCF deployment mode are:

API	HTTP method	New/modified	Section header
/2.0/admin/containers	GET	New	Container
/2.0/admin/containers	POST	New	Container
/2.0/vcf/user/login	POST	New	User Authentication
/3.0/storage/clusters	GET	Modified	Storage Systems
/3.0/storage/clusters	POST	Modified	Storage Systems
/3.0/storage/clusters	DELETE	New	Storage Systems
/3.0/storage/clusters	PUT	New	Storage Systems
/2.0/storage/clusters/discover	POST	Modified	Storage Systems
/2.0/storage/capability-profiles	GET	Modified	Storage Capability Profile
/2.0/tasks/{id}	GET	Modified	Task

You can only work with vVols datastores in the VCF deployment mode. To create container, you need to use REST APIs customized for VCF deployment. The REST APIs can be accessed from the Swagger interface after the deployment is complete. While creating containers in VCF mode, you need to provide names of storage VM, aggregate and volume. You need to use ONTAP APIs to get these details as the ONTAP tools GET APIs for these resources are not updated.

Storage object	API
Storage VM	api/svm/svms

Aggregate	storage/aggregates
Volume	storage/volumes

While executing container create API, you can add existing volumes to the container. But you should ensure that the compression and deduplication values of the existing volumes matches the storage capability of the container. The virtual machine creation fails when the values do not match. The following table provides details on the values that existing volumes should have for corresponding storage capability profiles.

Container Storage capability profile	Deduplication	Compression
Platinum_AFF_A	Both	Both
Platinum_AFF_C	Both	Both
Platinum_ASA_A	Both	Both
Platinum_ASA_C	Both	Both
AFF_NVMe_AFF_A	Both	Both
AFF_NVMe_AFF_C	Both	Both
AFF_NVMe_ASA_A	Both	Both
AFF_NVMe_ASA_C	Both	Both
AFF_Thick_AFF_A	Both	Both
AFF_Thick_AFF_C	Both	Both
AFF_Thick_ASA_A	Both	Both
AFF_Thick_ASA_C	Both	Both
AFF_Default_AFF_A	Background	None
AFF_Default_AFF_C	Background	None
AFF_Default_ASA_A	Background	None
AFF_Default_ASA_C	Background	None
AFF_Tiering_AFF_A	Both	Both

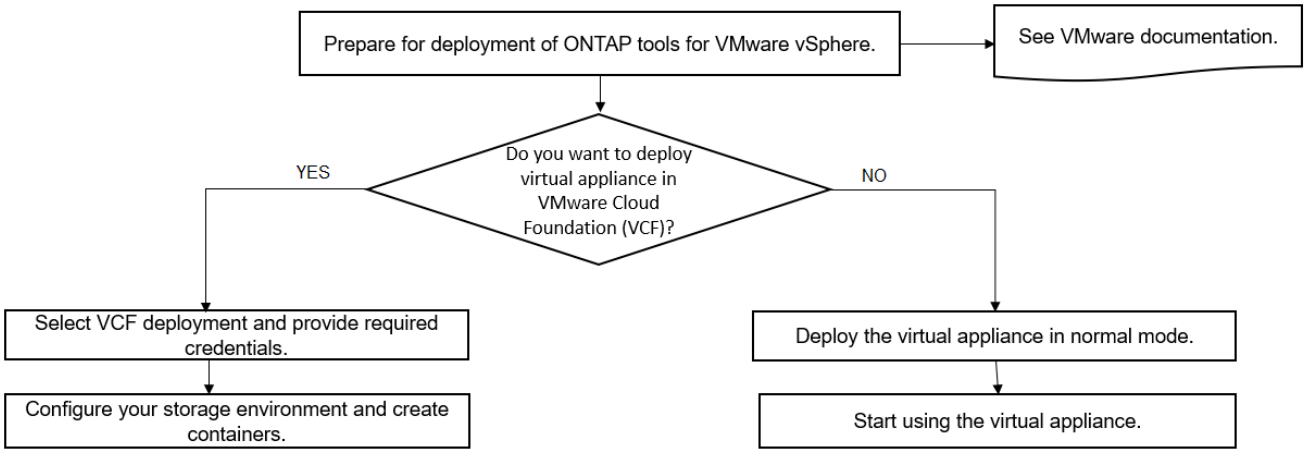
Container Storage capability profile	Deduplication	Compression
AFF_Tiering_AFF_C	Both	Both
AFF_Tiering_ASA_A	Both	Both
AFF_Tiering_ASA_C	Both	Both
AFF_Encrypted_AFF_A	Both	Both
AFF_Encrypted_AFF_C	Both	Both
AFF_Encrypted_ASA_A	Both	Both
AFF_Encrypted_ASA_C	Both	Both
AFF_Encrypted_Tiering_AFF_A	Both	Both
AFF_Encrypted_Tiering_AFF_C	Both	Both
AFF_Encrypted_Tiering_ASA_A	Both	Both
AFF_Encrypted_Tiering_ASA_C	Both	Both
AFF_Encrypted_Min50_AFF_A	Both	Both
AFF_Encrypted_Min50_AFF_C	Both	Both
AFF_Encrypted_Min50_ASA_A	Both	Both
AFF_Encrypted_Min50_ASA_C	Both	Both
Bronze	None	None

You can use the ONTAP PATCH API to set the appropriate values.

`https://<machine_IP>/api/storage/volumes/{uuid}`

The VCF deployment of ONTAP tools for VMware vSphere allows only container creation workflows. If you want to use other workflows such as provisioning datastores, creating storage capability profiles, or disaster recovery, then you should register ONTAP tools with vCenter Server using the swagger page. From ONTAP tools 9.12 onwards the registration of ONTAP tools with vCenter happens from the swagger page. The limitation of ONTAP tools in VCF mode is that you cannot configure SRA for disaster recovery until you register the plugin. When you deploy ONTAP tools without VCF mode, the registration happens automatically.

The Register.html will be removed in the upcoming releases of ONTAP tools.



How to 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, VASA Provider and Storage Replication Adapter (SRA) extensions. ONTAP tools is 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, and SRA works together with VMware Site Recovery Manager.

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

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

The minimum space and host sizing requirements are:

System	Minimum requirements
Space	2.1 GB for thin provisioned installations, 54.0 GB for thick provisioned installations
Host sizing	Recommended memory: 12 GB, Recommended CPUs: 2

You should be aware of the following licenses:

License	Description
SnapMirror	(optional) Required for performing failover operations for SRA and VASA Provider if u using vVols replication.

License	Description
FlexClone	(optional) Required for performing test failover operations for SRA and for vVols operations of VASA Provider.

ONTAP tools uses the following default bidirectional TCP ports:

Additional requirements	Description column
9083	When enabled, both VASA Provider and Storage Replication Adapter (SRA) use this port to communicate with the vCenter Server. This port is also required for obtaining the TCP/IP settings. This port needs to be enabled on the firewall from ESXi hosts to the ONTAP tools for VMware vSphere appliance. This port is used to download VP support bundle, access Web-CLI user interface, and control path communication from VMware to VP.
443	Depending on how you have configured your credentials, the VMware vCenter Server and the storage systems listen for secure communications on this port. The port is used in client-server communication architecture. The 443 port is enabled by default for secure connections. The client, which can be any automation client that uses REST API, initiates the connection to the server and the end points exchange data.
8143	ONTAP tools listens for secure communications on this port. The port is used in client-server communication architecture. The client, which can be any automation client that uses REST API, initiates the connection to the server and the end points exchange data. This port is enabled for ONTAP tools services and for exporting ONTAP tools server logs. The register.html page is hosted on this port. The REST swagger is exposed on this port.
8443	This port is used for ONTAP tools for VMware vSphere plugin service.

Minimum storage and application requirements:

Storage, host, and applications	Version requirements
ONTAP	ONTAP 9.7, 9.8P1 or later.
VMware vSphere, vCenter server, ESXi hosts, Site Recovery Manager (SRM), plug-in applications, and databases column 1	See the Interoperability Matrix Tool

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.

Optional requirements for SRA

If you are deploying the virtual appliance for use with VMware Site Recovery Manager, then you must have:
* Downloaded the `.tar.gz` file for SRA if you are using the SRM 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.

   You must deploy the `.ova` file on both the source and destination sites if you are deploying SRA.

3. Log in to the vSphere Web Client, select **Home** > **Host and Clusters**.
4. Right-click the required datacenter, and then click **Deploy OVF template**.

   If you are using vCenter7.0u3e and later releases perform the following actions, otherwise proceed to Step 5. This is an optional step to verify that the OVA binary integrity is not tampered.

   - Download the *OTV_INTER_ROOT_CERT_CHAIN.pem* file from the NetApp Support Site.
   - Navigate to **vcenter** > **administration** > **certificate management**.
   - Click on **Add trusted root certificate** option.
   - Click **Browse** and provide the path for *OTV_INTER_ROOT_CERT_CHAIN.pem* file.
   - Click **Add**.

   > The message Entrust Code Signing - OVCS2 (Trusted certificate) confirms the integrity of the downloaded OVA file.
   > If you see the message Entrust Code Signing - OVCS2 (Invalid certificate), then upgrade the VMware vCenter Server to 7.0U3E or greater version.

5. You can either enter the URL for the .ova file or browse to the folder where the .ova file is saved, and then click **Next**.
6. Enter the required details to complete the deployment.

> (Optional) If you want to create containers without registering to vCenter Server, then select the Enable VMware Cloud Foundation (VCF) checkbox in the Configure vCenter or Enable VCF section.

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

As part of the deployment checksum verifications are performed. If the deployment fails, do the following:

1. Verify vpserver/logs/checksum.log. If it says "checksum verification failed", you can see the failed jar's verification in same log.

   Log file contains the execution of *sha256sum -c /opt/netapp/vpserver/conf/checksums*.

2. Verify vscserver/log/checksum.log. If it says "checksum verification failed", you can see the failed jar's verification in same log.

   Log file contains the execution of *sha256sum -c /opt/netapp/vscerver/etc/checksums*.

Deploying SRA on SRM

You can deploy SRA either on Windows SRM server or on 8.2 SRM Appliance.

Uploading and configuring SRA on SRM Appliance

Steps

1. Download the `.tar.gz` file from the NetApp Support Site.
2. On the SRM Appliance screen, click **Storage Replication Adapter** > **New Adapter**.
3. Upload the `.tar.gz` file to SRM.
4. Rescan the adapters to verify that the details are updated in the SRM Storage Replication Adapters page.
5. Log in using administrator account to the SRM Appliance using the putty.
6. Switch to the root user: `su root`
7. At the log location enter command to get the docker ID used by SRA docker: `docker ps -l`
8. Login to the container ID: `docker exec -it -u srm <container id> sh`
9. Configure SRM with the ONTAP tools IP address and password: `perl command.pl -I <otv-IP> administrator <otv-password>`. You need to have a single quote around the password value.
   A success message confirming that the storage credentials are stored is displayed. SRA can communicate with SRA server using the provided IP address, port and credentials.

Updating SRA credentials

Steps

1. Delete the contents of the /srm/sra/conf directory using:
   a. `cd /srm/sra/conf`
   b. `rm -rf *`
2. Execute the perl command to configure SRA with the new credentials:
   a. `cd /srm/sra/`
   b. `perl command.pl -I <otv-IP> administrator <otv-password>`. You need to have a single quote around the password value.

      A success message confirming that the storage credentials are stored is displayed. SRA can

communicate with SRA server using the provided IP address, port and credentials.

Enabling VASA Provider and SRA

Steps

1. Log in to the vSphere web client by using the vCenter IP that was provided during OVA ONTAP tools deployment.
2. In the shortcuts page, click on **NetApp ONTAP tools** under plug-ins section.
3. In the left pane of ONTAP tools, **Settings > Administrative Settings > Manage Capabilities**, and enable the required capabilities.

   VASA Provider is enabled by default. If you want to use replication capability for vVols datastores, then use the Enable vVols replication toggle button.

4. Enter the IP address of the ONTAP tools for VMware vSphere and the administrator password, and then click **Apply**.

Requirements for deploying the ONTAP tools

Port requirements for ONTAP tools

By default, ONTAP tools uses designated ports to enable communication between its components, which include storage systems and the VMware vCenter Server. If you have firewalls enabled, you must ensure that the firewalls are set to allow exceptions.

For firewalls other than Windows, you should manually grant access to specific ports that ONTAP tools uses. If you do not grant access to these ports, an error message such as the following is displayed.

```
Unable to communicate with the server.
```

ONTAP tools uses the following default bidirectional TCP ports:

Default port number	Description
9083	When enabled, both VASA Provider and Storage Replication Adapter (SRA) use this port to communicate with the vCenter Server. This port is also required for obtaining the TCP/IP settings. This port needs to be enabled on the firewall from ESXi hosts to the ONTAP tools for VMware vSphere appliance. This port is used to download VP support bundle, access Web-CLI user interface, and control path communication from VMware to VP.

443	Depending on how you have configured your credentials, the VMware vCenter Server and the storage systems listen for secure communications on this port. The port is used in client-server communication architecture. The 443 port is enabled by default for secure connections. The client, which can be any automation client that uses REST API, initiates the connection to the server and the end points exchange data.
8143	ONTAP tools listens for secure communications on this port. The port is used in client-server communication architecture. The client, which can be any automation client that uses REST API, initiates the connection to the server and the end points exchange data. This port is enabled for ONTAP tools services and for exporting ONTAP tools server logs. The register.html page is hosted on this port. The REST swagger is exposed on this port.
8443	This port is used for ONTAP tools for VMware vSphere plugin service.
7	ONTAP tools sends an echo request to ONTAP to verify reachability and is required only when adding storage system and can be disabled later.

You should have enabled Internet Control Message Protocol (ICMP) before deploying the ONTAP tools.

If ICMP is disabled, then the initial configuration of ONTAP tools fails, and ONTAP tools cannot start the ONTAP tools for VMware vSphere and VASA Provider services after deployment. You must manually enable the ONTAP tools for VMware vSphere and VASA Provider services after deployment.

Space and sizing requirements for 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.

- **Installation package space requirements**
  - 2.1 GB for thin provisioned installations
  - 54.0 GB for thick provisioned installations
- **Host system sizing requirements**
  - ESXi 6.5U3 or later
  - Recommended memory: 12 GB RAM

- Recommended CPUs: 2

Supported storage system, licensing, and applications for the ONTAP tools

You should be aware of the basic storage system requirements, application requirements, and license requirements before you begin deploying the ONTAP tools for VMware vSphere.

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

Interoperability Matrix Tool

You must enable the FlexClone license for performing virtual machine snapshot operations and clone operations for VMware Virtual Volumes (vVols) datastores.

Storage Replication Adapter (SRA) requires the following licenses:

- SnapMirror license

  You must enable the SnapMirror license for performing failover operations for SRA.

- FlexClone license

  You must enable the FlexClone license for performing test failover operations for SRA.

To view the IOPS for a datastore, you must either enable Storage I/O control or uncheck the disable Storage I/O statistics collection checkbox in the Storage I/O control configuration. You can enable the Storage I/O control only if you have the Enterprise Plus license from VMware.

- Troubleshooting Storage I/O Control
- Storage I/O Control Requirements

Considerations for deploying ONTAP tools

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.

The following table presents an overview of what you should consider before you deploy ONTAP tools.

Considerations	Description
First-time deployment of ONTAP tools	The deployment of the ONTAP tools for VMware vSphere automatically installs the ONTAP tools features. Deployment workflow for new users of ONTAP tools for VMware vSphere

Upgrading from an existing deployment of ONTAP tools	The upgrade procedure from an existing deployment of ONTAP tools to ONTAP tools depends on the version of ONTAP tools, and whether you have deployed ONTAP tools. The deployment workflows and upgrade section has more information. Deployment workflow for existing users of ONTAP tools Best practices before an upgrade: • You should record information about the storage systems that are being used and their credentials. After the upgrade, you should verify that all of the storage systems were automatically discovered and that they have the correct credentials. • If you modified any of the standard ONTAP tools roles, you should copy those roles to save your changes. ONTAP tools overwrites the standard roles with the current defaults each time you restart the ONTAP tools service.
Regenerating an SSL certificate for ONTAP tools	The SSL certificate is automatically generated when you deploy the ONTAP tools. You might have to regenerate the SSL certificate to create a site-specific certificate. Regenerate an SSL certificate for Virtual Storage Console
Setting ESXi server values	Although most of your ESXi server values are set by default, it is a good practice to check the values. These values are based on internal testing. Depending on your environment, you might have to change some of the values to improve performance. • Configure ESXi server multipathing and timeout settings • ESXi host values set using ONTAP® tools for VMware vSphere
Guest operating system timeout values	The guest operating system (guest OS) timeout scripts set the SCSI I/O timeout values for supported Linux, Solaris, and Windows guest operating systems to provide correct failover behavior.

The following table presents an overview of what you require to configure the ONTAP tools.

Considerations	Description
Requirements of role-based access control (RBAC)	ONTAP tools supports both vCenter Server RBAC and ONTAP RBAC. The account used to register ONTAP tools to vCenter Server (`https://<appliance_ip>:8143/Register.html`) must be a vCenter Server administrator (assigned to the vCenter Server administrator or administrator role). If you plan to run ONTAP tools for VMware vSphere as an administrator, you must have all of the required permissions and privileges for all of the tasks. If your company requires that you restrict access to vSphere objects, you can create and assign standard ONTAP tools roles to users to meet the vCenter Server requirements. You can create the recommended ONTAP roles by using ONTAP System Manager using the JSON file provided with the ONTAP tools. If a user attempts to perform a task without the correct privileges and permissions, the task options are grayed out. • Standard roles packaged with ONTAP tools • Permissions for ONTAP storage systems and vSphere objects
ONTAP version	Your storage systems must be running ONTAP 9.7, 9.8P1 or later.
Storage capability profiles	To use storage capability profiles or to set up alarms, you must enable VASA Provider for ONTAP. After you enable VASA Provider, you can configure VMware Virtual Volumes (vVols) datastores, and you can create and manage storage capability profiles and alarms. The alarms warn you when a volume or an aggregate is at nearly full capacity or when a datastore is no longer in compliance with the associated storage capability profile.

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 administrator credentials

You can set the administrator credentials for the vCenter Server while deploying ONTAP tools.

If the password for the vCenter Server changes, then you can update the password for the administrator by using the following URL: `https://<IP>:8143/Register.html` where the IP address is of ONTAP tools that you provide during deployment.

Derby database password

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.

vCenter Server IP address

- You should provide the IP address (IPv4 or IPv6) of the vCenter Server instance to which you want to register ONTAP tools.

  The type of ONTAP tools for VMware vSphere and VASA certificates generated depends on the IP address (IPv4 or IPv6) that you have provided during deployment. While deploying ONTAP tools, if you have not entered any static IP details and your DHCP then the network provides both IPv4 and IPv6 addresses.

- The ONTAP tools IP address used to register with vCenter Server depends on the type of vCenter Server IP address (IPv4 or IPv6) entered in the deployment wizard.

  Both the ONTAP tools for VMware vSphere and VASA certificates will be generated using the same type of IP address used during vCenter Server registration.

  IPv6 is supported only with vCenter Server 6.7 and later.

Appliance network properties

If you are not using DHCP, specify a valid DNS hostname (unqualified) as well as the static IP address for the ONTAP tools for VMware vSphere and the other network parameters. All of these parameters are required for proper installation and operation.

Deploy ONTAP tools

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, VASA, and SRA 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 and SRA based on your requirements.

If you want to enable SRA in your deployment of ONTAP tools, then you must have installed the SRA plug-in on the Site Recovery Manager (SRM) server. You can download the installation file for the SRA plug-in from the **Storage Replication Adapter for ONTAP** menu in the Software Downloads section.

How to deploy ONTAP tools

To use the ONTAP tools for VMware vSphere appliance, deploy ONTAP tools for VMware vSphere in your environment and specify the required parameters.

What you will need

- You must have the supported release of vCenter Server.

  You can register ONTAP tools for VMware vSphere with either a Windows deployment of vCenter Server or a VMware vCenter Server Virtual Appliance (vCSA) deployment.

  Interoperability Matrix Tool

- You must have configured and set up your vCenter Server environment.
- You must have set up an ESXi host for your virtual machine.
- You must have downloaded the *.ova* file.
- You must have the administrator login credentials for your vCenter Server instance.
- You should have logged out of and closed all of the browser sessions of vSphere Client, and deleted the browser cache to avoid any browser cache issue during the deployment of ONTAP tools.
- You must have enabled Internet Control Message Protocol (ICMP).

  If ICMP is disabled, then the initial configuration of ONTAP tools for VMware vSphere fails. You must manually enable the ONTAP tools for VMware vSphere and VASA Provider services after deployment.

About this task

The VASA Provider is enabled by default for a fresh installation of ONTAP tools for VMware vSphere. But in case of an upgrade from an earlier release, the state of VASA Provider is retained and you might need to enable the VASA Provider manually.

Enable VASA Provider for configuring virtual datastores

Steps

1. Log in to the vSphere Client.
2. Select **Home** > **Hosts and Clusters**.
3. Right-click the required datacenter, and then click **Deploy OVF template…**.

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

4. Select the applicable method to provide the deployment file for ONTAP tools, and then click **Next**.

Location	Action

URL	Provide the URL for the *.ova* file for ONTAP tools.
Folder	Extract the .zip file, which contains the .ova file onto your local system. On the Select an OVF template page, specify the location of the .ova file inside the extracted folder.

5. Enter the details to customize the deployment wizard.

   (Optional) In the Configure vCenter or Enable VCF section, select the **Enable VMware Cloud Foundation (VCF)** checkbox and provide a password for ONTAP tools credentials. ONTAP tools stores the user details in an encoded format. For any communication from ONTAP tools to vCenter, these vCenter user details are used.
   You do not need to provide IP address but providing a password is mandatory.
   See the following for complete details.

   - Deployment customization considerations
   - VMware Cloud Foundation mode of deployment for ONTAP tools

6. Review the configuration data, and then click **Next** to finish deployment.

   As you wait for deployment to finish, you can view the progress of the deployment from the Tasks tab.

7. Power on the ONTAP tools virtual machine, and then open a console of the virtual machine running the ONTAP tools.
8. Verify that ONTAP tools is running after the deployment is completed.
9. If ONTAP tools is not registered with any vCenter Server, use `https://appliance_ip:8143/Register.html` to register the ONTAP tools instance. The Register.html redirects you to the swagger page. From ONTAP tools 9.12 onwards the registration of ONTAP tools with vCenter happens from the swagger page.

   Use the POST API to register ONTAP tools with vCenter from 9.12 onwards.

   ```
   /2.0/plugin/vcenter
   ```

10. Log out and re-log in to the vSphere Client to view the deployed ONTAP tools.

    It might take a few minutes for the plug-in to be updated in the vSphere Client.

    Troubleshooting: If you cannot view the plug-in even after logging in, you must clean the vSphere Client cache.

    Clear the vSphere cached downloaded plug-in packages

Enable VASA Provider for configuring virtual datastores

Related information

Error during fresh deployment of virtual appliance for VSC, VASA Provider, and SRA

Enable VASA Provider for configuring virtual datastores

The ONTAP tools for VMware vSphere has the VASA Provider capability enabled by default. You can configure VMware Virtual Volumes (vVols) datastores with required storage capability profiles for each vVols datastore.

What you will need

- You must have set up your vCenter Server instance and configured ESXi.
- You must have deployed ONTAP tools .

About this task

If the VASA Provider capability is disabled before upgrading to the 9.7.1 release of ONTAP tools , the VASA Provider capability remains disabled after the upgrade. This release allows you to enable vVols replication feature for vVols datastores.

Steps

1. Log in to the web user interface of VMware vSphere.
2. From the vSphere Client, select **Menu** > **NetApp ONTAP tools**.
3. Click **Settings**.
4. Click **Manage Capabilities** in the Administrative Settings tab.
5. In the Manage Capabilities dialog box, select the VASA Provider extension to enable.
6. If you want to use replication capability for vVols datastores, then use the **Enable vVols replication** toggle button.
7. Enter the IP address of ONTAP tools for VMware vSphere and the administrator password, and then click **Apply**.

> If VASA Provider status displays as “Offline” even after enabling the VASA Provider extension, then check the `/var/log/vmware/vmware-sps/sps.log` file for any connection errors with VASA Provider or restart the “vmware-sps” service.

Related information

NetApp Support

Install the NFS VAAI plug-in

You can install the NetApp NFS Plug-in for VMware vStorage APIs for Array Integration (VAAI) using the GUI of ONTAP tools for VMware vSphere.

What you will need

- You should have downloaded the installation package for the NFS Plug-in for VAAI (`.vib`) from the NetApp Support Site. NetApp Support
- You should have installed ESXi host 6.5 or later and ONTAP 9.1 or later.
- You should have powered on the ESXi host and mounted an NFS datastore.

- You should have set the values of the `DataMover.HardwareAcceleratedMove`, `DataMover.HardwareAcceleratedInit`, and `VMFS3.HardwareAcceleratedLocking` host settings to “1”.

  These values are set automatically on the ESXi host when the Recommended Settings dialog box is updated.

- You should have enabled the vstorage option on the storage virtual machine (SVM) by using the `vserver nfs modify -vserver vserver_name -vstorage enabled` command.
- You should have ESXi 7.0 update1 or later if you are using NetApp NFS VAAI plug-in 2.0.
- You should have the vSphere 7.x releases as vSphere 6.5 has been deprecated and vSphere 8.x is not supported.
- vSphere 8.x is supported with the NetApp NFS VAAI plug-in 2.0.1(build 16).

Steps

1. Rename the `.vib` file that you downloaded from the NetApp Support Site to NetAppNasPlugin.vib to match the predefined name that ONTAP tools uses.
2. Click **Settings** in the ONTAP tools home page.
3. Click **NFS VAAI Tools** tab.
4. Click **Change** in the **Existing version** section.
5. Browse and select the renamed `.vib` file, and then click **Upload** to upload the file to ONTAP tools.
6. In the Install on ESXi Hosts section, select the ESXi host on which you want to install the NFS VAAI plug-in, and then click **Install**.

   You should follow the on-screen instructions to complete the installation. You can monitor the installation progress in the Tasks section of vSphere Web Client.

7. Reboot the ESXi host after the installation finishes.

   When you reboot the ESXi host, ONTAP tools for VMware vSphere automatically detects the NFS VAAI plug-in. You do not have to perform additional steps to enable the plug-in.

Clear the vSphere cached downloaded plug-in packages

If plug-ins are not updated automatically after deploying or upgrading ONTAP tools, you should clean up the cached download plug-in packages on the browser and on the vCenter Server to resolve vCenter Server plug-in issues.

Steps

1. Logout from your existing vSphere web client or vSphere-UI.
2. Remove the browser cache.
3. Remove the vSphere Client cached plug-in packages. For VCSA, Perform the following:
   a. SSH into the VCSA appliance.
   b. Stop the VMware vSphere Client service:
   `service-control --stop vsphere-ui`

c. Change directories to the vCenter client UI extensions directory: `cd /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`

d. Remove the cached plug-in packages specific to NetApp using the `rm -rf` commands:

```
rm -rf com.netapp.nvpf.webclient-*

rm -rf com.netapp.vasa.vvol.webclient-*

rm -rf com.netapp.vsch5-*
```

e. Start the VMware vSphere Client service:
`service-control --start vsphere-ui`

Upgrade ONTAP tools

Upgrade to the latest release of ONTAP tools

You can perform an in-place upgrade to the latest release of ONTAP tools from your existing 9.10 or later release following the instructions provided here.

What you will need

- You must have downloaded the *.iso* file for the latest release of ONTAP tools.
- You must have reserved at least 12 GB of RAM for the ONTAP tools to work optimally after the upgrade.
- You must clean the vSphere Client browser cache.

  Clear the vSphere cached downloaded plug-in packages

Perform the following steps to validate the *.iso* file if required. This is an optional step:

1. Extract the public key from the code signing certificate you got issued from Entrust (OTV_ISO_CERT.pem)
   openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > csc-prod-OTV-SRA-TGZ.pub
2. Verify the signature in the digest using the public key (this step should happen in end user system prior to installing the binary. Certificate bundle should be included in the deployment package)

   openssl dgst -sha256 -verify csc-prod-OTV-SRA-TGZ.pub -signature netapp-ontap-tools-for-vmware-vsphere-9.12-9327-upgrade-iso.sig netapp-ontap-tools-for-vmware-vsphere-9.12-9327-upgrade.iso

The status of VASA Provider from the existing deployment is retained after the upgrade. You should manually enable or disable VASA Provider based on your requirement after you upgrade. However, it is best to enable VASA Provider even if VMware Virtual Volumes (vVols) are not in use, as it enables storage capability profiles for traditional datastore provisioning, and storage alarms.

You can perform an in-place upgrade to the latest release of ONTAP tools only from your existing 9.10 or later versions.

From ONTAP tools 9.12 upgrade all storage systems authentication and communication process is changed from basic authentication to certificate based authentication by auto trusting the ONTAP storage certificates. No action required from the user.

Adding a Storage system without certificate authentication is restricted.

If the storage system is added with custom created cluster scoped user using the json file and you want to upgrade to 9.12 and later versions, then
run the below commands on the ONTAP CLI before you upgrade to enable the certificate based communication between ONTAP tools for VMware vSphere and ONTAP.

1. *security login role create -role <existing-role-name> -cmddirname "security login show" -access all*
2. *security login role create -role <existing-role-name> -cmddirname "security certificate show" -access all*
3. *security login role create -role <existing-role-name> -cmddirname "security certificate install" -access all*

If the storage system is added with custom created SVM scoped user using the json file and you want to upgrade to 9.12 and later versions, then run the below commands on the ONTAP CLI with cluster admin access before upgrade to enable the certificate based communication between ONTAP tools for VMware vSphere and ONTAP:

1. *security login role create -role <existing-role-name> -cmddirname "security certificate install" -access all -vserver <vserver-name>*
2. *security login role create -role <existing-role-name> -cmddirname "security certificate show" -access all -vserver <vserver-name>*
3. *security login create -user-or-group-name <user> -application http -authentication-method cert -role <existing-role-name> -vserver <vserver-name>*
4. *security login create -user-or-group-name <user> -application ontapi -authentication-method cert -role <existing-role-name> -vserver <vserver-name>*

Steps

1. Mount the downloaded *.iso* file to the ONTAP tools:
   a. Click **Edit Settings** > **DVD/CD-ROM Drive**.
   b. Select **Datastore ISO** file from the drop-down list.
   c. Browse to and select the downloaded *.iso* file, and then select the **Connect at power on** checkbox.
2. Access the Summary tab of your deployed ONTAP tools.
3. Start the maintenance console.
4. At the “Main Menu” prompt, enter option `2` for **System Configuration**, and then enter option `8` for **Upgrade**.

   After the upgrade finishes, the ONTAP tools restarts. ONTAP tools is registered to the vCenter Server with the same IP address as before the upgrade.

5. If you want ONTAP tools to be registered with the vCenter Server with the IPv6 address, then you must perform the following:
   a. Unregister ONTAP tools.
   b. Register the IPv6 address of ONTAP tools to vCenter Server using the **Register** page.
   c. Regenerate ONTAP tools for VMware vSphere and VASA Provider certificates after the registration.

   IPv6 is supported only with vCenter Server 6.7 and later.

6. Log out and re-login to the vSphere Client to view the deployed ONTAP tools.

a. Log out from your existing vSphere web client or vSphere Client and close the window.

b. Log in to the vSphere Client.

It might take a few minutes for the plug-in to be updated in the vSphere Client.

- From ONTAP tools for VMware vSphere 9.12 onwards, the authentication with ONTAP is done through certificate. You can either add CA signed certificate or a self-signed certificate. See, Modify storage systems for instructions.
- If upgrading from the 7.0 version of ONTAP tools to the latest version of ONTAP tools, you must first create storage capability profiles before attempting to edit an existing VM Storage Policy or you might get an error that there are incorrect or missing values.
- If upgrading from an earlier version to the latest release of ONTAP tools, it is found that the `vvol.rebalance.threshold` property is missing in the `vvol.properties file.

  The default value of the property is set to 85%.* After you upgrade to the latest ONTAP tools release that has FIPS enabled but you have a older version of vCenter where FIPS is not supported, the deployment will still work.
  But if you upgrade your vCenter to the latest FIPS supported version and you have an earlier version of ONTAP tools, then the deployment will work only if FIPS is disabled on the vCenter.

Upgrade Storage Replication Adapter

After upgrading ONTAP tools or deploying the latest version of ONTAP tools, you have to upgrade your Storage Replication Adapter (SRA).

Step

1. You must upgrade to the latest adapter using one of the following procedures based on your adapter:

For…	Perform the following…
Windows	a. Log in to the SRM Windows Server. b. Change the system path to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\external\perl\c\bin` c. Enter the IP address and password of your deployed ONTAP tools .

Appliance based adapter	a. Log in to the SRM Appliance Management page. b. Click **Storage Replication Adapter**, and click **Delete** to remove the existing SRA. c. Click **New Adapter** > **Browse**. d. Click to select the latest SRA tarball file that you downloaded from NetApp support site, and then click **Install**. e. Configure SRA on the SRM Appliance. Configuring SRA on the SRM Appliance

Copyright information

Trademark information