



ONTAP tools for VMware vSphere 10.2 documentation

ONTAP tools for VMware vSphere 10.2

NetApp
January 17, 2025

Table of Contents

- ONTAP tools for VMware vSphere 10.2 documentation 1
- Release notes 2
 - Release notes 2
 - What’s new in ONTAP tools for VMware vSphere 10.2 2
 - ONTAP tools for VMware vSphere 9 and ONTAP tools for VMware vSphere 10 feature comparison 3
- Concepts 5
 - ONTAP tools for VMware vSphere overview 5
 - Key concepts and terms 5
 - Role based access control 7
 - High availability for ONTAP tools for VMware vSphere 13
 - AutoSupport 13
 - ONTAP tools Manager user interface 14
- Deploy ONTAP tools for VMware vSphere 15
 - Prerequisites for ONTAP tools for VMware vSphere deployment 15
 - Deploy ONTAP tools for VMware vSphere 17
 - Deployment error codes 21
- Configure ONTAP tools 25
 - Add vCenter Server instances 25
 - Register the VASA Provider with a vCenter Server instance 25
 - Install the NFS VAAI plug-in 26
 - Configure ESXi host settings 27
 - Configure ONTAP user roles and privileges 29
 - Add a storage backend 34
 - Associate a storage backend with a vCenter Server instance 35
 - Configure network access 36
- Protect datastores and virtual machines 37
 - Protect using host cluster protection 37
 - Protect using SRA protection 38
- Manage ONTAP tools 48
 - NetApp ONTAP tools for VMware vSphere plug-in Dashboard overview 48
 - Manage datastores 50

ONTAP tools for VMware vSphere 10.2 documentation

Release notes

Release notes

Learn about the new and enhanced features available in ONTAP tools for VMware vSphere 10.2.


For a complete list of new features and enhancements, see [What's new in ONTAP tools for VMware vSphere 10.2](#).

To learn more about whether migrating from ONTAP tools for VMware vSphere 9 to ONTAP tools 10.2 is right for your deployment, refer to [ONTAP tools for VMware vSphere 9 and ONTAP tools for VMware vSphere 10 feature comparison](#). Migration is supported from ONTAP tools for VMware vSphere 9.10D2, 9.11D4, 9.12, and 9.13 releases to ONTAP tools 10.2.

For more information, see the [ONTAP tools for VMware vSphere 10.2 Release Notes](#). You must sign in with your NetApp account or create an account to access the Release Notes.

What's new in ONTAP tools for VMware vSphere 10.2

Learn about the new capabilities available in ONTAP tools for VMware vSphere 10.2.

Update	Description
NVMe protocol support	ONTAP tools for VMware vSphere 10.2 supports both NVMe/FC and NVMe/TCP protocols to provision VMFS datastores. The seamless integrated workflows within the vCenter interface eases datastore provisioning. The benefits of using NVMe/FC and NVMe/TCP protocols to provision VMFS datastores include optimized performance, massive scalability and efficient handling of multiple data requests, significant reductions in latency, and efficient resource management. NVMe-based storage IO has up to 50% lower CPU utilization when compared to legacy data protocols.
Fibre Channel (FC) protocol support	ONTAP tools for VMware vSphere 10.2 supports the FC protocol to provision vVols and VMFS datastores. The benefits of FC protocol support include high performance, reliability and stability, scalability, enhanced security, and efficient resource management.
SnapMirror active sync	<p>SnapMirror active sync support with ONTAP tools for VMware vSphere 10.2 includes an all-new protect cluster capability that provides an end-to-end configuration workflow to build out a vSphere Metro Storage within the vCenter UI. This enables stretched cluster configurations wherein business services continue to operate even through a complete site failure, supporting applications to fail over transparently using a secondary copy.</p> <p> The SnapMirror wizard can configure SnapMirror async and sync in addition to SnapMirror active sync.</p>

Update	Description
Storage Replication Adapter (SRA) enhancements	SRA implements the VMware Site Recovery Manager (SRM) specification-based disaster recovery (DR) solution. SnapMirror active sync through SRM integration supports the disaster recovery planning and orchestrating solution to provide transparent application failover.

ONTAP tools for VMware vSphere 9 and ONTAP tools for VMware vSphere 10 feature comparison

Learn whether migrating from ONTAP tools for VMware vSphere 9 to ONTAP tools for VMware vSphere 10.1 or VMware vSphere 10.2 is right for you. For the most up-to-date compatibility information see [NetApp Interoperability Matrix Tool](#).

Feature	ONTAP tools 9.13	ONTAP tools 10.1	ONTAP tools 10.2
Key value proposition	Streamline and simplify day-0 to day-2 operations with enhanced security, compliance and automation capabilities	Evolving ONTAP tools 10.x towards 9.x parity while extending high availability, performance, and scale limits	Expanded support to include FC for VMFS and vVols, and NVMe-oF/FC, NVMe-oF/TCP for VMFS only. Ease of use for NetApp SnapMirror, simple setup for vSphere metro storage clusters, and three-site SRM support
ONTAP release qualification	ONTAP 9.9.1 to ONTAP 9.15.1	ONTAP 9.12.1 to ONTAP 9.14.1	ONTAP 9.12.1 to ONTAP 9.15.1
VMware release support	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 to VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 to VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 to VMware Live Site Recovery 9.0
Protocol support	NFS and VMFS datastores: NFS (v3 and v4.1), VMFS (iSCSI and FCP) vVols datastores: iSCSI, FCP, NVMe/FC, NFS v3	NFS and VMFS datastores: NFS (v3 and v4.1), VMFS (iSCSI) vVols datastores: iSCSI, NFS v3	NFS and VMFS datastores: NFS (v3 and v4.1), VMFS (iSCSI/FCP/NVMe-oF) vVols datastores: iSCSI, FCP, NFS v3
Scalability	Hosts and VMs: 300 Hosts, up to 10K VMs Datastores: 600 NFS, up to 50 VMFS, up to 250 vVols vVols: Up to 14,000	Hosts and VMs: 600 Hosts vVols: Up to 140,000	Hosts and VMs: 600 Hosts vVols: Up to 140,000

Feature	ONTAP tools 9.13	ONTAP tools 10.1	ONTAP tools 10.2
Observability	Performance, capacity, and host compliance dashboards Dynamic VM and datastore reports	Updated performance, capacity, and host compliance dashboards Dynamic VM and datastore reports	Updated performance, capacity, and host compliance dashboards Dynamic VM and datastore reports
Data protection	SRA replication for VMFS and NFS FlexVols based replication for vVols SCV integration and interoperable for backup	SRA replication for iSCSI VMFS and NFS v3 datastores	SRA replication for iSCSI VMFS and NFS v3 datastores three-site protection combining SMAS and SRM.
VASA provider support	VASA 4.0	VASA 3.0	VASA 3.0

Concepts

ONTAP tools for VMware vSphere overview

ONTAP tools for VMware vSphere is a set of tools for virtual machine lifecycle management. It integrates with the VMware ecosystem to help in datastore provisioning and in providing basic protection for virtual machines.

ONTAP tools for VMware vSphere is a collection of horizontally scalable, event-driven, microservices deployed as an Open Virtual Appliance (OVA). This release has REST API integration with ONTAP.

ONTAP tools for VMware vSphere consists of:

- Virtual machine functionality like basic protection and disaster recovery
- VASA Provider for VM granular management
- Storage policy-based management
- Storage Replication Adapter (SRA)

Key concepts and terms

The following section describes the key concepts and terms used in the document.

Certificate authority (CA)

CA is a trusted entity that issues Secure Sockets Layer (SSL) certificates.

Consistency group

A consistency group is a collection of volumes that are managed as a single unit. In ONTAP, consistency groups provide easy management and a protection guarantee for an application workload spanning multiple volumes. Learn more about [consistency group](#).

Dual stack

A dual-stack network is a networking environment that supports the simultaneous use of both IPv4 and IPv6 addresses.

High Availability (HA)

Cluster nodes are configured in HA pairs for non-disruptive operations.

Logical unit number (LUN)

A LUN is a number used to identify a logical unit within a Storage Area Network (SAN). These addressable devices are typically logical disks accessed through the Small Computer System Interface (SCSI) protocol or one of its encapsulated derivatives.

NVMe namespace and subsystem

An NVMe namespace is a quantity of non-volatile memory that can be formatted into logical blocks.

Namespaces are the equivalent of LUNs for FC and iSCSI protocols, and an NVMe subsystem is analogous to an igroup.

An NVMe subsystem can be associated with initiators so that namespaces within the subsystem can be accessed by the associated initiators.

ONTAP tools Manager

ONTAP tools Manager provides more control to ONTAP tools for VMware vSphere administrator over the managed vCenter Server instances and onboarded storage backends. ONTAP tools Manager helps in management of vCenter Server instances, storage backends, certificates, passwords and log bundle downloads.

Open Virtual Appliance (OVA)

OVA is an open standard for packaging and distributing virtual appliances or software that must be run on virtual machines.

SnapMirror active sync (SMAS)

SnapMirror active sync enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy. Manual intervention nor custom scripting are required to trigger a failover with SnapMirror active sync. Learn more about [SnapMirror active sync](#).

Storage Replication Adapter (SRA)

SRA is the storage vendor specific software that is installed inside the VMware Live Site Recovery appliance. The adapter enables communication between Site Recovery Manager and a storage controller at the Storage Virtual Machine (SVM) level and the cluster level configuration.

Storage virtual machine (SVM)

Like a virtual machine running on a hypervisor, SVM is a logical entity that abstracts physical resources. SVM contains data volumes and one or more LIFs through which they serve data to the clients.

Uniform and non-uniform configuration

- **Uniform host access** means that hosts from both sites are connected to all paths to storage clusters on both sites. Cross site paths are stretched across distance.
- **Non-uniform host access** means hosts in each site are connected only to the cluster in the same site. Cross-site paths and stretched paths aren't connected.



Uniform host access is supported for any SnapMirror active sync deployment; non-uniform host access is only supported for symmetric active/active deployments.

Virtual Machine File System (VMFS)

VMFS is a clustered file system specifically designed for storing virtual machine files in VMware vSphere environments.

Virtual volumes (vVols)

vVols provide a volume-level abstraction for storage used by a virtual machine. It includes several benefits and provides an alternative to using a traditional LUN. A vVol datastore is typically associated with a single LUN

which acts as a container for the vVols.

VM Storage Policy

VM Storage Policies are created in vCenter Server under Policies and Profiles. For vVols, create a rule set using rules from the NetApp vVols storage type provider.

VMware Live Site Recovery

VMware Live Site Recovery provides business continuity, disaster recovery, site migration, and non-disruptive testing capabilities for VMware virtual environments.

VMware vSphere APIs for Storage Awareness (VASA)

VASA is a set of APIs that integrate storage arrays with vCenter Server for management and administration. The architecture is based on several components including the VASA Provider which handles communication between VMware vSphere and the storage systems.

VMware vSphere Storage APIs - Array Integration (VAAI)

VAAI is a set of APIs that enables communication between VMware vSphere ESXi hosts and the storage devices. The APIs include a set of primitive operations used by the hosts to offload storage operations to the array. VAAI can provide significant performance improvements for storage-intensive tasks.

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) is a technology that enables and supports vSphere in a stretched cluster deployment. vMSC solutions are supported with NetApp MetroCluster and SnapMirror active sync (formerly SMBC). These solutions provide enhanced business continuity in the case of domain failure. The resiliency model is based on your specific configuration choices. Learn more about [VMware vSphere Metro Storage Cluster](#).

vVols datastore

The vVols datastore is a logical datastore representation of a vVols container which is created and maintained by a VASA Provider.

Zero RPO

RPO stands for recovery point objective, which is the amount of data loss deemed acceptable during a given time. Zero RPO signifies that no data loss is acceptable.

Role based access control

Overview of role-based access control in ONTAP tools for VMware vSphere

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

Components	Description
Privileges	A privilege enables or denies access to perform actions in vSphere.
Roles	A role contains one or more system privileges where each privilege defines an administrative right to a certain object or type of object in the system. By assigning a user a role, the user inherits the capabilities of the privileges defined in that role.
Users and groups	Users and groups are used in permissions to assign roles from Active Directory (AD). vCenter Server has its own local users and groups that you can use.
Permissions	Permissions allow you to assign privileges to users or groups to perform certain actions and make changes to objects inside vCenter Server. vCenter Server permissions affect only those users who log into vCenter Server rather than users who log into an ESXi host directly.
Object	An entity upon which actions are performed. VMware vCenter objects are data centers, folders, resource pools, clusters, hosts, and VMs

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



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

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

Key points about assigning and modifying roles for vCenter Server

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

Where you assign a role determines ONTAP tools for VMware vSphere tasks that a user can perform. You can modify one role at any time.

If you change the privileges within a role, the user associated with that role should log out and then log back in to enable the updated role.

Standard roles packaged with ONTAP tools for VMware vSphere

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

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

Role	Description
NetApp ONTAP tools for VMware vSphere Administrator	Provides all the native vCenter Server privileges and ONTAP tools-specific privileges that are required to perform some of ONTAP tools for VMware vSphere tasks.
NetApp ONTAP tools for VMware vSphere Read Only	Provides read-only access to ONTAP tools. These users cannot perform any ONTAP tools for VMware vSphere actions that are access-controlled.
NetApp ONTAP tools for VMware vSphere provision	Provides some of the native vCenter Server privileges and ONTAP tools-specific privileges that are required to provision storage. You can perform the following tasks: <ul style="list-style-type: none"> • Create new datastores • Manage datastores

The ONTAP tools Manager admin role is not registered with vCenter Server. This role is specific to the ONTAP tools Manager.

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

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

Permissions for ONTAP storage backends and vSphere objects

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

Components of vCenter Server permissions

The vCenter Server recognizes permissions, not privileges. Each vCenter Server permission consists of three components.

The vCenter Server has the following components:

- One or more privileges (the role)

The privileges define the tasks that a user can perform.

- A vSphere object

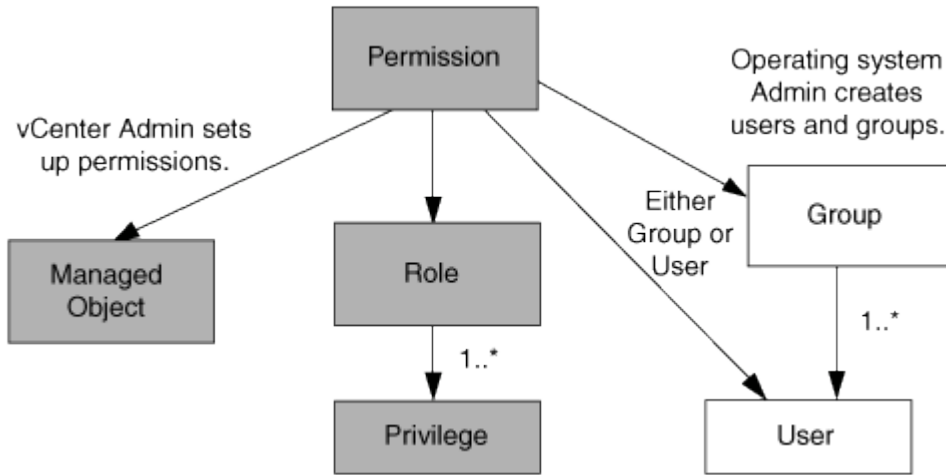
The object is the target for the tasks.

- A user or group

The user or group defines who can perform the task.



In this diagram, the gray boxes indicate components that exist in the vCenter Server, and the white boxes indicate components that exist in the operating system where the vCenter Server is running.



Privileges

Two kinds of privileges are associated with ONTAP tools for VMware vSphere:

- Native vCenter Server privileges

These privileges come with the vCenter Server.

- ONTAP tools-specific privileges

These privileges are defined for specific ONTAP tools for VMware vSphere tasks. They are unique to ONTAP tools for VMware vSphere.

ONTAP tools for VMware vSphere tasks require both ONTAP tools-specific privileges and vCenter Server native privileges. These privileges constitute the “role” for the user. A permission can have multiple privileges. These privileges are for a user that is logged into the vCenter Server.



To simplify working with vCenter Server RBAC, ONTAP tools for VMware vSphere provides several standard roles that contain all ONTAP tools-specific and native privileges that are required to perform ONTAP tools for VMware vSphere tasks.

If you change the privileges within a permission, the user that is associated with that permission should log out, and then log in to enable the updated permission.

vSphere objects

Permissions are associated with vSphere objects, such as the vCenter Server, ESXi hosts, virtual machines, datastores, datacenters, and folders. You can assign permissions to any vSphere object. Based on the permission that is assigned to a vSphere object, the vCenter Server determines who can perform which tasks

on that object. For ONTAP tools for VMware vSphere specific tasks, permissions are assigned and validated only at the root-folder level (vCenter Server) and not on any other entity. Except for VAAI plug-in operation, where permissions are validated against the concerned ESXi host.

Users and groups

You can use Active Directory (or the local vCenter Server machine) to set up users and groups of users. You can then use vCenter Server permissions to grant access to these users or groups to enable them to perform specific ONTAP tools for VMware vSphere tasks.



These vCenter Server permissions apply to ONTAP tools for VMware vSphere vCenter users, not to ONTAP tools for VMware vSphere administrators. By default, ONTAP tools for VMware vSphere administrators have full access to the product and do not require permissions assigned to them.

Users and groups do not have roles assigned to them. They gain access to a role by being part of a vCenter Server permission.

Assign and modify permissions for vCenter Server

There are several key points to keep in mind when you are working with vCenter Server permissions. Whether a ONTAP tools for VMware vSphere task succeeds can depend on where you assigned a permission, or what actions a user took after a permission was modified.

Assigning permissions

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

Where you assign permission determines ONTAP tools for VMware vSphere tasks that a user can perform.

Sometimes, to ensure the completion of a task, you should assign permission at a higher level, such as the root object. This is the case when a task requires a privilege that does not apply to a specific vSphere object (for example, tracking the task) or when a required privilege applies to a non-vSphere object (for example, a storage system).

In these cases, you can set up a permission so that it is inherited by the child entities. You can also assign other permissions to the child entities. The permission assigned to a child entity always overrides the permission inherited from the parent entity. This means you can give permissions to a child entity to restrict the scope of a permission assigned to a root object and inherited by the child entity.



Unless your company's security policies require more restrictive permissions, it is a good practice to assign permissions to the root object (also referred to as the root folder).

Permissions and non-vSphere objects

The permission that you create is applied to a non-vSphere object. For example, a storage system is not a vSphere object. If a privilege applies to a storage system, you should assign the permission containing that privilege to ONTAP tools for VMware vSphere root object because there is no vSphere object to which you can assign it.

For example, any permission that includes a privilege such as ONTAP tools for VMware vSphere privilege "Add/Modify/Skip storage systems" should be assigned at the root object level.

Modifying permissions

You can modify one permission at any time.

If you change the privileges within a permission, the user associated with that permission should log out and then log back in to enable the updated permission.

Privileges required for ONTAP tools for VMware vSphere tasks

Different ONTAP tools for VMware vSphere tasks require different combinations of privileges specific to ONTAP tools for VMware vSphere and native vCenter Server privileges.

To access ONTAP tools for VMware vSphere GUI, you should have the product-level, ONTAP tools-specific View privilege assigned at the correct vSphere object level. If you log in without this privilege, ONTAP tools for VMware vSphere displays an error message when you click the NetApp icon and prevents you from accessing ONTAP tools.

In **View** privilege, you can access ONTAP tools for VMware vSphere. This privilege does not enable you to perform tasks within ONTAP tools for VMware vSphere. To perform any ONTAP tools for VMware vSphere tasks, you should have the correct ONTAP tools-specific and native vCenter Server privileges for those tasks.

The assignment level determines which portions of the UI you can see. Assigning the View privilege to the root object (folder) enables you to enter ONTAP tools for VMware vSphere by clicking the NetApp icon.

You can assign the View privilege to another vSphere object level; however, doing that limits ONTAP tools for VMware vSphere menus that you can see and use.

The root object is the recommended place to assign any permission containing the View privilege.

Recommended ONTAP roles for ONTAP tools for VMware vSphere

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

To create new user roles, you should log in as an administrator of the storage systems running ONTAP. You can create ONTAP roles using ONTAP System Manager 9.8P1 or later.

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

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

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

Role	privileges
Discovery	This role enables you to add storage systems.
Create Storage	This role enables you to create storage. This role also includes all the privileges that are associated with the Discovery role.
Modify Storage	This role enables you to modify storage. This role also includes all the privileges that are associated with the Discovery role and the Create Storage role.
Destroy Storage	This role enables you to destroy storage. This role also includes all the privileges that are associated with the Discovery role, the Create Storage role, and the Modify Storage role.

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

High availability for ONTAP tools for VMware vSphere

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

High-availability (HA) solution provides for rapid recovery from outages caused by:

- Host failure



Only single node failure is supported.

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

No additional configuration is required for ONTAP tools for VMware vSphere to provide high availability (HA).



ONTAP tools for VMware vSphere does not support vCenter HA.

AutoSupport

AutoSupport is a mechanism that proactively monitors the health of your system and automatically sends messages to NetApp technical support, your internal support organization, and a support partner.

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

You can enable or disable AutoSupport only at the time of deployment. It is recommended to leave it enabled. Enabling AutoSupport helps to speed up problem detection and helps to achieve faster resolution. The system collects AutoSupport information and stores it locally, even when the AutoSupport is disabled. However, it does not send out the report to any network. You need to include 216.240.21.18 // support.netapp.com URL in your network for successful transmission.

ONTAP tools Manager user interface

ONTAP tools for VMware vSphere is a multi-tenant system that can manage multiple vCenter Server instances. ONTAP tools Manager provides more control to the ONTAP tools for VMware vSphere administrator over the managed vCenter Server instances and onboarded storage backends.

ONTAP tools Manager helps in:

- vCenter Server instance management - Add and manage vCenter Server instances to ONTAP tools.
- Storage backend management - Add and manage ONTAP storage clusters to ONTAP tools for VMware vSphere and map them to onboarded vCenter Server instances globally.
- Log bundle downloads - Collect log files for ONTAP tools for VMware vSphere.
- Certificate management - Change the self-signed certificate to a custom CA certificate and renew or refresh all certificates of VASA provider.
- Password management - Reset OVA application password for the user.

To access ONTAP tools Manager, launch <https://loadBalanceIP:8443/virtualization/ui/> from the browser and login with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.

Deploy ONTAP tools for VMware vSphere

Prerequisites for ONTAP tools for VMware vSphere deployment

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

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

System requirements

- **Installation package space requirements per node**

- 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

Refer to *Configuration limits to deploy ONTAP tools for VMware vSphere* section below for more details.

Minimum storage and application requirements

Storage, host, and applications	Minimum version requirements
ONTAP	Latest patch release of ONTAP 9.12.1, 9.13.1, 9.14.1, and 9.15.1.
ESXi hosts	ESXi 7.0.3
vCenter server	vCenter 7.0U3
VASA provider	3.0
OVA Application	10.2

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

[Interoperability Matrix Tool](#)

Configuration limits to deploy ONTAP tools for VMware vSphere

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

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

For details on host system sizing requirements per node, refer to [Prerequisites for deploying ONTAP tools for VMware vSphere](#).

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 checks

Ensure the following items are in place before you proceed with the deployment:

- vCenter Server environment is set up and configured.
- (Optional) For automation user - NetApp provided Postman collections JSON file is gathered.
- Parent vCenter Server Credentials to deploy the OVA are in place.



Parent vCenter Server password should not contain these special characters(\$, ', ").

- You have the login credentials for your vCenter Server instance to which the ONTAP tools for VMware vSphere will connect to post deployment, for registration.
- Browser cache is deleted.
- Ensure that you have three free IP addresses available for non-HA deployment - 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 for both HA and non-HA deployments. All the five IP addresses in HA deployment and the three IP addresses in non-HA deployment should be on the same VLAN that is selected for deployment.
- Ensure that 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. *nslookup* check on the domain name is performed 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.
- Before installing the ONTAP tools for VMware vSphere 10.2 in non-HA advanced and HA configuration, check the KB article: [Pre-requisites for non-HA advanced and HA configuration](#)

Deploy ONTAP tools for VMware vSphere

You can deploy ONTAP tools for VMware vSphere in two configurations:

- Non-HA single-node configuration
- HA configuration

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 must be accessible from VM management network.

For example, log in to ONTAP > run the command `network route create -vserver <SVM> -destination 0.0.0.0/0 -gateway <gateway_ip>`

Steps

1. Download the .zip file that contains binaries (.ova) and signed certificates for ONTAP tools for VMware vSphere from the [NetApp Support Site](#).
2. Log in to the vSphere server.
3. Navigate to the resource pool that you have created or to the cluster or to the host where you want to deploy the OVA.
4. Right-click the required location and select **Deploy OVF template....**



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

5. Select the OVA file either through the URL for the .ova file or browse to the folder where the .ova file is saved, and then click **Next**.
6. Select a computer resource and click **Next**.
7. Review the details of the template and click **Next**.
8. Read and accept the license agreement.
9. Select the deployment configuration and click **Next**.

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

10. Select the storage for the configuration and the disk files and click **Next**.
11. Select the destination network for each source network and click **Next**.
12. In the **Customize template**, enter the required details and click **Next**
 - When SVM scope is enabled you should have already enabled SVM support with management IP address.
 - The information provided here is validated for proper patterns during installation process. In case of discrepancy, an error message is displayed on the web console, and you are prompted to correct any incorrect information provided.
 - Host names must consist of uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), or the hyphen (-) special character. If you want to configure dual stack, specify the host name mapped to IPv6 address.



Pure IPV6 is not supported. Mixed mode is supported with VLAN having both IPv6 and IPv4 addresses.

13. Review the details in the **Ready to complete** window, select **Finish**.

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

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

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 prerequisite step for deploying HA three nodes configuration. 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.



Content library template once uploaded should not be deleted post deployment, as it will be used during reboots.

Create the content library using the following steps:

1. Download the .zip file that contains binaries (.ova) and signed certificates for ONTAP tools for VMware vSphere from the [NetApp Support Site](#).
2. Log in to the vSphere client using `https://vcenterip/ui`
3. Select the horizontal ellipses next to vSphere client and select **Content library**.
4. Select **Create** on the right of the page.
5. Provide a name for the library and create the content library.
6. Navigate to the content library you created.
7. Select **Actions** in the right of the page and select **Import item** and import the OVA file.



For more information, refer to [Creating and Using Content Library](#) blog.

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. Download the `.zip` file that contains binaries (`.ova`) and signed certificates for ONTAP tools for VMware vSphere from the [NetApp Support Site](#).
2. Log in to the vSphere server.
3. Navigate to the resource pool that you have created or to the cluster or to the host where you want to deploy the OVA.
4. Right-click the required location and select **Deploy OVF template....**



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

5. Select the OVA file either through the URL for the `.ova` file or browse to the folder where the `.ova` file is saved, and then click **Next**.
6. To deploy ONTAP tools for VMware vSphere 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**
7. Select a computer resource and click **Next**.
8. Review the details of the template and click **Next**.
9. Read and accept the license agreement and click **Next**.
10. Select the deployment configuration and click **Next**.
11. Select the storage for the configuration and the disk files and click **Next**.
12. Select the destination network for each source network and click **Next**.
13. In the **Customize template** window, fill in the required fields and click **Next**.
 - In HA mode of deployment, do not rename the VM names after the deployment.
 - When SVM scope is enabled you should have already enabled SVM support with management IP address.
 - The information provided here is validated for proper patterns during installation process. In case of discrepancy, an error message is displayed on the web console, and you are prompted to correct any incorrect information provided.
 - Host names must consist of uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), or the hyphen (-) special character. If you want to configure dual stack, specify the host name mapped to IPv6 address.



Pure IPV6 is not supported. Mixed mode is supported with VLAN having both IPv6 and IPv4 addresses.

14. 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.

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

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

In case of any discrepancies in the values entered in the OVF form, a dialog box will prompt you to take corrective action. Make the necessary changes within the dialog box, utilizing the tab button to navigate and select "OK." You have three attempts to rectify any issues. If issues persist after three attempts, the installation process will cease, and it is recommended to retry the installation on a fresh VM.

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	<p>* 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.</p> <p>* 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.</p> <p>* Redeploy.</p>
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	<p>*Ensure Management LIF and Data LIF IP addresses are reachable from VM.</p> <p>*Ensure NFS or iSCSI protocol is enabled and configured properly on ONTAP.</p> <p>*Ensure that the NFS/iSCSI Data LIF IP address provided is correct and online.</p> <p>*Ensure that the user name and password provided are correct and the user has sufficient privileges to create volume.</p> <p>* Restart if all the above points are correct. Else, redeploy.</p>

058	Trident import has failed	<p>*Ensure that the user name and password provided are correct and the user has sufficient privileges to create, mount, clone, and delete volumes.</p> <p>*Ensure that the same ONTAP setup is used to recover the setup and retry recovery.</p>
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.	<ul style="list-style-type: none"> * 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 Data 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

Configure ONTAP tools

Add vCenter Server instances

vCenter Server provides the central management platform that allows you to control hosts, virtual machines (VMs), and storage backends.

About this task

You can add and manage multiple vCenter Server instances with one instance of ONTAP tools for VMware vSphere.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **vCenters** from the sidebar.
4. Select **Add** to onboard vCenter Server instances and provide your vCenter IP address/hostname, username, password, and port details.

When you add a vCenter Server instance to ONTAP tools, the following actions are performed automatically:

- The vCenter Client Plug-in is registered
- Custom privileges for the plug-ins and APIs are pushed to the vCenter Server instance
- Custom roles are created to manage the users.

When you add a vCenter Server instance, ONTAP tools for VMware vSphere plug-in is registered automatically to vCenter Server as a remote plug-in. The plug-in is visible on the vSphere user interface shortcuts.

The plug-in is registered with a key `com.netapp.otv` to the vCenter Server instance and can be seen in the ExtensionManager of the vCenter Server instance.

Register the VASA Provider with a vCenter Server instance

You can register and unregister the VASA provider with a vCenter Server instance using ONTAP tools for VMware vSphere remote plugin interface.

VASA Provider Settings section shows the VASA Provider registration state for the selected vCenter Server.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
3. Select **Settings > VASA provider settings**. VASA provider registration state shows as not registered.
4. Click on **REGISTER** button to register the VASA Provider.

5. Enter a name for the VASA provider and provide ONTAP tools for VMware vSphere application user credentials and click **REGISTER**.
6. On successful registration and page refresh, UI shows the state, name, and version of the registered VASA provider. The unregister action is activated.
7. If you want to unregister the VASA provider, perform the following steps:
 - a. To unregister the VASA provider select **Unregister** option at the bottom of the screen.
 - b. In the **Unregister VASA provider** page, you can see the name of the VASA provider. In this page provide the application user credentials and click **Unregister**.

After you finish

Verify that the onboarded VASA provider is listed under VASA Provider from vCenter client UI and from remote plug-in UI.

Steps

1. To verify VASA Provider from vCenter client UI follow these steps:
 - a. Navigate to vCenter Server.
 - b. Log in with the administrator credentials.
 - c. Select **Storage Providers**.
 - d. Select **Configure**.
 - e. Under Storage Provider/storage backends verify that the onboarded VASA provider is listed correctly.
2. To verify VASA Provider from the remote plug-in UI follow these steps:
 - a. Log in to the vSphere client using `https://vcenterip/ui`
 - b. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
 - c. You can see the registered VASA Provider in the overview page and in the **Settings > VASA provider settings** page.

Install the NFS VAAI plug-in

You can install the NetApp NFS Plug-in for vSphere APIs for Array Integration (VAAI) using 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 NFS Plug-in for VMware VAAI](#)
- You should have installed ESXi host 7.0U3 latest patch as minimum version and ONTAP 9.12.1Px (latest P release) 9.13.1Px, 9.14.1Px, 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 7.0U3 or later if you are using NetApp NFS VAAI plug-in 2.0.
- You should have the vSphere 7.0U3 latest patch releases as vSphere 6.5 has been deprecated.
- vSphere 8.x is supported with the NetApp NFS VAAI plug-in 2.0.1(build 16).

Steps

1. Click **Settings** from the ONTAP tools for VMware vSphere home page.
2. Click **NFS VAAI Tools** tab.
3. When the VAAI plug-in is uploaded to vCenter Server, select **Change** in the **Existing version** section. If a VAAI plug-in is not uploaded to the vCenter Server, select **Upload** button.
4. Browse and select the `.vib` file and click **Upload** to upload the file to ONTAP tools.
5. Click **Install on ESXi host**, select the ESXi host on which you want to install the NFS VAAI plug-in, and then click **Install**.

Only the ESXi hosts that are eligible for the plug-in installation are displayed. You should follow the on-screen instructions to complete the installation. You can monitor the installation progress in the Recent Tasks section of vSphere Web Client.

6. You should manually reboot the ESXi host after the installation finishes.

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

Configure the correct NFS export policies for VAAI copy offload

When configuring VAAI in a NFS environment, export policy rules should be configured with the following requirements in mind:

- The relevant volume needs to allow the NFSv4 calls.
- The root user should remain as root and NFSv4 should be allowed in all junction parent volumes.
- The option for VAAI support needs to be set on the relevant NFS server.

For more information on the procedure, refer to [Configure the correct NFS export policies for VAAI copy offload](#) KB article.

Configure ESXi host settings

Configure ESXi server multipath and timeout settings

ONTAP tools for VMware vSphere checks and sets the ESXi host multipath settings and HBA timeout settings that work best with NetApp storage systems.

About this task

This process might take a long time, depending on your configuration and system load. The task progress is displayed in the Recent Tasks panel. As the tasks are completed, the host status Alert icon is replaced by the Normal icon or the Pending Reboot icon.

Steps

1. From the VMware vSphere Web Client home page, click **Hosts and Clusters**.
2. Right-click a host and select **NetApp ONTAP tools > Update host data**.
3. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
4. Go to ESXi Host compliance card in the Overview (Dashboard) of the ONTAP tools for VMware vSphere plug-in.
5. Select **Apply Recommended Settings** link.
6. In the **Apply recommended host settings** window, select the hosts that you want to comply with NetApp recommended host settings and click **Next**.



You can expand the ESXi host to see the current values.

7. In the settings page, select the recommended values as required.
8. In the summary pane, check the values and click **Finish**.
You can track the progress in the Recent task panel.

Set ESXi host values

You can set timeouts and other values on the ESXi hosts using ONTAP tools for VMware vSphere to ensure best performance and successful failover. The values that ONTAP tools for VMware vSphere sets are based on internal NetApp testing.

You can set the following values on an ESXi host:

HBA/CNA Adapter Settings

Sets the recommended HBA timeout settings for NetApp storage systems.

- **Disk.QFullSampleSize**

Set this value to 32 for all configurations. Setting this value helps to prevent I/O errors.

- **Disk.QFullThreshold**

Set this value to 8 for all configurations. Setting this value helps prevent I/O errors.

- **Emulex FC HBA timeouts**

Use the default value.

- **QLogic FC HBA timeouts**

Use the default value.

MPIO Settings

MPIO settings define preferred paths for NetApp storage systems. The MPIO settings determine which of the available paths are optimized (as opposed to non-optimized paths that traverse the interconnect cable) and they set the preferred path to one of those paths.

In high-performance environments, or when you are testing performance with a single LUN datastore, consider changing the load balance setting of the round-robin (VMW_PSP_RR) path selection policy (PSP) from the default IOPS setting of 1000 to a value of 1.

NFS settings

- **Net.TcpipHeapSize**

Set this value to 32.

- **Net.TcpipHeapMax**

Set this value to 1024MB.

- **NFS.MaxVolumes**

Set this value to 256.

- **NFS41.MaxVolumes**

Set this value to 256.

- **NFS.MaxQueueDepth**

Set this value to 128 or higher to avoid queuing bottlenecks.

- **NFS.HeartbeatMaxFailures**

Set this value to 10 for all NFS configurations.

- **NFS.HeartbeatFrequency**

Set this value to 12 for all NFS configurations.

- **NFS.HeartbeatTimeout**

Set this value to 5 for all NFS configurations.

Configure ONTAP user roles and privileges

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

What you'll need

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



You can create users at cluster or directly at storage virtual machines (SVMs) level. You can also create users without using the `user_roles.json` file and if done so, you need to have a minimum set of privileges at SVM level.

- You should have logged in with administrator privileges for the storage backend.

Steps

1. Extract the downloaded `https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip` file.
2. Access ONTAP System Manager using the cluster management IP address of the cluster.
3. Login to cluster with admin privileges. To configure a user, perform the following steps:
 - a. To configure cluster ONTAP tools user, select **Cluster > Settings > Users and Roles** pane.
 - b. To configure SVM ONTAP tools user, select **Storage SVM > Settings > Users and Roles** pane.
 - c. Select **Add** under Users.
 - d. In the **Add User** dialog box, select **Virtualization products**.
 - e. **Browse** to select and upload the ONTAP Privileges JSON file.

The Product field is auto populated.

- f. Select the required capability from the product capability drop-down menu.

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

- g. Enter the required username and password.
- h. Select the privileges (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) required for the user, and then click **Add**.

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



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

SVM aggregate mapping requirements

To use SVM user credentials for provisioning datastores, internally ONTAP tools for VMware vSphere creates volumes on the aggregate specified in the datastores POST API. The ONTAP does not allow the creation of volumes on unmapped aggregates on an SVM using SVM user credentials. To resolve this, you need to map the SVMs with the aggregates using the ONTAP REST API or CLI as described here.

REST API:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```


ONTAP CLI:

```
still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver          Aggregate          State          Size Type          SnapLock
Type-----
-----svm_test          still15_vsim_ucs630f_aggr1
online          10.11GB vmdisk  non-snaplock
```

Create ONTAP user and role manually

Follow the instructions in this section to create the user and roles manually without using the JSON file.

1. Access ONTAP System Manager using the cluster management IP address of the cluster.
2. Login to cluster with admin privileges.
 - a. To configure cluster ONTAP tools roles, select **Cluster > Settings > Users and Roles** pane.
 - b. To configure cluster SVM ONTAP tools roles, select **Storage SVM > Settings > Users and Roles** pane
3. Create Roles:
 - a. Select **Add** under **Roles** table.
 - b. Enter the **Role name** and **Role Attributes** details.

Add the **REST API Path** and the respective access from the drop down.

- c. Add all the needed APIs and save the changes.
4. Create Users:
 - a. Select **Add** under **Users** table.
 - b. In the **Add User** dialog box, select **System Manager**.
 - c. Enter the **Username**.
 - d. Select **Role** from the options created in the **Create Roles** step above.
 - e. Enter the applications to give access to and the authentication method. ONTAPI and HTTP are the required applications, and the authentication type is **Password**.
 - f. Set the **Password for the User** and **Save** the user.

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

The minimum privileges required for non-admin global scoped cluster user created without using the users JSON file are listed in this section.

If a cluster is added in local scope, it is recommended to use the JSON file to create the users, as ONTAP tools for VMware vSphere requires more than just the Read privileges for provisioning on ONTAP.

Using APIs:

API	Access level	Used for
/api/cluster	Read-Only	Cluster Configuration Discovery

/api/cluster/licensing/licenses	Read-Only	License Check for Protocol specific licenses
/api/cluster/nodes	Read-Only	Platform type discovery
/api/storage/aggregates	Read-Only	Aggregate space check during Datastore/Volume provisioning
/api/storage/cluster	Read-Only	To get the Cluster level Space and Efficiency Data
/api/storage/disks	Read-Only	To get the Disks associated in an Aggregate
/api/storage/qos/policies	Read/Create/Modify	QoS and VM Policy management
/api/svm/svms	Read-Only	To get SVM configuration in the case the Cluster is added locally.
/api/network/ip/interfaces	Read-Only	Add Storage Backend - To identify the management LIF scope is Cluster/SVM
/api	Read-Only	Cluster users should have this privilege to get the correct storage backend status. Otherwise, ONTAP tools Manager shows "unknown" storage backend status.

Upgrade ONTAP tools for VMware vSphere 10.1 user to 10.2 user

If the ONTAP tools for VMware vSphere 10.1 user is a cluster scoped user created using the json file, then run the following commands on the ONTAP CLI using the admin user to upgrade to 10.2 release.

For product capabilities:

- VSC
- VSC and VASA Provider
- VSC and SRA
- VSC, VASA Provider, and SRA.

Cluster privileges:

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access
```

all

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all
```

If the ONTAP tools for VMware vSphere 10.1 user is a SVM scoped user created using the json file, then run the following commands on the ONTAP CLI using the admin user to upgrade to 10.2 release.

SVM privileges:

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>
```

Adding command *vserver nvme namespace show* and *vserver nvme subsystem show* to the existing role adds the following commands.

```
vserver nvme namespace create
```

```
vserver nvme namespace modify
```

```
vserver nvme subsystem create
```

```
vserver nvme subsystem modify
```

Add a storage backend

Storage backends are systems that the ESXi hosts use for data storage. You can add a storage backend using either the ONTAP tools Manager or the vSphere client UI.

About this task

This task helps you to onboard an ONTAP cluster. When you add storage backend using ONTAP tools Manager, the storage backend is added to the global cluster. Associate the global cluster with a vCenter Server instance to enable an SVM user for vVols datastore provisioning.

Using ONTAP tools Manager



A storage backend is global when added from ONTAP tools Manager or the ONTAP tools APIs. A storage backend is local when added from the vCenter Server APIs. For example, in a multi-tenant setup, you can add a storage backend (cluster) globally and SVM locally to use SVM user credentials.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Storage Backends** from the sidebar.
4. Select **Add**.
5. Provide the Server IP address or FQDN, username, and password details and select **Add**.



IPV4 and IPV6 management LIFs are supported. SVM user-based credentials with management LIFs are also supported.

Using vSphere client UI



When you add a storage backend using the vSphere client UI, vVols datastore does not support adding of an SVM user directly.

1. Log in to the vSphere client using `https://vcenterip/ui`
2. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Storage Backends** and select **Add**.
4. In the **Add Storage Backend** window, provide the Server IP address, username, password, and port details and click **Add**.



You can add cluster-based credentials and IPV4 and IPV6 management LIFs or provide SVM-based credentials with management LIF of SVM to add an SVM user directly.

The list gets refreshed, and you can see the newly added storage backend in the list.

Associate a storage backend with a vCenter Server instance

The vCenter Server listing page shows the associated number of storage backends. Each vCenter Server instance has the option to associate a storage backend.

About this task

This task helps you to create mapping between storage backend and the onboarded vCenter Server instance globally.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select vCenter from the sidebar.
4. Click on the vertical ellipses against the vCenter that you want to associate with storage backends.
5. Select storage backend from the dropdown in the pop up.
6. Select **Associate Storage Backend** option to associate vCenter Server instance with the required storage backend.

Configure network access

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

You can choose to allow a few specific ESXi host addresses for datastore mount operation. If the setting is not provided, the export policy adds all IP addresses discovered in the pre-mount step. If the setting is provided, ONTAP tools for VMware vSphere add only the ones which fall within the listed IP addresses or range. If none of the IP addresses of a host belong to the listed IP addresses, the mount on that host fails.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Settings > Manage Network Access > Edit**.

Use a comma (,) to separate the IP addresses. You can specify a specific IP address, or a range of IP addresses or IPv6 addresses.

4. Click **Save**.

Protect datastores and virtual machines

Protect using host cluster protection

Create host cluster protection

ONTAP tools for VMware vSphere manages protection of host clusters.

All the datastores belonging to the selected SVM and mounted on one or more hosts of the cluster are protected under a host cluster.

Prerequisites

Ensure the following prerequisites are met:

- The host cluster has datastores only from one SVM.
- Datastore mounted on the host cluster should not be mounted on any host outside of the cluster.
- All Datastores mounted on the host cluster must be VMFS datastores with iSCSI/FC protocol. VMFS datastores with NVMe/FC and NVMe/TCP protocols are not supported.
- FlexVol/LUN forming datastores mounted on the host cluster should not be part of any existing consistency group (CG).
- FlexVol/LUN forming datastores mounted on the host cluster should not be part of any existing SnapMirror relationship.
- The host cluster should have at least one datastore.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. Right-click a host cluster and select **NetApp ONTAP tools > Protect Cluster**.
3. In the protect cluster window, the datastore type and source storage virtual machine (VM) details are auto populated. Select the datastores link to view the datastores that are protected.
4. Enter the **consistency group name**.
5. Select **Add Relationship**.
6. In the **Add SnapMirror Relationship** window, select the **Target storage VM** and the **Policy** type.

The policy type can be Asynchronous or AutomatedFailOverDuplex.

When you add SnapMirror relationship as AutomatedFailOverDuplex type policy, it is mandatory to add the target storage VM as storage backend to the same vCenter where ONTAP tools for VMware vSphere is deployed.

In AutomatedFailOverDuplex policy type, there is uniform and non-uniform host configuration.

When you select the **uniform host configuration** toggle button, the host initiator group configuration is implicitly replicated on the target site. For details, refer to [Key concepts and terms](#)

7. If you choose to have a non-uniform host configuration, select the host access (source/target) for each host inside that cluster.
8. Select **Add**.
9. In the **Protect cluster** window, during create operation, only delete action is supported. You can delete and

add the protection again. During Modify host cluster protection operation, edit option is available. You can edit or delete the relationships using the kebab menu options.

10. Select **Protect** button.

A vCenter task is created with job ID details and the progress is shown in the Recent tasks panel. This is an asynchronous task, user interface shows only the request submission status and does not wait for the task completion.

11. To view the protected host clusters, navigate to **NetApp ONTAP tools > Protection > Host cluster relationships**.

Protect using SRA protection

Enable SRA to protect datastores

ONTAP tools for VMware vSphere provides the option to enable the SRA capability to configure disaster recovery.

What you will need

- You should have set up your vCenter Server instance and configured ESXi host.
- You should have deployed ONTAP tools.
- You should have downloaded the SRA Adapter `.tar.gz` file from the [NetApp Support Site](#).

Steps

1. Log in to the VMware Live Site Recovery appliance management interface using the URL: `https://:<srm_ip>:5480`, and then go to Storage Replication Adapters in VMware VMware Live Site Recovery appliance management interface.
2. Select **New Adapter**.
3. Upload the `.tar.gz` installer for the SRA plug-in to VMware Live Site Recovery.
4. Rescan the adapters to verify that the details are updated on the VMware Live Site Recovery Storage Replication Adapters page.

Configure SRA for SAN and NAS environments

You should set up the storage systems before running Storage Replication Adapter (SRA) for VMware Live Site Recovery.

Configure SRA for SAN environments

What you will need

You should have the following programs installed on the protected site and the recovery site:

- VMware Live Site Recovery

Documentation about installing VMware Live Site Recovery is on the VMware site.

[About VMware Live Site Recovery](#)

- SRA

The adapter is installed on VMware Live Site Recovery.

Steps

1. Verify that the primary ESXi hosts are connected to the LUNs in the primary storage system on the protected site.
2. Verify that the LUNS are in igroups that have the `ostype` option set to *VMware* on the primary storage system.
3. Verify that the ESXi hosts at the recovery site have appropriate iSCSI connectivity to the storage virtual machine (SVM). The secondary site ESXi hosts should have access to the secondary site storage, and the primary site ESXi hosts should have access to the primary site storage.

You can do this either by verifying that the ESXi hosts have local LUNs connected on the SVM or the `iscsi show initiators` command on the SVMs.

Check the LUN access for the mapped LUNs in the ESXi host to verify iSCSI connectivity.

Configure SRA for NAS environments

What you will need

You should have the following programs installed on the protected site and the recovery site:

- VMware Live Site Recovery

Documentation about installing VMware Live Site Recovery can be found on the VMware site.

[About VMware Live Site Recovery](#)

- SRA

The adapter is installed on VMware Live Site Recovery and the SRA server.

Steps

1. Verify that the datastores at the protected site contain virtual machines that are registered with vCenter Server.
2. Verify that the ESXi hosts at the protected site have mounted the NFS exports volumes from the storage virtual machine (SVM).
3. Verify that valid addresses such as the IP address, host name, or FQDN on which the NFS exports are present are specified in the **NFS Addresses** field when using the Array Manager wizard to add arrays to VMware Live Site Recovery.
4. Use the `ping` command on each ESXi host at the recovery site to verify that the host has a VMkernel port that can access the IP addresses that are used to serve NFS exports from the SVM.

Configure SRA for highly scaled environments

You should configure the storage timeout intervals per the recommended settings for

Storage Replication Adapter (SRA) to perform optimally in highly scaled environments.

Storage Provider settings

You should set the following timeout values on VMware Live Site Recovery for scaled environment:

Advanced settings	Timeout values
<code>StorageProvider.resignatureTimeout</code>	Increase the value of the setting from 900 seconds to 12000 seconds.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Set a high value (For example: 99999)

You should also enable the `StorageProvider.autoResignatureMode` option.

See the VMware documentation for more information on modifying Storage Provider settings.

[VMware vSphere Documentation: Change Storage Provider Settings](#)

Storage settings

When you hit a timeout, increase the values of `storage.commandTimeout` and `storage.maxConcurrentCommandCnt` to a higher value.



The timeout interval specified is the maximum value. You do not need to wait for the maximum timeout to be reached. Most commands finish within the set maximum timeout interval.

See the VMware documentation on modifying SAN Provider settings for more information.

[VMware Site Recovery Manager Documentation: Change Storage Settings](#)

Configure SRA on VMware Live Site Recovery appliance

After you have deployed the VMware Live Site Recovery appliance, you should configure SRA on VMware Live Site Recovery appliance. The successful configuration of SRA enables the VMware Live Site Recovery appliance to communicate with SRA for disaster recovery management. You should store ONTAP tools for VMware vSphere credentials (IP address) in the VMware Live Site Recovery appliance to enable communication between VMware Live Site Recovery appliance and SRA.

What you will need

You should have downloaded the `tar.gz` file from [NetApp Support Site](#).

About this task

The configuration of SRA on VMware Live Site Recovery appliance stores the SRA credentials in the VMware Live Site Recovery appliance.

Steps

1. On the VMware Live Site Recovery appliance screen, click **Storage Replication Adapter > New Adapter**.
2. Upload the `.tar.gz` file to VMware Live Site Recovery.
3. Log in using administrator account to the VMware Live Site Recovery appliance using putty.
4. Switch to the root user using the command: `su root`
5. Run the command `cd /var/log/vmware/srm` to navigate to the log directory.
6. At the log location, enter the command to get the docker ID used by SRA: `docker ps -l`
7. To log in to the container ID, enter the command: `docker exec -it -u srm <container id> sh`
8. Configure VMware Live Site Recovery with ONTAP tools for VMware vSphere IP address and password using the command: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>'`



You need to provide the password value within single quotes to ensure that the Perl script does not read the special characters in the password as a delimiter of the input.



The application username and password is set during the ONTAP tools deployment. This is needed for VASA provider/SRA registration.

9. Rescan the adapters to verify that the details are updated on the VMware Live Site Recovery Storage Replication Adapters page.

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.

Update SRA credentials

For VMware Live Site Recovery to communicate with SRA, you should update SRA credentials on the VMware Live Site Recovery server if you have modified the credentials.

What you will need

You should have executed the steps mentioned in the topic [Configuring SRA on VMware Live Site Recovery appliance](#).

Steps

1. Run the following commands to delete the VMware Live Site Recovery machine folder cached ONTAP tools username password:
 - a. `sudo su <enter root password>`
 - b. `docker ps`
 - c. `docker exec -it <container_id> sh`

d. `cd /conf`

e. `rm -rf *`

2. Run the Perl command to configure SRA with the new credentials:

a. `cd ..`

b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` 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.

Configure protection groups

You should create protection groups to protect a group of virtual machines on the protected site.

What you will need

You should ensure that both the source and target sites are configured for the following:

- Same version of VMware Live Site Recovery installed
- Virtual machines
- Paired protected and recovery sites
- Source and destination datastores should be mounted on respective sites

Steps

1. Log in to vCenter Server and then click **Site Recovery > Protection Groups**.
2. In the **Protection Groups** pane, click **New**.
3. Specify a name and description for the protection group, direction and click **Next**.
4. In the **Type** field, select the **Type field option...** as Datastore groups (array-based replication) for NFS and VMFS datastore.
The fault domain is nothing but SVMs with replication enabled. The SVMs that have only peering implemented and have no issues are displayed.
5. In the Replication groups tab, select either the enabled array pair or the replication groups that have the virtual machine you configured, and then click **Next**.

All the virtual machines on the replication group are added to the protection group.

6. Select either the existing recovery plan or create a new plan by clicking **Add to new recovery plan**.
7. In the Ready to complete tab, review the details of the protection group that you created, and then click **Finish**.

Pair protected and recovery sites

You should pair the protected and recovery sites created using your vSphere Client to enable Storage Replication Adapter (SRA) to discover the storage systems.



Storage Replication Adapter (SRA) does not support fan-out SnapMirror configurations. SnapMirror fan-out configurations are those where a source volume is replicated to two different destinations. These create a problem during recovery when VMware Live Site Recovery needs to recover the virtual machine from its destination.

What you will need

- You should have VMware Live Site Recovery installed on the protected and recovery sites.
- You should have SRA installed on the protected and recovery sites.

Steps

1. Double-click **Site Recovery** on the vSphere Client home page and click **Sites**.
2. Click **Objects > Actions > Pair Sites**.
3. In the **Pair Site Recovery Manager Servers** dialog box, enter the address of the protected site's Platform Services Controller, and then click **Next**.
4. In the Select vCenter Server section, do the following:
 - a. Verify that the protected site's vCenter Server appears as a matching candidate to pair.
 - b. Enter the SSO administrative credentials, and then click **Finish**.
5. If prompted, click **Yes** to accept the security certificates.

Result

Both the protected and recovery sites will appear in the Objects dialog box.

Configure protected and recovery site resources

Configure network mappings

You should configure your resource mappings like VM networks, ESXi hosts, and folders on both sites to enable the mapping of each resource from the protected site to the appropriate resource at the recovery site.

You should complete the following resource configurations:

- Network mappings
- Folder mappings
- Resource mappings
- Placeholder datastores

What you will need

You should have connected the protected and recovery sites.

Steps

1. Log in to vCenter Server and click on **Site Recovery > Sites**.
2. Select your protected site and click **Manage**.

3. In the Manage tab, select **Network Mappings**.
4. Click **New** to create a new network mapping.

The Create Network Mapping wizard appears.

5. In the Create Network Mapping wizard, perform the following:
 - a. Select **Automatically Prepare Mappings for Networks with Matching Names** and click **Next**.
 - b. Select the required data center objects for the protected and recovery sites and click **Add Mappings**.
 - c. Click **Next** after mappings are created successfully.
 - d. Select the object used earlier to create reverse mapping, then click **Finish**.

Result

The Network Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configure folder mappings

You should map your folders on the protected site and recovery site to enable communication between them.

What you will need

You should have connected the protected and recovery sites.

Steps

1. Log in to vCenter Server and click on **Site Recovery > Sites**.
2. Select your protected site and click **Manage**.
3. In the Manage tab, select **Folder Mappings**.
4. Select **Folder** icon to create a new folder mapping.

The Create Folder Mapping wizard appears.

5. In the Create Folder Mapping wizard, perform the following:
 - a. Select **Automatically Prepare Mappings for Folders with Matching Names** and click **Next**.
 - b. Select the required data center objects for the protected and recovery sites and click **Add Mappings**.
 - c. Click **Next** after mappings are created successfully.
 - d. Select the object used earlier to create reverse mapping and then click **Finish**.

Result

The Folder Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configure resource mappings

You should map your resources on the protected site and recovery site so that virtual machines are configured to fail over into one group of hosts or the other.

What you will need

You should have connected the protected and recovery sites.



In VMware Live Site Recovery, resources can be resource pools, ESXi hosts, or vSphere clusters.

Steps

1. Log in to vCenter Server and click on **Site Recovery > Sites**.
2. Select your protected site and click **Manage**.
3. In the Manage tab, select **Resource Mappings**.
4. Click **New** to create a new resource mapping.

The Create Resource Mapping wizard appears.

5. In the Create Resource Mapping wizard, perform the following:
 - a. Select **Automatically Prepare Mappings for Resource with Matching Names** and click **Next**.
 - b. Select the required data center objects for the protected and recovery sites and click **Add Mappings**.
 - c. Click **Next** after mappings are created successfully.
 - d. Select the object used earlier to create reverse mapping and then click **Finish**.

Result

The Resource Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configure placeholder datastores

You should configure a placeholder datastore to hold a place in the vCenter inventory at the recovery site for the protected virtual machine (VM). The placeholder datastore does not need to be large as the placeholder VMs are small and use only a few hundred or fewer kilobytes.

What you will need

- You should have connected the protected and recovery sites.
- You should have configured your resource mappings.

Steps

1. Log in to vCenter Server and click on **Site Recovery > Sites**.
2. Select your protected site and click **Manage**.
3. In the Manage tab, select **Placeholder Datastores**.
4. Click **New** to create a new placeholder datastore.
5. Select the appropriate datastore and click **OK**.



Placeholder datastores can be local or remote and should not be replicated.

6. Repeat steps 3 to 5 to configure a placeholder datastore for the recovery site.

Configure SRA using array manager

You can configure Storage Replication Adapter (SRA) by using the Array Manager wizard of VMware Live Site Recovery to enable interactions between VMware Live Site Recovery and storage virtual machines (SVMs).

What you will need

- You should have paired the protected sites and recovery sites in VMware Live Site Recovery.
- You should have configured your onboarded storage before configuring the array manager.
- You should have configured and replicated the SnapMirror relationships between the protected sites and recovery sites.
- You should have enabled the SVM management LIFs to enable multitenancy.

SRA supports cluster-level management and SVM-level management. If you add storage at a cluster level, then you can discover and perform operations on all the SVMs in the cluster. If you add storage at an SVM level, then you can manage only that specific SVM.

Steps

1. In VMware Live Site Recovery, click **Array Managers** and click **Add Array Manager**.
2. Enter the following information to describe the array in VMware Live Site Recovery:
 - a. Enter a name to identify the array manager in the **Display Name** field.
 - b. In the **SRA Type** field, select **NetApp Storage Replication Adapter for ONTAP**.
 - c. Enter the information to connect to the cluster or the SVM:
 - If you are connecting to a cluster, you should enter the cluster management LIF.
 - If you are connecting directly to an SVM, you should enter the IP address of the SVM management LIF.



When configuring the array manager, you should use the same connection (IP address) for the storage system that was used to onboard the storage system in ONTAP tools.

For example, if the array manager configuration is SVM scoped, then the storage under ONTAP tools for VMware vSphere should be added at SVM level.

- d. If you are connecting to a cluster, enter the name of the SVM in the **SVM name** field.

You can also leave this field blank.

- e. Enter the volumes to be discovered in the **Volume include list** field.

You can enter the source volume at the protected site and the replicated destination volume at the recovery site.

For example, if you want to discover volume src_vol1 that is in a SnapMirror relationship with volume

dst_vol1, you should specify src_vol1 in the protected site field and dst_vol1 in the recovery site field.

- f. **(Optional)** Enter the volumes to be excluded from discovery in the **Volume exclude list** field.

You can enter the source volume at the protected site and the replicated destination volume at the recovery site.

For example, if you want to exclude volume *src_vol1* that is in a SnapMirror relationship with volume *dst_vol1*, you should specify *src_vol1* in the protected site field and *dst_vol1* in the recovery site field.

3. Click **Next**.
4. Verify that the array is discovered and displayed at the bottom of the Add Array Manager window and click **Finish**.

You can follow the same steps for the recovery site by using the appropriate SVM management IP addresses and credentials. On the Enable Array Pairs screen of the Add Array Manager wizard, you should verify that the correct array pair is selected, and that it shows as ready to be enabled.

Verify replicated storage systems

You should verify that the protected site and recovery site are successfully paired after configuring Storage Replication Adapter (SRA). The replicated storage system should be discoverable by both the protected site and the recovery site.

What you will need

- You should have configured your storage system.
- You should have paired the protected site and recovery site by using the VMware Live Site Recovery array manager.
- You should have enabled FlexClone license and SnapMirror license before performing the test failover operation and failover operation for SRA.

Steps

1. Log in to your vCenter Server.
2. Navigate to **Site Recovery > Array Based Replication**.
3. Select the required Array Pair and verify the corresponding details.

The storage systems should be discovered at the protected site and recovery site with the Status as "Enabled".

Manage ONTAP tools

NetApp ONTAP tools for VMware vSphere plug-in Dashboard overview

When you select the NetApp ONTAP tools for VMware vSphere plug-in icon in the shortcuts section on the vCenter client, the user interface navigates to the overview page. This page acts like the dashboard providing you the summary of the ONTAP tools for VMware vSphere plug-in.

In the case of Enhanced Linked Mode setup (ELM), the vCenter Server select dropdown appears and you can select a desired vCenter Server to see the data relevant to it. This dropdown is available for all the other listing views of the plugin.

vCenter Server selection made in one page persists across the tabs of the plug-in.

vmw vSphere Client Menu Search in all environments

NetApp ONTAP Tools INSTANCE 10.224.132.8444

Overview vCenter server: 172.21.104.101

6 Storage backends

Unhealthy

VASA provider **Online**

[other vasa provider states](#)

Storage backends - capacity

197.3 GB USED AND RESERVED 481.69 GB PHYSICAL AVAILABLE

[VIEW ALL STORAGE BACKENDS \(6\)](#)

Virtual machines

Name	vCenter VM latency	vCenter VM committed capacity	Max datastore latency	Total datastore IOPS	Avg datastore throughput
AE-WEB-APSG-P01	176 ms	33 GB	176 ms	33 k	62 MB/s
AE-WEB-AUD-P01	168 ms	10 GB	168 ms	10 k	96 MB/s
ib-sne-vnx-p01	162 ms	6 GB	162 ms	6 k	180 MB/s
AE-VESTA3	151 ms	11 GB	151 ms	11 k	354 MB/s
AE-VMware1-Network-AAEF0038	75 ms	19 GB	75 ms	19 k	106 MB/s
AE-WEB-APSG-P03	73 ms	40 GB	73 ms	40 k	62 MB/s
AE-WEB-AUD-P07	68 ms	8 GB	68 ms	8 k	96 MB/s
ib-sne-vnx-p04	66 ms	16 GB	66 ms	16 k	180 MB/s
AE-VESTA9	65 ms	24 GB	65 ms	24 k	354 MB/s
AE-VMware1-Network-AAEF0038	63 ms	12 GB	63 ms	12 k	106 MB/s

[VIEW ALL VIRTUAL MACHINES \(318\)](#)

Datstores Datastore type: All

Name	Space utilized (Top 10↓)	IOPS	Latency	Throughput	Storage VM	Type
datastore01	98%	33 k	176 ms	200	storage_vm_01	NFS
datastore02_long_name	83%	10 k	168 ms	300	svm_02	NFS
datastore03	72%	6 k	162 ms	200	storage_vm_03_long_name	VVols
datastore04	68%	11 k	151 ms	300	storage_vm_04	VMFS
datastore05_long_name	61%	19 k	75 ms	500	storage_vm_05	NFS
datastore06	55%	40 k	73 ms	200	storage_vm_06_long_name	VVols
datastore07	45%	8 k	68 ms	200	storage_vm_07	VMFS
datastore08	36%	16 k	66 ms	500	storage_vm_08	NFS
datastore09	27%	24 k	65 ms	300	storage_vm_09	VMFS
datastore10_very_long_name	12%	12 k	63 ms	500	storage_vm_10_long_name	NFS

[VIEW ALL DATASTORES \(54\)](#)

ESXi host compliance

NFS **Issues (15)** **Unknown (7)** **Compliant (27)**

MPIO **Issues (15)** **Unknown (7)** **Compliant (27)**

[APPLY RECOMMENDED SETTINGS](#) [VIEW ALL HOSTS \(49\)](#)

The dashboard has several cards showing different elements of the system. The following table shows the

different cards and what they represent.

Card name	Description
Status	<p>The Status card shows the number of storage backends added and the overall health status of storage backends and VASA Provider status of a vCenter.</p> <p>Storage backends status shows as "Healthy" when all the storage backends status is normal. Storage backends status shows as "Unhealthy" if any one of the storage backends have an issue (Unknown/Unreachable/Degraded status).</p> <p>When you click on the "Unhealthy" status, a tool tip opens with the status of the storage backends. You can click on any storage backend for more details.</p> <p>Other VASA Provider (VP) states link shows the current state of the VP that is registered in the vCenter Server.</p>
Storage Backends - Capacity	<p>This card shows the aggregated used and available capacity of all storage backends for the selected vCenter Server instance.</p>
Virtual machines	<p>This card shows the top 10 VMs sorted by performance metric. You can click on the header to get the top 10 VMs for the selected metric sorted by either ascending or descending order. The sorting and filtering changes made on the card persists until you change or clear the browser cache.</p>
Datastores	<p>This card shows the Top 10 datastores sorted by a performance metric. You can click on the header to get the top 10 datastores for the selected metric sorted by either ascending or descending order. The sorting and filtering changes made on the card persists until you change or clear the browser cache. There is a Datastore type drop-down to select the type of the datastores - NFS, VMFS, or vVols.</p>
ESXi Host compliance card	<p>This card shows overall compliance status of all ESXi Hosts (for the selected vCenter) settings with respect to the recommended NetApp host settings by settings group/category. You can click on Apply Recommended Settings link to apply the recommended settings. You can click on issues/unknown to see the list of hosts.</p>

Manage datastores

Create a datastore

When you create a datastore at host cluster level, the datastore is created and mounted on all the hosts of the destination and the action is enabled only if the current user has privilege to execute.

The create Datastore action wizard supports creation of NFS, VMFS, and vVols datastore.

- You can create only VMFS datastores on a protected cluster. When you add a VMFS datastore to a protected cluster, the datastore becomes protected automatically.
- You cannot create a datastore on a datacenter that has one or more protected host clusters.
- You cannot create a datastore at host if the parent host cluster is protected with a relationship of Automated Failover Duplex policy type (uniform/non-uniform config).
- You can create a VMFS datastore on a host, only when it has an async relationship.

Create a vVols datastore

You can create a vVols datastore with either new volumes or existing volumes. You cannot create vVols datastore with the mix of existing and new volumes.



Check to ensure root aggregates are not mapped to SVM.

Before you begin

Ensure that VASA provider is registered with the selected vCenter.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. Right-click a host system or a host cluster or a datacenter and select **NetApp ONTAP tools > Create Datastore**.
3. In the **Type** pane, select vVols in **Datastore Type**.
4. In the **Name and Protocol** pane, provide **Datastore name** and **Protocol** information.
5. In the **Storage** pane, select **Platform** and **storage VM**. In the **Advanced options** section, select custom export policy (for NFS protocol) or custom initiator group name (for iSCSI and FC protocol) as applicable.
 - Platform and asymmetric options help you to filter out the SVMs dropdown options. You should select the SVM to create or use the volume(s) for datastore creation.
 - The **Asymmetric** toggle button is visible only if iSCSI was selected in the previous step and performance or capacity is selected in the platform drop-down.
 - Select the **Asymmetric** toggle button for AFF platform and disable it for ASA platform.
6. In the **Storage attributes** pane, you can either create new volumes or use the existing volumes. When creating new volume, you can enable QoS on the datastore.
7. Review your selection in the **Summary** pane and click **Finish**.
The vVols Datastore is created and mounted on all the hosts.

Create an NFS datastore

A VMware Network File System (NFS) datastore uses the NFS protocol to connect ESXi hosts to a shared storage device over a network. NFS datastores are commonly used in VMware vSphere environments and offer several advantages, such as simplicity and flexibility.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. Right-click a Host System or a Host Cluster or a Datacenter and select **NetApp ONTAP tools > Create Datastore**.
3. In the **Type** pane, select NFS in **Datastore Type**.
4. In the **Name and Protocol** pane, enter datastore name, size, and protocol information. In the advanced options, select **Datastore cluster** and **Kerberos Authentication**.



Kerberos Authentication is available only when the NFS 4.1 protocol is selected.

5. In the **Storage** pane, select **Platform** and **Storage VM**. You can select **custom Export Policy** in the **Advanced Option** section.

- **Asymmetric** toggle button is visible only if performance or capacity is selected in the platform drop-down.
 - **Any** option in the platform dropdown enables you to see all the SVMs that are part of the vCenter irrespective of the platform or asymmetric flag.
6. In the **Storage Attributes** pane, select the aggregate for creation of volume. In the advanced options choose **Space Reserve** and **Enable QoS** as required.
 7. Review the selections in the **Summary** pane and click **Finish**.

The NFS datastore is created and mounted on all the hosts.

Create a VMFS datastore

Virtual Machine File System (VMFS) is a clustered file system specifically designed for storing virtual machine files in VMware vSphere environments. It allows multiple ESXi hosts to access the same virtual machine files concurrently, enabling features like vMotion and High Availability.

Before you begin

Check the following items before proceeding:

- For each protocol on ONTAP storage side, respective services and LIF's need to be enabled.
- If you are using the NVMe/TCP protocol, perform the following steps to configure the ESXi host:

1. Review the [VMware Compatibility Guide](#)



VMware vSphere 7.0 U3 and later versions support NVMe/TCP protocol. However, VMware vSphere 8.0 and later version is recommended.

2. Validate if the Network Interface Card (NIC) vendor supports ESXi NIC with NVMe/TCP protocol.
 3. Configure the ESXi NIC for NVMe/TCP according to the NIC vendor specifications.
 4. When using VMware vSphere 7 release, follow the instructions on the VMware site [Configure VMkernel Binding for the NVMe over TCP Adapter](#) to configure NVMe/TCP port binding. When using VMware vSphere 8 release, follow [Configuring NVMe over TCP on ESXi](#), to configure the NVMe/TCP port binding.
 5. For VMware vSphere 7 release, follow the instructions on the VMware site [Enable NVMe over RDMA or NVMe over TCP Software Adapters](#) to configure NVMe/TCP software adapters. For VMware vSphere 8 release, follow [Add Software NVMe over RDMA or NVMe over TCP Adapters](#) to configure the NVMe/TCP software adapters.
 6. Run [Discover storage systems and hosts](#) action on the ESXi host.
For more information, refer to [How to Configure NVMe/TCP with vSphere 8.0 Update 1 and ONTAP 9.13.1 for VMFS Datastores](#)
- If you are using the NVMe/FC protocol, perform the following steps to configure the ESXi host:
 1. Enable NVMe over Fabrics(NVMe-oF) on your ESXi host(s).
 2. Complete SCSI zoning.
 3. Ensure that ESXi hosts and the ONTAP system are connected at a physical and a logical layer.

To configure an ONTAP SVM for FC protocol, refer to [Configure an SVM for FC](#).

For more information on using NVMe/FC protocol with VMware vSphere 8.0, refer to [NVMe-oF Host Configuration for ESXi 8.x with ONTAP](#).

For more information on using NVMe/FC with VMware vSphere 7.0, refer to [ONTAP NVMe/FC Host Configuration guide](#) and [TR-4684](#).

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. Right-click a Host System or a Host Cluster or a Datastore and select **NetApp ONTAP tools > Create Datastore**.
3. In the **Type** pane, select VMFS in **Datastore Type**.
4. In the **Name and Protocol** pane, enter the datastore name, size, and protocol information. In the **Advanced options** section of the pane, select the Datastore cluster you want to add this datastore to.
5. Select Platform and storage VM in the **Storage** pane. Select the Asymmetric toggle button. Provide the **Custom initiator group name** in the **Advanced options** section of the pane (optional). You can either choose an existing igroup for the datastore or create a new igroup with a custom name.

If you choose the **Any** option in the platform dropdown you can see all the SVMs that are part of the vCenter irrespective of the platform or asymmetric flag.

When the protocol is selected as NVMe/FC or NVMe/TCP, a new namespace subsystem is created and is used for namespace mapping. By default, the namespace subsystem is created using the auto generated name that includes the datastore name. You can rename the namespace subsystem in the **custom namespace subsystem name** field in the advanced options of **Storage** pane.

6. From the **storage attributes** pane, select **Aggregate** from the drop-down menu. Select **Space Reserve**, **Use existing volume**, and **Enable QoS** options as required from the **Advanced options** section and provide the details as required.



For VMFS datastore creation with NVMe/FC or NVMe/TCP protocol you cannot use the existing volume, you should create new volume.

7. Review the datastore details in the **Summary** pane and click **Finish**.



If you're creating the datastore on a protected cluster, you can see a readonly message "The datastore is being mounted on a protected Cluster."
The VMFS datastore is created and mounted on all the hosts.

= Mount NFS and VMFS datastores

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

Mounting a datastore provides storage access to additional (NFS/VMFS) hosts. You can mount the datastore on the additional hosts after you add the hosts to your VMware environment.

- Some of the right click actions are disabled or unavailable depending on vSphere client versions and the type of datastore selected. If you're using vSphere client 8.0 or later versions, some of the right-click options are hidden.
- From vSphere 7.0U3 to vSphere 8.0 versions even though the options appear, the action will be disabled.
- Mount datastore is disabled when the host cluster is protected with uniform configurations.

Steps

1. From the vSphere Client home page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the host.
3. Repeat Step 2 for any additional hosts.
4. To mount NFS/VMFS datastores on host or host cluster, right-click on it and select **NetApp ONTAP tools > Mount Datastores**.
5. Select the datastores that you want to mount and click **Mount**.

You can track the progress in the Recent Task panel.

= Unmount NFS and VMFS datastores

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

Unmount datastore action unmounts a NFS or VMFS datastore from ESXi hosts. Unmount datastore action is enabled for NFS and VMFS datastores that are discovered or managed by the ONTAP tools for VMware vSphere.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. Right-click a NFS or VMFS datastore object and select **Unmount datastore**.

A dialog box opens and lists the ESXi hosts that the datastore is mounted on.

When the operation is performed on a protected datastore, a warning message is displayed on the screen.

3. Select one or more ESXi hosts to unmount the datastore.

You cannot unmount the datastore from all hosts. The UI suggests that you use the delete datastore operation instead.

4. Select the **Unmount** button.

If the datastore is part of a protected host cluster, a warning message is displayed.



If the protected datastore is unmounted the existing protection setting may result in partial protection. Refer to [Modify protected host cluster](#) to enable complete protection.

You can track the progress in the Recent Task panel.

= Mount a vVols datastore

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

You can mount a VMware Virtual Volumes (vVols) datastore to one or more additional hosts to provide storage access to additional hosts. You can unmount vVols datastore

only through the APIs.

Steps

1. From the vSphere Client home page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the datastore.
3. Right-click the datastore and select **NetApp ONTAP tools > Mount datastore**.
4. In the **Mount datastores on Hosts** dialog box, select the hosts on which you want to mount the datastore, and then click **Mount**.

You can track the progress in the Recent Task panel.

= Resize NFS and VMFS datastore

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

Resizing a datastore enables you to increase the storage for your virtual machine files. You can change the size of a datastore as your infrastructure requirements change.

About this task

You can only increase the size of an NFS and VMFS datastores. A FlexVol volume that is part of a NFS and VMFS datastores cannot shrink below the existing size but can grow by 120% maximum.

Steps

1. From the vSphere Client home page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the datastore.
3. Right-click the NFS or VMFS datastore and select **NetApp ONTAP tools > Resize datastore**.
4. In the Resize dialog box, specify a new size for the datastore and click **OK**.

= Expand vVols Datastore

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

When you right click on datastore object in the vCenter object view, ONTAP tools for VMware vSphere supported actions are shown under the plug-in section. Specific actions are enabled depending on the type of datastore and the current user privileges.

Steps

1. From the vSphere Client home page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the datastore.
3. Right-click the datastore and select **NetApp ONTAP tools > Add storage to datastore**.
4. In the **create or Select Volumes** window, you can either create new volumes or choose from the

existing volumes. The UI is self-explanatory. Follow the instructions as per your choice.

5. In the **Summary** window, review the selections and click **Expand**.
You can track the progress in the Recent Tasks panel.

= Shrink vVols datastore

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

Delete datastore action deletes the datastore when there are no vVols on the selected datastore.

Steps

1. From the vSphere Client home page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the datastore.
3. Right click on the vVol datastore and select **NetApp ONTAP tools > Remove storage from datastore**.
4. Select volumes which do not have vVols and click **Remove**.



The option to select the volume on which the vVols is residing is disabled.

5. In the **Remove storage** pop-up, select **Delete volumes from ONTAP cluster** checkbox to delete the volumes from datastore and from ONTAP storage and click **Delete**.

= Delete datastores

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

Remove storage from datastore action is supported on all ONTAP tools for VMware vSphere discovered or managed vVols datastores in the vCenter Server. This action allows the removal of volumes from the vVols datastore.

The remove option is disabled when there are vVols residing on a particular volume. In addition to removing volumes from datastore, you can delete the selected volume on ONTAP storage.

Delete datastore task from ONTAP tools for VMware vSphere in the vCenter Server does the following:

- Unmounts the vVol container.
- Cleans up igroup. If igroup is not in use, removes iqn from igroup.
- Deletes Vvol container.
- Leaves the Flex volumes on the storage array.

Follow the steps below to delete NFS, VMFS, or vVOL datastore from ONTAP tools from the vCenter Server:

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. Right-click a Host System or a Host Cluster or a Datastore and select **NetApp ONTAP tools > Delete**

datastore.



You cannot delete the datastores if there are virtual machines using that datastore. You need to move the virtual machines to a different datastore before deleting the datastore. You cannot select Volume delete checkbox if the datastore belongs to a protected host cluster.

- a. In the case of NFS or VMFS datastore a dialog box appears with the list of VMs that are using the datastore.
 - b. In the case of vVols datastore, Delete datastore action deletes the datastore only when there are no vVols associated with it. The Delete datastore dialog box provides an option to delete volumes from ONTAP cluster.
3. To delete the backing volumes on ONTAP storage, select **Delete volumes on ONTAP cluster**.



You cannot delete the volume on ONTAP cluster for a VMFS datastore that is part of the protected host cluster.

= ONTAP storage views for datastores

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

ONTAP storage view under configure tab of ONTAP tools for VMware vSphere provides data related to the datastores and their volume. This view provides the storage side view of the datastore.

== ONTAP storage views for NFS datastores

Steps

1. From the vSphere Client navigate to the NFS datastore.
2. Click the **Configure** tab in the right pane.
3. Select **NetApp ONTAP tools > ONTAP Storage**. The **Storage details** and **NFS details** appear on the right pane.
 - The storage details page contains information about storage backends, aggregate, and volume.
 - The NFS details page contains data related to the NFS datastore.

== ONTAP storage views for VMFS datastores

.Steps

1. From the vSphere Client navigate to the VMFS datastore.
2. Click the **Configure** tab in the right pane.
3. Select **NetApp ONTAP tools > ONTAP Storage**. The **Storage details** and **LUN details** or **Namespace details** in case of NVMe/TCP or NVMe/FC protocol appear on the right pane.
 - The storage details page contains information about storage backends, aggregate, and volume.
 - The LUN details page contains data related to the LUN.
 - When using NVMe/TCP or NVMe/FC protocol for VMFS datastore, the Namespace details page contains data related to Namespace.

== ONTAP storage views for vVols datastores

.Steps

1. From the vSphere Client navigate to the vVols datastore.
2. Click the **Configure** tab in the right pane.
3. Select **NetApp ONTAP tools > ONTAP Storage**.
4. The ONTAP storage view lists all the volumes. You can expand or remove storage from the ONTAP storage pane.

Follow the instructions in [Expand vVols Datastore](#) section to add vVols datastore and [Shrink vVols datastore](#) section to delete the datastore.

= Virtual machine storage view

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

The storage view shows the list of vVols that are created by the virtual machine.



This view is applicable for the VM which has at least one ONTAP tools for VMware vSphere managed vVols datastore related disk mounted on it.

Steps

1. From the vSphere Client navigate to the virtual machine.
2. Click the **Monitor** tab in the right pane.
3. Select **NetApp ONTAP tools > Storage**. The **Storage** details appear on the right pane. You can see the list of vVols that are present on the VM.

You can use the 'Manage Columns' option to hide or show different columns.

= Manage storage thresholds

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

You can set the threshold to receive notifications in vCenter Server when the volume and the aggregate capacity reaches certain levels.

Steps:

1. Log in to the vSphere client using `https://vcenterip/ui`
2. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Settings > Threshold Settings > Edit**.
4. In the **Edit Threshold** window, provide the desired values in the **Nearly Full** and **Full** fields and click Save.

You can reset the numbers to recommended values, which is 80 for Nearly full and 90 for full.

= Manage storage backends

:icons: font

```
:relative_path: ./manage/  
:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/
```

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

== Discover storage

You can run the discovery of a storage backend on demand without waiting for a scheduled discovery to update the storage details.

Follow the steps below to discover the storage backends.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Storage Backends** and select a storage backend.
4. Click on the vertical ellipses menu and select **Discover storage**

You can track the progress in the Recent Tasks panel.

== Modify storage backends

Follow the steps in this section to modify a storage backend.

1. Log in to the vSphere client using `https://vcenterip/ui`
2. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Storage Backends** and select a storage backend.
4. Click on the vertical ellipses menu and select **Modify** to modify the credentials or the port name.
You can track the progress in the Recent Tasks panel.

You can perform the Modify operation for global ONTAP clusters using ONTAP tools Manager using the following steps.

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select storage backends from the sidebar.
4. Select the Storage Backend you want to modify.
5. Click on the vertical ellipses menu and select **Modify**.
6. You can modify the credentials or the port. Enter the **Username** and **Password** to modify the storage backend.

== Remove storage backends

You need to delete all the datastores attached to the storage backend before removing the storage backend.

Follow the steps below to remove a storage backend.

1. Log in to the vSphere client using `https://vcenterip/ui`

2. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, navigate to **Storage Backends** and select a storage backend.
4. Click on the vertical ellipses menu and select **Remove**. Ensure that the storage backend does not contain any datastores.
You can track the progress in the Recent Tasks panel.

You can perform the remove operation for global ONTAP clusters using ONTAP tools Manager.

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Storage Backends** from the sidebar.
4. Select the storage backend you want to remove
5. Click on the vertical ellipses menu and select **Remove**.

== Drill down view of storage backend

The storage backend page lists all the storage backends. You can perform discover storage, modify, and remove operations on the storage backends you added and not the individual child under the cluster.

When you click on either the parent cluster or the child under the storage backend, you can see the overall summary of the component. When you click on the parent cluster you have the actions dropdown from which you can perform the discover storage, modify, and remove operations. This option is missing when you click on the child SVM.

The summary page provides the following details:

- Status of the storage backend
- Capacity information
- Basic information about the VM
- Network information like the IP address and port of the network. For the child SVM, the information will be same as the parent storage backend.
- Privileges allowed and restricted for the storage backend. For the child SVM, the information will be same as the parent storage backend. Privileges are shown only on the cluster-based storage backends. If you add SVM as the storage backend, privileges information will not be shown.

The Interface tab provides detailed information about the interface.

The Local Tiers tab provides detailed information about the aggregate list.

= Manage vCenter Server instances

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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

== Associate or dissociate storage backends with vCenter Server instance

The vCenter Server listing page shows the associated number of storage backends. Each vCenter Server instance has the option to associate or disassociate a storage backend.

This task helps you to create mapping between storage backend and onboarded vCenter Server instance globally.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the required vCenter Server instance from the sidebar.
4. Click on the vertical ellipses against the vCenter Server that you want to associate or dissociate with storage backends.
5. Select **Associate or Dissociate storage backend** depending on what action you want to perform.

== Modify a vCenter Server instance

Follow the steps below to modify a vCenter Server instances.

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the applicable vCenter Server instance from the sidebar
4. Click on the vertical ellipses against the vCenter Server that you want to modify and select **Modify**.
5. Modify the vCenter Server instance details and select **Modify**.

== Remove a vCenter Server instance

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

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the applicable vCenter Server instances from the sidebar
4. Click on the vertical ellipses against the vCenter Server that you want remove and select **Remove**.



Once you remove vCenter Server instances, they will no longer be maintained by the application.

When you remove vCenter Server instances in ONTAP tools, the following actions are performed automatically:

- Plug-in is unregistered.
- Plug-in privileges and plug-in roles are removed.

= Manage certificates

:icons: font


```
:relative_path: ./manage/  
:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/
```

A single instance of ONTAP tools for VMware vSphere can manage multiple vCenter Server instances. ONTAP tools for VMware vSphere is deployed with a self-signed certificate for VASA Provider. With this, only one vCenter Server instance can be managed for vVols datastores. When you're managing multiple vCenter Server instances and you want to enable vVols capability on multiple vCenter Server instances, you need to change the self-signed certificate to custom CA certificate using ONTAP tools Manager interface. You can use the same interface to renew or refresh all certificates.



A different load balancer IP address mapped to different domains is not supported when you upgrade self-signed to custom CA.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Certificates** > **VASA provider** > **Renew** option to renew the certificates.



The system will be offline till the certificate is renewed.

4. To upgrade the self-signed certificate to custom CA certificate, select **Certificates** > **VASA provider** > **Upgrade to CA** option.
 - a. In the **Upgrade certificate to custom CA** pop-up, upload the server certificate, server certificate private key, root CA certificate, and intermediate certificate files. The tool tip provides description of the certificates.
 - b. Enter the domain name for which you generated this certificate.
 - c. Click **Upgrade**.



The system will be offline till the upgrade is complete.

= Manage igroups and export policies

```
:icons: font
```

```
:relative_path: ./manage/
```

```
:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/
```

In ONTAP, export policies are used to provide volume data path access to hosts and initiator groups (igroups) are used to provide logical unit number (LUN) data path access to ESXi hosts. ONTAP tools for VMware vSphere makes igroup creation easy and intuitive and provides rich end-to-end workflows. To ensure consistency, direct iGroup creation on storage platforms is not supported.

When virtual volume datastores are created or mounted to hosts in vCenter Server, the hosts need to be

given access to volumes (NFS) or LUNs (iSCSI) depending on the protocol type of the datastore.

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

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

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

= Access ONTAP tools for VMware vSphere maintenance console

= Overview of ONTAP tools for VMware vSphere maintenance console

:icons: font

:relative_path: ./manage/


:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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

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



You should set a password for the `diag` user while enabling remote diagnostics.

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

Console Menu	Options
Application Configuration	<ol style="list-style-type: none">1. Display server status summary2. Change LOG level for VASA Provider Services and SRA Services3. Disable AutoSupport

System Configuration	<ol style="list-style-type: none"> 1. Reboot virtual machine 2. Shutdown virtual machine 3. Change 'maint' user password 4. Change time zone 5. Add new NTP server 6. Increase jail disk size (/jail) 7. Upgrade 8. Install VMware Tools
Network Configuration	<ol style="list-style-type: none"> 1. Display IP address settings 2. Display domain name search settings 3. Change domain name search settings 4. Display static routes 5. Change static routes 6. Commit changes 7. Ping a host 8. Restore default settings
Support and Diagnostics	<ol style="list-style-type: none"> 1. Access diagnostic shell 2. Enable remote diagnostic access

= Configure remote diagnostic access

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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

What you will need

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

About this task

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

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

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

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

Steps

1. From vCenter Server, open a console to VASA Provider.
2. Log in as the maintenance user.
3. Enter 4 to select Support and Diagnostics.
4. Enter 2 to select Enable remote diagnostics access.
5. Enter `y` in the Confirmation dialog box to enable remote diagnostic access.
6. Enter a password for remote diagnostic access.

= Start SSH on other nodes

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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

What you will need

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

About this task

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

Steps

1. From vCenter Server, open a console to VASA Provider.
2. Log in as the maintenance user.
3. Enter 4 to select Support and Diagnostics.
4. Enter 1 to select Access diagnostic shell.
5. Enter `y` to proceed.
6. Run the command `sudo systemctl restart ssh`.

= Update the vCenter Server and ONTAP credentials

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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

What you will need

You need to have maintenance user login credentials.

About this task

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

Steps

1. From vCenter Server, open a console to VASA Provider.
2. Log in as the maintenance user.
3. Enter 2 to select System Configuration Menu.
4. Enter 9 to change ONTAP credentials.
5. Enter 10 to change vCenter credentials.

= ONTAP tool reports

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

ONTAP tools for VMware vSphere plug-in provides reports for virtual machines and datastores.

When you select the NetApp ONTAP tools for VMware vSphere plug-in icon in the shortcuts section on the vCenter client, the user interface navigates to the Overview page.

Select the Reports tab to view the virtual machine and the datastores report.

The virtual Machines report shows the list of discovered virtual machines (should have at least one disk from ONTAP storage based datastores) with performance metrics.

When you expand the VM record, all the disk related datastore info is displayed.

Datastores report shows the list of discovered or recognized ONTAP tools for VMware vSphere managed Datastores that are provisioned from ONTAP storage backend of all types with performance metrics.

You can use the Manage Columns option to hide or show different columns.

= Collect the log files

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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 vCenter client UI are scoped for the selected vCenter Server.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP: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 UI:

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`

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 may take some time.



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

= Manage virtual machines

= Considerations to migrate or clone virtual machines

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

You should be aware of some of the considerations while migrating existing virtual machines in your datacenter.

== Migrate protected virtual machines

You can migrate the protected virtual machines to:

- Same vVols datastore in a different ESXi host
- Different compatible vVols datastore in same ESXi host
- Different compatible vVols datastore in a different ESXi host

If the virtual machine is migrated to a different FlexVol volume, then the respective metadata file also gets updated with the virtual machine information. If a virtual machine is migrated to a different ESXi host but same storage, then underlying FlexVol volume metadata file will not be modified.

== Clone protected virtual machines

You can clone protected virtual machines to the following:

- Same container of same FlexVol volume using replication group

Same FlexVol volume's metadata file is updated with the cloned virtual machine details.

- Same container of a different FlexVol volume using replication group

The FlexVol volume where the cloned virtual machine is placed, the metadata file gets updated with the cloned virtual machine details.

- Different container or vVols datastore

The FlexVol volume where the cloned virtual machine is placed, the metadata file gets updated virtual machine details.

VMware presently does not support virtual machines cloned to a VM template.

Clone-of-Clone of a protected virtual machine is supported.

== Virtual Machine Snapshots

Presently only virtual machine Snapshots without memory are supported. If virtual machine has Snapshot with memory, then the virtual machine is not considered for protection.

You also cannot protect unprotected virtual machines that have memory Snapshot. For this release, you are expected to delete memory snapshot before enabling protection for the virtual machine.

= Migrate virtual machines with NFS and VMFS datastores to vVols datastores

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

You can migrate virtual machines from NFS and VMFS datastores to Virtual Volumes (vVols) datastores to take advantage of policy-based VM management and other vVols capabilities. vVols datastores enable you to meet increased workload requirements.

What you will need

Ensure that VASA Provider is not running on any of the virtual machines that you plan to migrate. If you migrate a virtual machine that is running VASA Provider to a vVols datastore, you cannot perform any management operations, including powering on the virtual machines that are on vVols datastores.

About this task

When you migrate from a NFS and VMFS datastore to a vVols datastore, the vCenter Server uses vStorage APIs for Array Integration (VAAI) offloads when moving data from VMFS datastores, but not from an NFS VMDK file. VAAI offloads normally reduce the load on the host.

Steps

1. Right-click the virtual machine that you want to migrate and click **Migrate**.
2. Select **Change storage only** and then click **Next**.
3. Select a virtual disk format, a VM Storage Policy, and a vVol datastore that matches the features of the datastore that you are migrating. Click **Next**.
4. Review the settings and click **Finish**.

= VASA cleanup

:icons: font

```
:relative_path: ./manage/  
:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/
```

Use the steps in this section to perform VASA cleanup.



It is recommended that you remove any vVols datastores before performing the VASA Cleanup.

Steps

1. Unregister the plug-in by going into https://OTV_IP:8143/Register.html
2. Verify that the plug-in is no longer available on the vCenter Server.
3. Shut down ONTAP tools for VMware vSphere VM.
4. Delete ONTAP tools for VMware vSphere VM.

= Discover storage systems and hosts

```
:icons: font
```

```
:relative_path: ./configure/
```

```
:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/
```

When you first run ONTAP tools for VMware vSphere in a vSphere Client, ONTAP tools discovers the ESXi hosts, their LUNs and NFS exports, and the NetApp storage systems that own those LUNs and exports.

What you will need

- All the ESXi hosts should be powered on and connected.
- All the storage virtual machines (SVMs) to be discovered should be running, and each cluster node should have at least one data LIF configured for the storage protocol in use (NFS or iSCSI).

About this task

You can discover new storage systems or update information about existing storage systems to obtain the latest capacity and configuration information at any time. You can also modify the credentials that ONTAP tools for VMware vSphere uses to log in to the storage systems.

While discovering the storage systems, ONTAP tools for VMware vSphere collects information from the ESXi hosts that are managed by the vCenter Server instance.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. Right-click the required datacenter and select **NetApp ONTAP tools > Update Host Data**.

ONTAP tools for VMware vSphere displays a **Confirm** dialog box with the following message:

"This action will restart the discovery of all connected storage systems and might take a few minutes. Do you want to continue?"

3. Click **Yes**.
4. Select the discovered storage controllers that have the status `Authentication Failure` and click

Actions > Modify.

5. Fill in the required information in the **Modify Storage System** dialog box.
6. Repeat steps 4 and 5 for all storage controllers with `Authentication Failure` status.

After the discovery process is complete, perform the following actions:

- Use ONTAP tools for VMware vSphere to configure ESXi host settings for hosts that display the Alert icon in the Adapter Settings column, the MPIO Settings column, or the NFS Settings column.
- Provide the storage system credentials.

= Modify ESXi host settings using ONTAP tools

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

You can use the dashboard of ONTAP tools for VMware vSphere to edit your ESXi host settings.

What you will need

If there is an issue with your ESXi host settings, the issue is displayed in the ESXi host systems portlet of the dashboard. You can click the issue to view the host name or the IP address of the ESXi host that has the issue.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. In the shortcuts page, click on **NetApp ONTAP tools** under the plug-ins section.
3. Go to **ESXi Host compliance** portlet in the Overview (Dashboard) of the ONTAP tools for VMware vSphere plug-in.
4. Select **Apply Recommended Settings** link.
5. In the **Apply recommended host settings** window, select the hosts that you want to comply with NetApp recommended host settings and click **Next**.



You can expand the ESXi host to see the current values.

6. In the settings page, select the recommended values as required.
7. In the summary pane, check the values and click **Finish**.
You can track the progress in the Recent task panel.

= Manage passwords

= Change ONTAP tools Manager password

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

You can change the administrator password using ONTAP tools Manager.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Click on the **administrator** icon on the top right corner of the screen and select **Change password**.
4. In the change password pop-up window, enter the old password and the new password details. The constraint for changing the password is displayed on the UI screen.
5. Click **Change** to implement the changes.

= Reset ONTAP tools Manager password

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

If you've forgotten the ONTAP tools Manager password, you can reset the administrator credentials using the token generated by ONTAP tools for VMware vSphere maintenance console.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. On the login screen, select **Reset password** option.

To reset the Manager password, you need to generate the reset token using the ONTAP tools for VMware vSphere maintenance console.

- .. From vCenter Server, open the maintenance console
- .. Enter '2' to select System Configuration option
- .. Enter '3' to Change 'maint' user password.

3. In the change password pop-up window, enter the password reset token, username, and the new password details.
4. Click **Reset** to implement the changes.
On successful password reset, you can use new password to log in.

= Reset application user password

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

The application user password is used for SRA and VASA provider registration with vCenter Server.

Steps

1. Launch ONTAP tools Manager from a web browser:
`https://loadBalanceIP:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.

3. Click on **Settings** from the sidebar.
4. In the **Application user credentials** screen, select **Reset password**.
5. Provide username, new password and confirm new password inputs.
6. Click **Reset** to implement the changes.

= Reset maintenance console user password

:icons: font

:relative_path: ./manage/

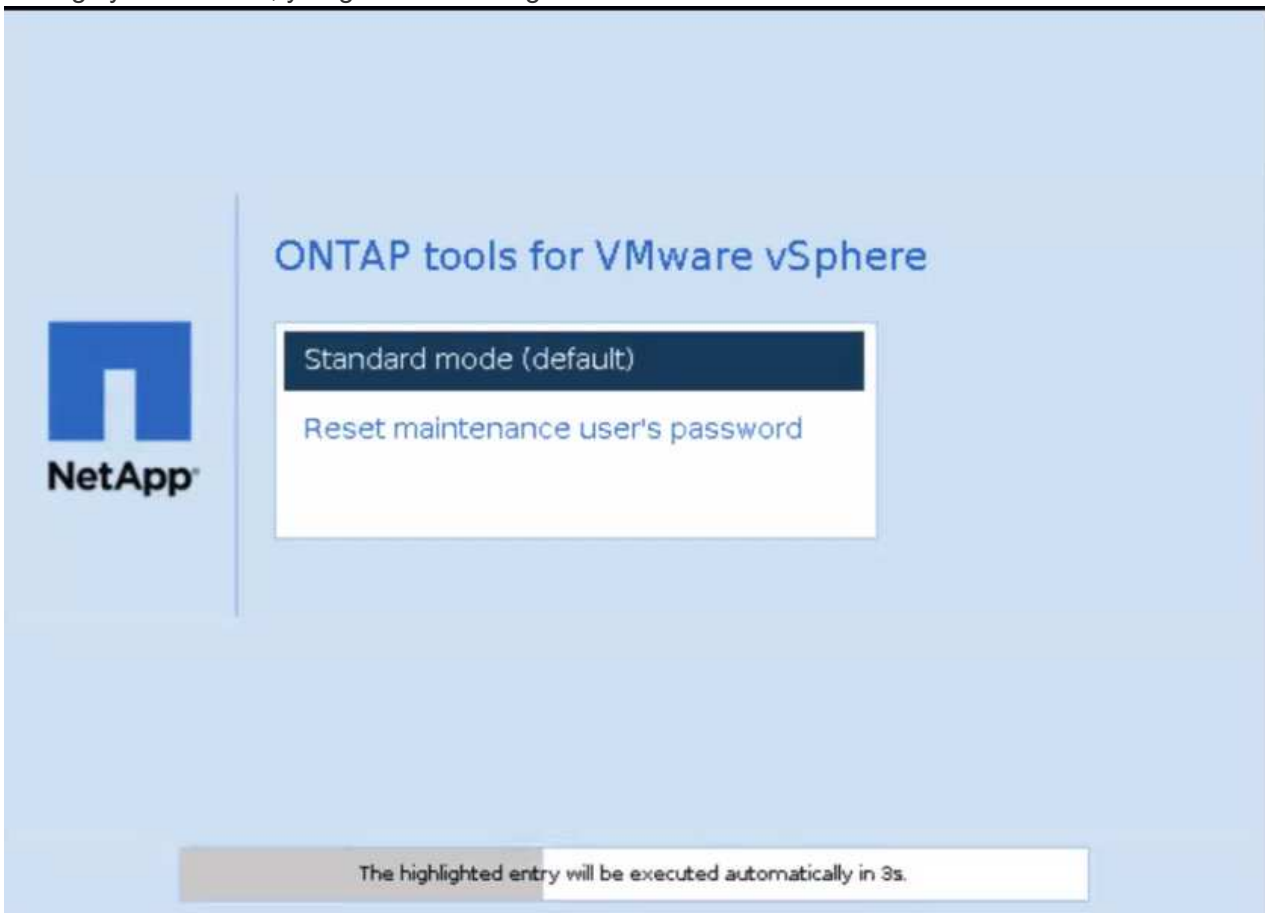
:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

During guest OS restart operation, grub menu displays an option to reset maintenance console user password.

This option is used to update the maintenance console user password present on the corresponding VM. Once the reset password is complete, the VM restarts to set the new password. In HA deployment scenario, after the VM restart, the password is automatically updated on the other two VMs.

Steps

1. Log in to your vCenter Server
2. Right-click on the VM and select **Power > Restart Guest OS**
During system restart, you get the following screen:



You have 5 seconds to choose your option. Press any key to stop the progress and freeze the GRUB menu.

3. Select **Reset maintenance user's password** option. The maintenance console opens.
4. In the console, enter the new password details. New password and retype new password details should match to successfully reset the password. You have three chances to enter the correct password. The system restarts after successfully entering the new password.
5. Press Enter to continue.
The password is updated on the VM.



The same GRUB menu comes up during power on of the VM as well. However, you should use the reset password option only with **Restart Guest OS** option.

= Clean up volumes

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

After deleting ONTAP tools for VMware vSphere deployment, you should clean up the FlexVolumes created during the deployment. If you have used a dedicated ONTAP cluster for deployments, you should clean up the FlexVolumes as the deployment creates lot of FlexVolumes which are unused resulting in lowered performance.

Use the following guidelines to clean up the FlexVolumes post removal of ONTAP tools for VMware vSphere deployment.

Steps

1. From the primary node VM of ONTAP tools for VMware vSphere, run the following command to identify the type of deployment.

```
cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol
```

If it is an iSCSI deployment, then you need to delete igroups as well.

2. Fetch the list of FlexVolumes created in ONTAP during the deployment using the following command.

```
kubectl describe persistentvolumes | grep internalName | awk -F=' ' '{print $2}'
```

3. Delete VMs from vCenter Server, see [Remove VMs or VM Templates from vCenter Server or from the Datastore](#)
4. Delete volumes from ONTAP system manager, see [Delete a FlexVol volume](#). Give the exact name of the FlexVolume in the cli command to delete the volume.
5. In case of iSCSI deployment, delete SAN igroups from ONTAP, see [View and manage SAN initiators and igroups](#).

In HA deployment, four igroups are created and in non-HA deployment two igroups are created. Run the following command to find the first igroup name:

```
kubectl -n trident get tbc trident-backend -o yaml | grep igroupName: | awk -F:' ' '{print $2}'
```

The other igroup names start with the hostname of the VM.

= Manage host cluster protection

= Modify protected host cluster

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

You can perform the following tasks as part of modify protection. You can perform all the changes in the same workflow.

- Add new datastores or hosts to the protected cluster.
- Add new SnapMirror relationships to the protection settings.
- Delete existing SnapMirror relationships from the protection settings.
- Modify an existing SnapMirror relationship.

== Monitor host cluster protection

Use this procedure to monitor the status of the host cluster protection. You can monitor every protected host cluster along with its protection state, SnapMirror relationships, datastores, and the corresponding SnapMirror status.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. Navigate to **NetApp ONTAP tools > Protection > Host cluster relationships**.

The icon under the protection column shows the status of the protection

3. Hover over the icon to see more details.

== Add new datastores or hosts

Use this procedure to protect the newly added datastores or hosts. You can add new hosts to the protected cluster or create new datastores on host cluster using the vCenter native user interface.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. To edit the properties of a protected cluster, you can either
 - a. Navigate to **NetApp ONTAP tools > Protection > Host cluster relationships**, click on the kebab menu against the cluster and select **Edit** or
 - b. Right-click a host cluster and select **NetApp ONTAP tools > Protect Cluster**.
3. If you have created a datastore in vCenter native user interface, then that datastore is shown as unprotected. The user interface shows all datastores in the cluster and their protection status in a dialog box. Select **Protect** button to enable complete protection.
4. If you have added a new ESXi host, the protection status shows as partially protected. Select the kebab menu under the SnapMirror settings and select **Edit** to set the proximity of the newly added ESXi host.



In case of Asynchronous type relationship, edit action is not supported as you cannot add the target SVM for tertiary site to the same ONTAP tools instance. However, you can use the system manager or CLI of the target SVM to change the relationship configuration.

5. Click **Save** after making the necessary changes.
6. You can see the changes in the **Protect Cluster** window.

A vCenter task is created and you can track the progress in the **Recent task** panel.

== Add a new SnapMirror relationship

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. To edit the properties of a protected cluster, you can either
 - a. Navigate to **NetApp ONTAP tools > Protection > Host cluster relationships**, click on the kebab menu against the cluster and select **Edit** or
 - b. Right-click a host cluster and select **NetApp ONTAP tools > Protect Cluster**.
3. Select **Add relationship**.
4. Add new relationship as either **Asynchronous** or **AutomatedFailOverDuplex** policy type.
5. Click **Protect**.
6. You can see the changes in the **Protect Cluster** window.

A vCenter task is created and you can track the progress in the **Recent task** panel.

== Delete an existing SnapMirror relationship

To delete an asynchronous SnapMirror relationship, secondary site SVM or cluster should be added as storage backend on ONTAP tools for VMware vSphere.

You cannot delete all the SnapMirror relationships. When you delete a relationship, respective relationship on ONTAP cluster is also removed.

When you delete an AutomatedFailOverDuplex SnapMirror relationship, the datastores on the destination are unmapped and consistency group, LUNs, volumes, and igroups are removed from the destination ONTAP cluster.

Deleting the relationship triggers a rescan on secondary site to remove the unmapped LUN as active path from the hosts.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. To edit the properties of a protected cluster, you can either
 - a. Navigate to **NetApp ONTAP tools > Protection > Host cluster relationships**, click on the kebab menu against the cluster and select **Edit** or
 - b. Right-click a host cluster and select **NetApp ONTAP tools > Protect Cluster**.
3. Select the kebab menu under the SnapMirror settings and select **Delete**.

A vCenter task is created and you can track the progress in the **Recent task** panel.

== Modify an existing SnapMirror relationship

To modify an asynchronous SnapMirror relationship, secondary site SVM or cluster should be added as storage backend on ONTAP tools for VMware vSphere.

If it is an AutomatedFailOverDuplex SnapMirror relationship, you can modify the host proximity in case of uniform configuration and the host access in case of non-uniform configuration.

You cannot interchange Asynchronous and AutomatedFailOverDuplex policy types.

You can set the proximity or access for the newly discovered hosts on the cluster.



You cannot edit an existing asynchronous SnapMirror relationship.

Steps

1. Log in to the vSphere client using `https://vcenterip/ui`
2. To edit the properties of a protected cluster, you can either
 - a. Navigate to **NetApp ONTAP tools > Protection > Host cluster relationships**, click on the kebab menu against the cluster and select **Edit** or
 - b. Right-click a host cluster and select **NetApp ONTAP tools > Protect Cluster**.
3. If AutomatedFailOverDuplex policy type is selected, add host proximity or host access details.
4. Select **Protect** button.

A vCenter task is created and you can track the progress in the **Recent task** panel.

= Remove host cluster protection

:icons: font

:relative_path: ./manage/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

When you remove the host cluster protection, the datastores become unprotected.

Steps

1. To view the protected host clusters, navigate to **NetApp ONTAP tools > Protection > Host cluster relationships**.

In this page, you can monitor the protected host clusters along with its protection state, SnapMirror relationship, and its corresponding SnapMirror status.

2. In the **Host cluster protection** window, click on the kebab menu against the cluster, and then select **Remove protection**.

= Upgrade ONTAP tools

= Upgrade from ONTAP tools for VMware vSphere 10.x to 10.2

:icons: font

:relative_path: ./upgrade/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

Upgrade is supported for both HA and non-HA deployments.



To upgrade from ONTAP tools for VMware vSphere 10.0 to 10.2 release, you need to first upgrade to ONTAP tools for VMware vSphere 10.1 and then to 10.2 release.

Before you begin

If you're upgrading from ONTAP tools for VMware vSphere 10.0 to 10.1, you need to complete the following steps before proceeding with the upgrade task:

Enable Diagnostics

1. From vCenter Server, open a console to ONTAP tools.
2. Log in as the maintenance user.
3. Enter **4** to select Support and Diagnostics.
4. Enter **2** to select Enable remote diagnostic access.
5. Enter **y** to set the password of your choice.
6. Login to VM IP address from the terminal/putty with user as 'diag' and password that was set in the previous step.

Take Backup of MongoDB

Run the following commands to take a backup of mongoDB:

- `kn exec -it ntv-mongodb-0 sh - kn` is an alias of `kubectl -n ntv-system`.
- `env | grep MONGODB_ROOT_PASSWORD` - run this command inside the pod.
- 'exit' - run this to come out of the pod.
- `kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip` - run this command to replace `MONGO_ROOT_PASSWORD` set from above command.
- `kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz` - run this command to copy the mongodb backup created using above command from pod to host.

Take the snapshot of all the volumes

- Run 'kn get pvc' command and save the output of the command.
- Take snapshots of all the volumes one by one using one of the following methods:
 - From CLI, run the command `volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>`
 - From ONTAP system manager user interface search the volume by its name in the search bar then open that volume by clicking on the name. Go to snapshot and add the snapshot of that volume.

Take the snapshot of ONTAP tools for VMware vSphere VMs in vCenter (3VMs in case of HA Deployment, 1 VM in case of non-HA deployment)

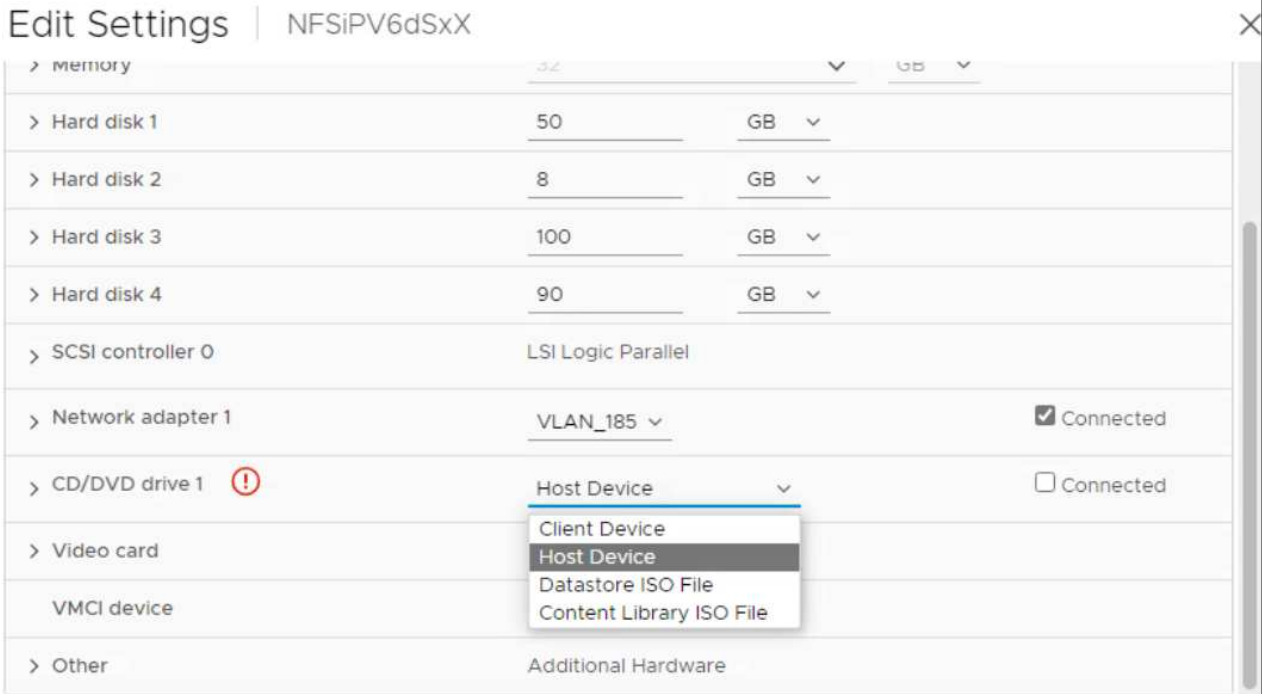
- In the vSphere client user interface, select the VM.
- Go to the snapshots tab and click the **Take Snapshot** button.

From the log bundle, delete the completed pods with prefix "generate-support-bundle-job" before performing the upgrade.

If support bundle generation is in progress, wait for it to complete and then delete the pod.

Steps

1. Upload ONTAP tools for VMware vSphere upgrade ISO to content library.
2. In the primary VM page, select **Actions > Edit Settings**
3. In the edit settings window under **CD/DVD drive** field, select content library ISO file.
4. Select the ISO file and click **OK**. Choose the connected checkbox across the **CD/DVD drive** field.



5. From vCenter Server, open a console to ONTAP tools.
6. Log in as the maintenance user.
7. Enter **3** to select the System Configuration menu.
8. Enter **7** to select the upgrade option.
9. When you upgrade, the following actions are performed automatically:
 - a. Certificate upgrade
 - b. Remote plug-in upgrade

= Upgrade error codes

:icons: font

:relative_path: ./upgrade/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

You might encounter error codes during ONTAP tools for VMware vSphere upgrade operation.

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:

Upgrade error code	Workflow	Resolution
063	Copying contents to recovery volume has failed	Perform snapshot-based recovery.
068	Debian packages rollback has failed	Perform snapshot-based recovery.
069	Failed restoring files	Perform snapshot-based recovery.
070	Failed deleting backup	Perform snapshot-based recovery.
071	Kubernetes cluster was not healthy	Perform snapshot-based recovery.
072	CR file does not exist in jail disk	Perform snapshot-based recovery.
073	Applying the CR failed while setting force reconcile flag to false	Perform snapshot-based recovery.
074	Mount ISO has failed	Retry the upgrade.
075	Upgrade pre-checks has failed	Retry the upgrade.
076	Registry upgrade has failed	Perform snapshot-based recovery.
077	Registry rollback has failed	Perform snapshot-based recovery.
078	Operator upgrade has failed	Perform snapshot-based recovery.
079	Operator rollback has failed	Perform snapshot-based recovery.
080	Services upgrade has failed	Perform snapshot-based recovery.

081	Services rollback has failed	Perform snapshot-based recovery.
082	Deleting old images from container failed	Perform snapshot-based recovery.
083	Deleting backup has failed	Perform snapshot-based recovery.
084	Changing JobManager back to Production failed	Perform snapshot-based recovery.
085	failed creating CA certificate secrets	Perform snapshot-based recovery.
086	failed creating server/private-key certificate secrets	Perform snapshot-based recovery.
087	Failed! to complete post 10.0 to 10.1 upgrade steps	Post upgrade steps failed.
088	Configuring log rotate for journald has failed	Retry the upgrade.
089	Changing ownership of summary log rotate config file has failed	Retry the upgrade.
091	iSCSI upgrade has failed	Retry the upgrade.
092	iSCSI rollback has failed	Retry the upgrade.
093	trident upgrade has failed	Retry the upgrade.
094	trident rollback has failed	Retry the upgrade.
095	Debian Upgrade failed	No recovery for debian upgrade. Services are upgraded and new pods will be running

Learn more about [How to restore ONTAP tools for VMware vSphere if upgrade fails from version 10.0 to 10.1](#)

= Recover ONTAP tools

= Recover your ONTAP tools for VMware vSphere setup

:icons: font

:relative_path: ./recover/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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 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 that you have created or to the node cluster or to the host where you want to deploy the OVA.
3. Right-click the required location and select **Deploy OVF template**.
4. Select the OVA file either through the URL for the .ova file or browse to the folder where the .ova file is saved, and then click **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. In the **Customize template** window, enter the required details and click **Next**



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

13. Review the details in the **Ready to complete** window, select **Finish**.

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

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

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.

15. Make necessary changes in the dialog prompt. Use tab button to navigate across the panel and select **OK**.

The values provided are validated again. ONTAP tools for VMware vSphere allows you three attempts to correct any invalid values. If you are unable to correct issues after three 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.

= Migrate ONTAP tools

= Migrate from ONTAP tools for VMware vSphere 9.x to 10.2

:icons: font

:relative_path: ./migrate/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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



It is recommended to migrate ONTAP tools for VMware vSphere 9.x setup only if the setup is servicing the VASA provider feature alone.



After migrating from ONTAP tools for VMware vSphere 9.x to 10.2, vVols datastores with NVMe/FC protocol do not work because ONTAP tools 10.2 only supports NVMe-oF with VMFS datastores.

About this task

Migration is supported from ONTAP tools for VMware vSphere 9.10D2, 9.11D4, 9.12D1, and 9.13D2 releases to 10.2 release.



If you are using ONTAP tools for VMware vSphere 9.13P1 version, you should upgrade to 9.13D2 before the migration to 10.2 version.



As an existing user, you need to take the OVA backup from your current release before upgrading to the patch releases.

== Common migration steps

1. Deploy OVA for ONTAP tools for VMware vSphere 10.2 release.
2. Add the vCenter Server instance that you want to migrate to ONTAP tools for VMware vSphere 10.2 release. See [Add vCenter Server instances](#)
3. Onboard storage backend locally from the ONTAP tools for VMware vSphere plug-in vCenter server APIs. Add storage as a locally scoped storage for migration.
4. The NFS and VMFS datastores migrated from ONTAP tools for VMware vSphere 9.xx is visible in ONTAP tools for VMware vSphere 10.2 only after the datastore discovery job is triggered, which might take up to 30 minutes to trigger. Verify if the datastores are visible in the Overview page of the ONTAP tools for VMware vSphere Plugin UI page.

== SRA migration steps

Before you begin

Before migrating, ensure that one of the sites is in a protected state and the other is in recovery state.



Do not migrate if the failover just completed and re-protect is pending. Complete the re-protect and then perform the migration. Same applies to testing the recovery plan. Once the testing of recovery plan is complete, cleanup the test recovery and then start the migration.

1. Perform the following steps to delete ONTAP tools for VMware vSphere 9.xx release SRA adapter in VMware Live Site Recovery UI:
 - a. Go to VMware Live Site Recovery Configuration management page
 - b. Go to Storage Replication Adapter section
 - c. Click on Kebab menu, and click on **Reset configuration**
 - d. Click on Kebab menu and select **Delete**

Perform these steps on both protection and recovery sites.

2. Install ONTAP tools for VMware vSphere 10.2 SRA adapter on both protection and recovery sites using the steps in [Configure SRA on VMware Live Site Recovery appliance](#)
3. In the VMware Live Site Recovery UI page, perform **Discover Arrays** and **Discover Devices** operations and verify that the devices are showing up as it was before the migration.

== VASA provider migration steps

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

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

2. Deploy OVA for ONTAP tools for VMware vSphere 10.2 release.
3. Add the vCenter Server instance that you want to migrate to ONTAP tools for VMware vSphere 10.2 release. See [Add a vCenter Server instance](#).
4. Onboard storage backend locally from the remote plug-in vCenter server APIs. Add storage as local scoped for migration.
5. Issue the following API call to migrate:

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
POST	/api/v1

Processing type

Asynchronous

Curl example

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

JSON input example

Request body for migrating from 9.12 and 9.13:

```
{
  "otv_ip": "10.12.13.45",
```

```
"vasa_provider_credentials": {
  "username": "vasauser",
  "password": ""
}
"database_password": ""
}
```

Request body for other release migration:

```
{
  "otv_ip": "10.12.13.45",
  "vasa_provider_credentials": {
    "username": "vasauser",
    "password": ""
  }
}
```

JSON output example

A job object is returned. You should save the job identifier to use it in the next step.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

1. Use the following URI to check the status:

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

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

2. Add ONTAP tools for VMware vSphere storage provider to the vCenter Server and [Register VASA Provider to vCenter Server](#).
3. Stop ONTAP tools for VMware vSphere storage provider 9.10/9.11/9.12/9.13 VASA Provider service from maintenance console.

Do not delete the VASA provider.

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

4. Perform the patch migrate using the following API:

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
PATCH	/api/v1

Processing type

Asynchronous

Curl example

```
PATCH "/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43"
```

JSON input example

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

JSON output example

A job object is returned. You should save the job identifier to use it in the next step.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

Request body is empty for patch operation.



uuid is the migration uuid returned in the response of post migrate API.

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

1. The delete API for migration is:

HTTP method	Path
DELETE	/api/v1

Processing type

Asynchronous

Curl example

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

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

After successful migration and after you register ONTAP tools 10.2 to the vCenter Server, do the following:

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

= Automate using REST APIs

= Overview of REST APIs

:icons: font

:relative_path: ./automation/

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

REST APIs can be used to perform several ONTAP tools for VMware vSphere management operations. REST APIs are exposed through the Swagger web page.

You can access the Swagger web page available at <https://loadbalancerIP:8443/> to display the REST API documentation, as well as to manually issue an API call.



All the APIs have request body and examples mentioned in the swagger page. The workflows and examples provided in this section are for reference purposes only.

== How to access ONTAP tools for VMware vSphere REST API

You can access the ONTAP REST API in several different ways.

== Network considerations

You can connect to the REST API through the following interfaces:

- Cluster management LIF
- Node management LIF
- SVM management LIF

The LIF you choose to use should be configured to support the HTTPS management protocol. Also, the firewall configuration in your network should allow the HTTPS traffic.



You should always use a cluster management LIF. This will load balance the API requests across all the nodes and avoid nodes that are offline or experiencing connectivity issues. If you have multiple cluster management LIFs configured, they are all equivalent regarding access to the REST API.

== ONTAP tools for VMware vSphere API online documentation page

You can access the Swagger from the hyperlink in the support page of the NetAPP ONTAP tools for VMware vSphere plug-in.

The format of the URL used to access the documentation page for the most recent version of the API is:

`https://<loadbalancer_ip_address>/docs/api`

== Custom software and tools

You can access ONTAP tools for VMware vSphere API using any of several different programming languages and tools. Popular choices include Python, Java, Curl, and PowerShell. A program, script, or tool that uses the API acts as a REST web services client. Using a programming language enables a deeper understanding of the API and provides an opportunity to automate ONTAP tools for VMware vSphere administration.

The format of the base URL used to directly access the most recent version of the API is:

```
`https://<loadbalancer_ip_address>/api`
```

To access a specific API version where multiple versions are supported, the format of the URL is:

```
`https://<loadbalancer_ip_address>/api/v1`
```

== Access ONTAP tools for VMware vSphere API reference documentation through the Swagger UI

You can access the ONTAP REST API documentation through the Swagger UI at your local ONTAP system.

Before you begin

You should have the following:

- IP address or host name of the ONTAP cluster management LIF
- Username and password for an account with authority to access the ONTAP REST API

Steps

1. Type the URL in your browser and press **Enter**:
`https://<ip_address>/docs/api`
2. Sign in using the ONTAP account

The ONTAP API documentation page is displayed with the API calls organized in major resource categories at the bottom.

3. As an example of an individual API call, scroll down to the **cluster** category and click **GET /cluster**.

= Get started with the REST API

```
:icons: font
```

```
:relative_path: ./automation/
```

```
:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/
```

You can quickly get started using ONTAP tools for VMware vSphere REST API. Accessing the API provides some perspective before you begin using it with the more complex workflow processes on a live setup.

== Hello World

You can run a simple command on your system to get started using ONTAP tools for VMware vSphere REST API and confirm its availability.

Before you begin

- Ensure that the Curl utility is available on your system.
- IP address or host name of ONTAP tools for VMware vSphere server
- Username and password for an account with authority to access ONTAP tools for VMware vSphere REST API.



If your credentials include special characters, you need to format them in a way that is acceptable to Curl based on the shell you are using. For example, you can insert a backslash before each special character or wrap the entire `username:password` string in single quotes.

Step

At the command line interface, run the following to retrieve the plug-in information:

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Example:

```
curl -X GET -u admin:password -k
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

== How to access ONTAP tools for VMware vSphere REST API

You can access the ONTAP REST API in several different ways.

== Network considerations

You can connect to the REST API through the following interfaces:

- Cluster management LIF
- Node management LIF
- SVM management LIF

The LIF you choose to use should be configured to support the HTTPS management protocol. Also, the firewall configuration in your network should allow the HTTPS traffic.



You should always use a cluster management LIF. This will load balance the API requests across all the nodes and avoid nodes that are offline or experiencing connectivity issues. If you have multiple cluster management LIFs configured, they are all equivalent regarding access to the REST API.

== Input variables controlling an API request

You can control how an API call is processed through parameters and variables set in the HTTP request.

== HTTP methods

The HTTP methods supported by ONTAP tools for VMware vSphere REST API are shown in the following table.



Not all the HTTP methods are available at each of the REST endpoints.

HTTP method	Description
GET	Retrieves object properties on a resource instance or collection.
POST	Creates a new resource instance based on the supplied input.
DELETE	Deletes an existing resource instance.
PUT	Modifies an existing resource instance.

== Request headers

You should include several headers in the HTTP request.

=== Content-type

If the request body includes JSON, this header should be set to *application/json*.

=== Accept

This header should be set to *application/json*.

=== Authorization

Basic authentication should be set with the username and password encoded as a base64 string.

== Request body

The content of the request body varies depending on the specific call. The HTTP request body consists of one of the following:

- JSON object with input variables
- Empty

== Filtering objects

When issuing an API call that uses GET, you can limit or filter the returned objects based on any attribute. For example, you can specify an exact value to match:

```
<field>=<query value>
```

In addition to an exact match, other operators are available to return a set of objects over a range of values. ONTAP tools for VMware vSphere REST API supports the filtering operators shown in the table below.

Operator	Description
=	Equal to
<	Less than
>	Greater than
≤	Less than or equal to

Operator	Description
>=	Greater than or equal to
UPDATE	Or
!	Not equal to
*	Greedy wildcard

You can also return a collection of objects based on whether a specific field is set or not set by using the **null** keyword or its negation **!null** as part of the query.



Any fields that are not set are generally excluded from matching queries.

== Requesting specific object fields

By default, issuing an API call using GET returns only the attributes that uniquely identify the object or objects. This minimum set of fields acts as a key for each object and varies based on the object type. You can select additional object properties using the `fields` query parameter in the following ways:

=== Common or standard fields

Specify **fields=*** to retrieve the most commonly used object fields. These fields are typically maintained in local server memory or require little processing to access. These are the same properties returned for an object after using GET with a URL path key (UUID).

=== All fields

Specify **fields=**** to retrieve all the object fields, including those requiring additional server processing to access.

=== Custom field selection

Use **fields=<field_name>** to specify the exact field you want. When requesting multiple fields, the values should be separated using commas without spaces.



As a best practice, you should always identify the specific fields you want. You should only retrieve the set of common fields or all fields when needed. Which fields are classified as common, and returned using `fields=*`, is determined by NetApp based on internal performance analysis. The classification of a field might change in future releases.

== Sorting objects in the output set

The records in a resource collection are returned in the default order defined by the object. You can change the order using the `order_by` query parameter with the field name and sort direction as follows:

```
order_by=<field name> asc|desc
```

For example, you can sort the type field in descending order followed by id in ascending order:

```
order_by=type desc, id asc
```

- If you specify a sort field but do not provide a direction, the values are sorted in ascending order.

- When including multiple parameters, you should separate the fields with a comma.

== Pagination when retrieving objects in a collection

When issuing an API call using GET to access a collection of objects of the same type, ONTAP tools for VMware vSphere attempts to return as many objects as possible based on two constraints. You can control each of these constraints using additional query parameters on the request. The first constraint reached for a specific GET request terminates the request and therefore limits the number of records returned.



If a request ends before iterating over all the objects, the response contains the link needed to retrieve the next batch of records.

=== Limiting the number of objects

By default, ONTAP tools for VMware vSphere returns a maximum of 10,000 objects for a GET request. You can change this limit using the *max_records* query parameter. For example:

```
max_records=20
```

The number of objects returned can be less than the maximum in effect, based on the related time constraint as well as the total number of objects in the system.

=== Limiting the time used to retrieve the objects

By default, ONTAP tools for VMware vSphere returns as many objects as possible within the time allowed for the GET request. The default timeout is 15 seconds. You can change this limit using the *return_timeout* query parameter. For example:

```
return_timeout=5
```

The number of objects returned can be less than the maximum in effect, based on the related constraint on the number of objects as well as the total number of objects in the system.

=== Narrowing the result set

If needed, you can combine these two parameters with additional query parameters to narrow the result set. For example, the following returns up to 10 EMS events generated after the specified time:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

You can issue multiple requests to page through the objects. Each subsequent API call should use a new time value based on the latest event in the last result set.

== Size properties

The input values used with some API calls as well as certain query parameters are numeric. Rather than provide an integer in bytes, you can optionally use a suffix as shown in the following table.

Suffix	Description
KB	KB Kilobytes (1024 bytes) or kibibytes
MB	MB Megabytes (KB x 1024 bytes) or mebibytes

Suffix	Description
GB	GB Gigabytes (MB x 1024 bytes) or gibibytes
TB	TB Terabytes (GB x 1024 bytes) or tebibytes
PB	PB Petabytes (TB x 1024 bytes) or pebibytes

= Legal notices

:icons: font

:relative_path: ./

:imagesdir: /tmp/d20250117-1148470-xakrys/source/./configure/./media/

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

== Copyright

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

== Trademarks

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

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

== Patents

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

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

== Privacy policy

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

== Open source

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

[Notice for ONTAP tools for VMware vSphere 10.2](#)

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.