ONTAP tools for VMware vSphere documentation

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

Table of Contents

ONTAP tools for VMware vSphere documentation

Release notes

Release notes for ONTAP tools

Learn about the new and enhanced features available in ONTAP tools for VMware vSphere 10.5.

For a complete list of new features and enhancements, refer What's new in ONTAP tools for VMware vSphere 10.5.

For the most up-to-date compatibility information, refer NetApp Interoperability Matrix Tool.

Migration is supported from ONTAP tools for VMware vSphere 9.12D1, 9.13D2, and 9.13P2 releases to ONTAP tools for VMware vSphere 10.5.

For more information, refer the ONTAP tools for VMware vSphere 10.5 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 10.5

Learn about the new capabilities available in ONTAP tools for VMware vSphere 10.5.

- **Platform qualification**

ONTAP tools for VMware vSphere 10.5 adds support for ASA r2 systems, providing compatibility with the latest hardware and software configurations. This release also includes integration with ONTAP 9.16.1 and 9.17.1, expanding the supported environments.

- **VMware qualification and certifications**

ONTAP tools for VMware vSphere 10.5 complies with current VMware interoperability certification standards, supporting both ESXi host and vCenter Server.

- **MetroCluster support**

This release introduces support for MetroCluster configurations, enhancing high availability and disaster recovery capabilities.

- **Security and certificate management**

This release introduces streamlined management of self-signed certificates, enhancing both user experience and adherence to security standards. It provides improved certificate validation workflows to secure ONTAP and ONTAP tools for VMware vSphere communications.

- **Replication enhancements**

This release supports VMFS replication with hierarchical consistency group including SRA and SnapMirror active sync in ASA r2 systems. It supports zero RPO backups to improve data protection and recovery.

- **Upgrade and migration**

The upgrade and migration process from previous versions of ONTAP tools for VMware vSphere to ONTAP tools for VMware vSphere 10.5 is designed to be seamless and efficient, minimizing downtime and ensuring a

smooth transition.

Supported ONTAP platforms and vCenter Server versions

ONTAP tools for VMware vSphere 10.5 P1 supports vCenter High Availability (HA) configurations for SRA and SnapMirror active sync components. vVols is not supported in this configuration. During an HA failover, vCenter might be unavailable for several minutes. In large environments or if an error occurs, failover times can exceed 15 minutes.

For more information, see the vCenter High Availability documentation. For questions about vCenter HA, contact Broadcom Support.

For the latest details on version compatibility, refer to NetApp Interoperability Matrix Tool.

ONTAP tools for VMware vSphere 9 and 10 feature comparison

Learn whether migrating from ONTAP tools for VMware vSphere 9 to ONTAP tools for VMware vSphere 10.2 or later versions is right for you.

For the most up-to-date compatibility information, refer NetApp Interoperability Matrix Tool.

Feature	ONTAP tools 9.13	ONTAP tools 10.2 onwards
Key value proposition	Streamline and simplify day-0 to day-2 operations with enhanced security, compliance and automation capabilities	Expanded support to include FC for VMFS and NVMe-oF for VMFS only. Ease of use for NetApp SnapMirror, simple setup for vSphere metro storage clusters, and three-site VMware Live Site Recovery support
ONTAP release qualification	ONTAP 9.9.1 to ONTAP 9.16.1	ONTAP 9.12.1 to 9.15.1 for ONTAP tools 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0, and 9.16.1 for ONTAP tools 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0, and 9.16.1 for ONTAP tools 10.4. ONTAP 9.16.1P3 and later is required for ONTAP tools 10.4 when using ASA r2 systems. ONTAP 9.15.1, 9.16.1, and 9.17.0 for ONTAP tools 10.5

Feature	ONTAP tools 9.13	ONTAP tools 10.2 onwards
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 vSphere 9.0 from ONTAP tools 10.5 onwards VMware Site Recovery Manager (SRM) 8.7 to VMware Live Site Recovery 9.0 **NOTE:** In ONTAP tools 10.x, SRM supports shared sites, enabling enhanced scalability and improved performance.
Protocol support	NFS and VMFS datastores: NFS (v3 and v4.1), VMFS (iSCSI and FCP)	NFS and VMFS datastores: NFS (v3 and v4.1), VMFS (iSCSI/FCP/NVMe-oF)
Scalability	Hosts and VMs: 300 Hosts, up to 10K VMs Datastores: 600 NFS, up to 50 VMFS	Hosts and VMs: 600 Hosts
Observability	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. SCV integration and interoperable for backup.	SRA replication for iSCSI VMFS and NFS v3 datastores three-site protection combining SMAS and VMware Live Site Recovery. SRA support for FCP with VMFS.
VASA Provider support	VASA 4.0	VASA 3.0

Concepts

Learn about ONTAP tools

ONTAP tools for VMware vSphere is a set of tools for virtual machine lifecycle management. It integrates with the VMware ecosystem to simplify datastore provisioning and provide basic protection for virtual machines. It is a collection of horizontally scalable, event-driven microservices deployed as an Open Virtual Appliance (OVA).

ONTAP tools for VMware vSphere supports:

- Core virtual machine (VM) features such as protection and disaster recovery
- VASA Provider for storage policy-based management
- Storage policy-based management
- Storage Replication Adapter (SRA)

High availability for ONTAP tools for VMware

ONTAP tools for VMware vSphere offers high-availability (HA) support to help maintain uninterrupted operation during failures.

The HA solution helps you recover quickly from the following types of outages:

- Host failure - Only a single-node failure is supported.
- Network failure
- Virtual machine (guest OS) failure
- Application (ONTAP tools) failure

You do not need to perform any additional configuration to enable HA for ONTAP tools for VMware vSphere.

ONTAP tools for VMware vSphere doesn't support vCenter HA.

To use the HA feature, ensure that CPU hot add and memory hot plug are enabled during deployment or later in the VM settings.

Key concepts and terms in ONTAP tools

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 managed as a single unit. Consistency groups are synchronized for data consistency across storage units and volumes. In ONTAP, they provide easy management and a protection guarantee for an application workload spanning multiple volumes. Learn more about consistency groups.

Dual stack

A dual-stack network is a networking environment that supports the simultaneous use of 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 the associated initiators can access namespaces within the subsystem.

ONTAP tools Manager

ONTAP tools Manager provides more control to ONTAP tools for VMware vSphere administrators over the managed vCenter Server instances and onboarded storage backends. It helps manage 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.

Recovery Point Objective (RPO)

RPO measures how frequently you back up or replicate data. It specifies the exact point in time you need to restore data after an outage to resume business operations. For example, if an organization has an RPO of 4 hours, it can tolerate losing up to 4 hours of data in the event of a disaster.

SnapMirror active sync

SnapMirror active sync enables business services to continue operating even with a complete site failure, supporting applications to fail over transparently using a secondary copy. Manual intervention or custom scripting is not required to trigger a failover with SnapMirror active sync. Learn more about SnapMirror active sync.

Storage backends

Storage backends are the underlying storage infrastructure that the ESXi host uses to store virtual machine files, data, and other resources. They allow the ESXi host to access and manage persistent data, providing the required storage capability and performance for a virtualized environment.

Global cluster (storage backend)

Global storage backends, available only with ONTAP cluster credentials, are onboarded through the ONTAP tools Manager interface. They can be added with minimal privileges to enable the discovery of essential cluster resources needed for vVols management. Global clusters are ideal for multitenancy scenarios where an SVM user is added locally for vVols management.

Local storage backend

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

Storage Replication Adapter (SRA)

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

Storage virtual machine (SVM)

SVM is the unit of multitenancy in ONTAP. 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 two sites are connected to all paths to storage clusters on both sites. Cross-site paths are stretched across distances.
- **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.
> Learn more about SnapMirror active sync overview in ONTAP.

Virtual Machine File System (VMFS)

VMFS is a clustered file system designed to store 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 vVols.

VM Storage Policy

VM Storage Policies are created in the 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 formerly known as Site Recovery Manager (SRM) 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 an architecture 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 created and maintained by a VASA Provider.

Zero RPO

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

Role based access control (RBAC)

Learn about ONTAP tools RBAC

Role-based access control (RBAC) is a security framework for controlling access to resources within an organization. RBAC simplifies administration by defining roles with specific levels of authority to perform actions, instead of assigning authorization to individual users. The defined roles are assigned to users, which helps reduce risk of error and simplifies management of access control across your organization.

The RBAC standard model consists of several implementation technologies or phases of increasing complexity. The result is that actual RBAC deployments, based on the needs of the software vendors and their customers, can differ and range from relatively simple to very complex.

RBAC components

At a high level, there are several components which are generally included with every RBAC implementation. These components are bound together in different ways as part of defining the authorization processes.

Privileges

A *privilege* is an action or capability that can be allowed or denied. It might be something simple such as the ability to read a file or it could be a more abstract operation specific to a given software system. Privileges can

also be defined to restrict access to REST API endpoints and CLI commands. Every RBAC implementation includes pre-defined privileges and might also allow administrators to create custom privileges.

Roles

A *role* is a container that includes one or more privileges. Roles are generally defined based on particular tasks or job functions. When a role is assigned to a user, the user is granted all the privileges contained in the role. And as with privileges, implementations include pre-defined roles and generally allow custom roles to be created.

Objects

An *object* represents a real or abstract resource identified within the RBAC environment. The actions defined through the privileges are performed on or with the associated objects. Depending on the implementation, privileges can be granted to an object type or a specific object instance.

Users and groups

Users are assigned or associated with a role applied after authentication. Some RBAC implementations allow only one role to be assigned to a user while others allow multiple roles per user, perhaps with only one role active at a time. Assigning roles to *groups* can further simplify security administration.

Permissions

A *permission* is a definition that binds a user or group along with a role to an object. Permissions can be useful with a hierarchical object model where they can optionally be inherited by the children in the hierarchy.

Two RBAC environments

There are two distinct RBAC environments you need to consider when working with ONTAP tools for VMware vSphere 10.
ONTAP tools for VMware vSphere 10 requires specific privileges in both vCenter and ONTAP to perform its operations. While ONTAP tools automates storage management tasks, it does not create user accounts in either vCenter or ONTAP. Service accounts must be created by a vSphere administrator as needed. This documentation provides guidance for administrators to assign the necessary roles and permissions for effective ONTAP tools management.

VMware vCenter Server

The RBAC implementation in VMware vCenter Server is used to restrict access to objects exposed through the vSphere Client user interface. As part of installing ONTAP tools for VMware vSphere 10, the RBAC environment is extended to include additional objects representing the capabilities of ONTAP tools. Access to these objects is provided through the remote plug-in. See vCenter Server RBAC environment for more information.

ONTAP cluster

ONTAP tools for VMware vSphere 10 connects to an ONTAP cluster through the ONTAP REST API to perform storage related operations. Access to the storage resources is controlled through an ONTAP role associated with the ONTAP user provided during authentication. See ONTAP RBAC environment for more information.

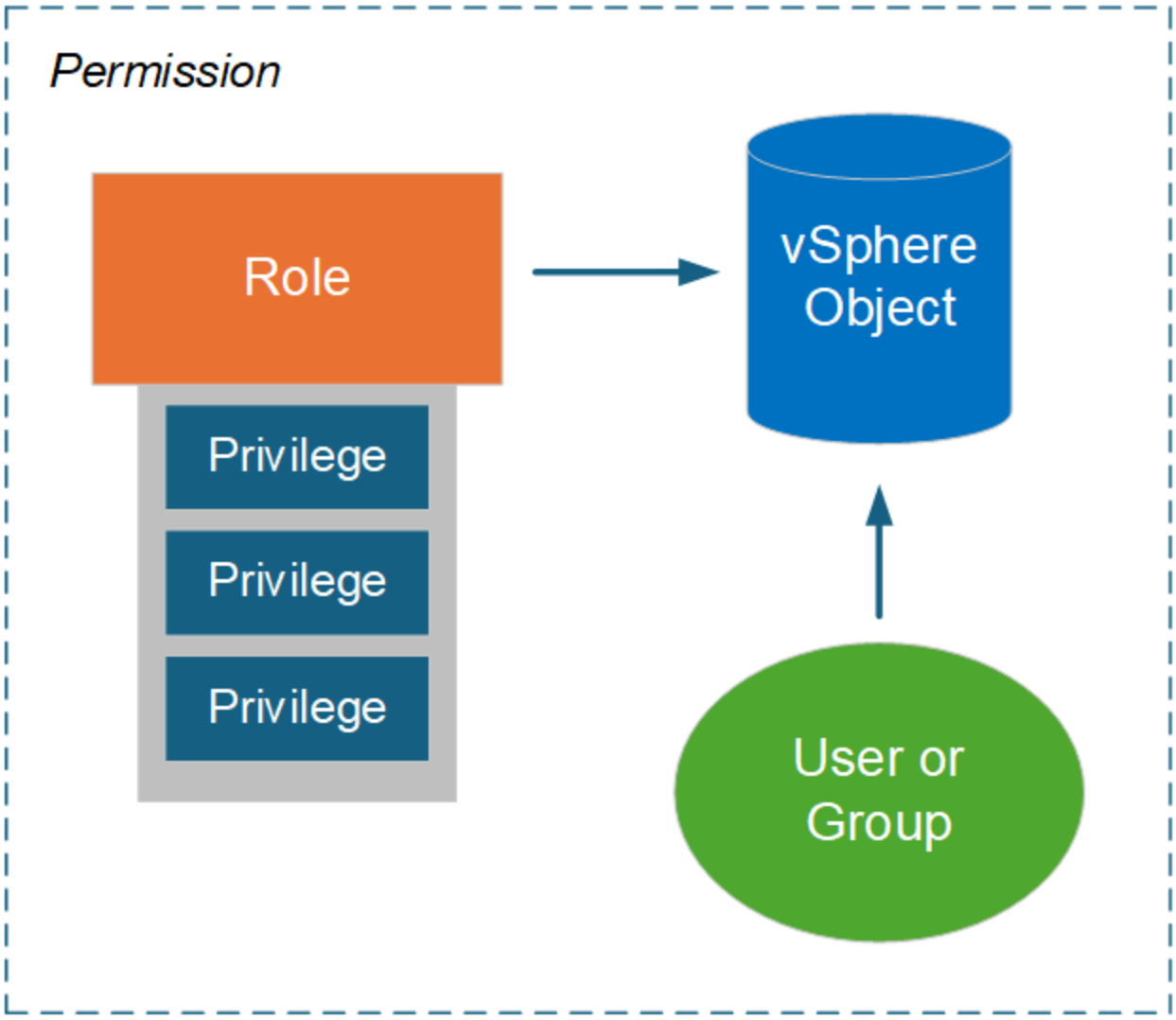
RBAC with VMware vSphere

How vCenter Server RBAC works with ONTAP tools

VMware vCenter Server provides an RBAC capability that enables you to control access to vSphere objects. It is an important part of the vCenter centralized authentication and authorization security services.

Illustration of a vCenter Server permission

A permission is the foundation for enforcing access control in the vCenter Server environment. It's applied to a vSphere object with a user or group included with the permission definition. A high-level illustration of a vCenter permission is provided in the figure below.



Components of a vCenter Server permission

A vCenter Server permission is a package of several components that are bound together when the permission is created.

vSphere objects

Permissions are associated with vSphere objects, such as the vCenter Server, ESXi hosts, virtual machines, datastores, data centers, and folders. Based on the object's assigned permissions, vCenter Server determines which actions or tasks can be performed on the object by each user or group. For the tasks specific to ONTAP tools for VMware vSphere, all permissions are assigned and validated at the root or root folder level of vCenter Server. See Use RBAC with vCenter server for more information.

Privileges and roles

There are two types of vSphere privileges used with ONTAP tools for VMware vSphere 10. To simplify working with RBAC in this environment, ONTAP tools provides roles containing the required native and custom privileges. The privileges include:

- Native vCenter Server privileges

  These are the privileges provided by vCenter Server.

- ONTAP tools-specific privileges

  These are custom privileges unique to ONTAP tools for VMware vSphere.

Users and groups

You can define users and groups using Active Directory or the local vCenter Server instance. Combined with a role, you can create a permission on an object in the vSphere object hierarchy. The permission grants access based on the privileges in the associated role. Note that roles aren't assigned directly to users in isolation. Instead, users and groups gain access to an object through role privileges as part of the larger vCenter Server permission.

vCenter Server RBAC considerations for ONTAP tools

There are several aspects of the ONTAP tools for VMware vSphere 10 RBAC implementation with vCenter Server you should consider before using it in a production environment.

vCenter roles and the administrator account

You only need to define and use the custom vCenter Server roles if you want to limit access to the vSphere objects and associated administrative tasks. If limiting access is not required, you can use an administrator account instead. Each administrator account is defined with the Administrator role at the top level of the object hierarchy. This provides full access to the vSphere objects, including those added by ONTAP tools for VMware vSphere 10.

vSphere object hierarchy

The vSphere object inventory is organized in a hierarchy. For example, you can move down the hierarchy as follows:

`vCenter Server` --> `Datacenter` --> `Cluster` --> `ESXi host` --> `Virtual Machine`

All permissions are validated in the vSphere object hierarchy except the VAAI plug-in operations, which are validated against the target ESXi host.

Roles included with ONTAP tools for VMware vSphere 10

To simplify working with vCenter Server RBAC, ONTAP tools for VMware vSphere provides predefined roles tailored to various administration tasks.

You can create new custom roles if needed. In this case, you should clone one of the existing ONTAP tools roles and edit it as needed. After making the configuration changes, the affected vSphere client users need to log out and log back in to activate the changes.

To view the ONTAP tools for VMware vSphere roles, select **Menu** at the top of the vSphere Client and click **Administration** and then **Roles** on the left.
The following privileges must be included in the role assigned to the vCenter user responsible for deploying or onboarding vCenter. Ensure these privileges are configured as a prerequisite for the deployment or onboarding process.

- Alarms
  - Acknowledge alarm
- Content Library
  - Add library item
  - Check in a template
  - Check out a template
  - Download files
  - Import storage
  - Read storage
  - Sync library item
  - Sync subscribed library
  - View configuration settings
- Datastore
  - Allocate space
  - Browse datastore
  - Low level file operations
  - Remove file
  - Update virtual machine files
  - Update virtual machine metadata
- ESX Agent Manager
  - View
- Folder
  - Create folder
- Host
  - Configuration
    - Advanced settings
    - Change settings
    - Network configuration
    - System resources
    - Virtual machine autostart configuration

    - Local operations
        - Create virtual machine
        - Delete virtual machine
        - Reconfigure virtual machine
- Network
    - Assign network
    - Configure
- OvfManager
    - OvfConsumer Access
- Host profile
    - View
- Resource
    - Assign virtual machine to resource pool
- Scheduled task
    - Create tasks
    - Modify task
    - Run task
- Tasks
    - Create task
    - Update task
- vApp
    - Add virtual machine
    - Assign resource pool
    - Assign vApp
    - Create
    - Import
    - Move
    - Power off
    - Power on
    - Pull from URL
    - View OVF environment
- Virtual machine
    - Change Configuration
        - Add existing disk
        - Add new disk
        - Add or remove device
        - Advanced configuration

        - Change CPU count
        - Change Memory
        - Change Settings
        - Change resource
        - Extend virtual disk
        - Modify device settings
        - Remove disk
        - Reset guest information
        - Upgrade virtual machine compatibility
    - Edit Inventory
        - Create from existing
        - Create new
        - Move
        - Register
        - Remove
        - Unregister
    - Interaction
        - Backup operation on virtual machine
        - Configure CD media
        - Configure floppy media
        - Connect devices
        - Console interaction
        - Guest operating system management by VIX API
        - Power off
        - Power on
        - Reset
        - Suspend
    - Provisioning
        - Allow disk access
        - Clone template
        - Customize guest
        - Deploy template
        - Modify customization specification
        - Read customization specifications
    - Snapshot management
        - Create snapshot
        - Remove snapshot

- Rename snapshot
- Revert to snapshot

There are three predefined roles as described below.

NetApp ONTAP tools for VMware vSphere Administrator

Provides all the native vCenter Server privileges and ONTAP tools-specific privileges required to perform core ONTAP tools for VMware vSphere administrator 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:

- Create new datastores
- Manage datastores

vSphere objects and ONTAP storage backends

The two RBAC environments work together. When performing a task in the vSphere client interface, the ONTAP tools roles defined to vCenter Server are checked first. If the operation is permitted by vSphere, then the ONTAP role privileges are examined. This second step is performed based on the ONTAP role assigned to the user when the storage backend was created and configured.

Working with vCenter Server RBAC

There are a few things to consider when working with the vCenter Server privileges and permissions.

Required privileges

To access the ONTAP tools for VMware vSphere 10 user interface, you need to have the ONTAP tools-specific *View* privilege. If you sign in to vSphere without this privilege and click the NetApp icon, ONTAP tools for VMware vSphere displays an error message and prevents you from accessing the user interface.

The assignment level in the vSphere object hierarchy determines which portions of the user interface you can access. Assigning the View privilege to the root object enables you to access ONTAP tools for VMware vSphere by clicking the NetApp icon.

You can instead assign the View privilege to another lower vSphere object level. However, this will limit the ONTAP tools for VMware vSphere menus that you can access and use.

Assigning permissions

You need to use vCenter Server permissions if you want to limit access to the vSphere objects and tasks. Where you assign permission in the vSphere object hierarchy determines the ONTAP tools for VMware vSphere 10 tasks users can perform.

Unless you need to define more restrictive access, it’s generally a good practice to assign permissions at the root object or root folder level.

The permissions available with ONTAP tools for VMware vSphere 10 apply to custom non-vSphere objects, such as storage systems. If possible, you should assign these permissions to ONTAP tools for VMware vSphere root object because there is no vSphere object you can assign it to. For example, any permission that includes an ONTAP tools for VMware vSphere "Add/Modify/Remove storage systems" privilege should be assigned at the root object level.

When defining a permission at a higher level in the object hierarchy, you can configure the permission so it is passed down and inherited by the child objects. If needed you can assign additional permissions to the child objects that override the permissions inherited from the parent.

You can modify a permission at any time. If you change any of the privileges within a permission, users associated with the permission need to log out of vSphere and log back in to enable the change.

RBAC with ONTAP

How ONTAP RBAC works with ONTAP tools

ONTAP provides a robust and extensible RBAC environment. You can use the RBAC capability to control access to the storage and system operations as exposed through the REST API and CLI. It's helpful to be familiar with the environment before using it with an ONTAP tools for VMware vSphere 10 deployment.

Overview of the administrative options

There are several options available when using ONTAP RBAC depending on your environment and goals. An overview of the major administrative decisions is presented below. Also see ONTAP Automation: Overview of RBAC security for more information.

> ONTAP RBAC is tailored to a storage environment and is simpler than the RBAC implementation provided with vCenter Server. With ONTAP, you assign a role directly to the user. Configuring explicit permissions, such as those used with vCenter Server, aren't needed with ONTAP RBAC.

Types of roles and privileges

An ONTAP role is required when defining an ONTAP user. There are two types of ONTAP roles:

- REST

  The REST roles were introduced with ONTAP 9.6 and are generally applied to users accessing ONTAP through the REST API. The privileges included in these roles are defined in terms of access to the ONTAP REST API endpoints and the associated actions.

- Traditional

  These are the legacy roles included prior to ONTAP 9.6. They continue to be a foundational aspect of RBAC. The privileges are defined in terms of access to the ONTAP CLI commands.

While the REST roles were introduced more recently, the traditional roles have some advantages. For example, additional query parameters can optionally be included so the privileges more precisely define the objects they are applied to.

Scope

ONTAP roles can be defined with one of two different scopes. They can be applied to a specific data SVM (SVM level) or to the entire ONTAP cluster (cluster level).

Role definitions

ONTAP provides a set of pre-defined roles at both the cluster and SVM level. You can also define custom roles.

Working with ONTAP REST roles

There are several considerations when using the ONTAP REST roles included with ONTAP tools for VMware vSphere 10.

Role mapping

Whether using a traditional or REST role, all ONTAP access decisions are made based on the underlying CLI command. But because the privileges in a REST role are defined in terms of the REST API endpoints, ONTAP needs to create a *mapped* traditional role for each of the REST roles. Therefore each REST role maps to an underlying traditional role. This allows ONTAP to make access control decisions in a consistent way regardless of the role type. You cannot modify the parallel mapped roles.

Defining a REST role using CLI privileges

Because ONTAP always uses the CLI commands to determine access at a base level, it's possible to express a REST role using CLI command privileges instead of REST endpoints. One benefit of this approach is the additional granularity available with the traditional roles.

Administrative interface when defining ONTAP roles

You can create users and roles with the ONTAP CLI and REST API. However, it's more convenient to use the System Manager interface along with the JSON file available through the ONTAP tools Manager. See Use ONTAP RBAC with ONTAP tools for VMware vSphere 10 for more information.

ONTAP RBAC considerations for ONTAP tools

There are several aspects of the ONTAP tools for VMware vSphere 10 RBAC implementation with ONTAP you should consider before using it in a production environment.

Overview of the configuration process

ONTAP tools for VMware vSphere includes support for creating an ONTAP user with a custom role. The definitions are packaged in a JSON file that you can upload to the ONTAP cluster. You can create the user and tailor the role for your environment and security needs.

The major configuration steps are described at a high level below. Refer to Configure ONTAP user roles and privileges for more details.

1. Prepare

You need to have administrative credentials for both the ONTAP tools Manager and the ONTAP cluster.

2. Download the JSON definition file

After signing in to the ONTAP tools Manager user interface, you can download the JSON file containing the RBAC definitions.

3. Create an ONTAP user with a role

After signing in to System Manager, you can create the user and role:

a. Select **Cluster** on the left and then **Settings**.

b. Scroll down to **Users and roles** and click −→.

c. Select **Add** under **Users** and select **Virtualization products**.

d. Select the JSON file on your local workstation and upload it.

4. Configure the role

As part of defining the role, you need to make several administrative decisions. See Configure the role using System Manager for more details.

Configure the role using System Manager

After you begin creating a new user and role with System Manager and you have uploaded the JSON file, you can customize the role based on your environment and needs.

Core user and role configuration

The RBAC definitions are packaged as several product capabilities, including combinations of VSC, VASA Provider, and SRA. You should select the environment or environments where you need RBAC support. For example, if you want roles to support the remote plug-in capability, select VSC. You also need to choose the user name and associated password.

Privileges

The role privileges are arranged in four sets based on the level of access needed to the ONTAP storage. The privileges which the roles are based on include:

- Discovery

  This role enables you to add storage systems.

- Create storage

  This role enables you to create storage. It also includes all the privileges associated with the discovery role.

- Modify storage

  This role enables you to modify storage. It also includes all the privileges associated with the discovery and create storage roles.

- Destroy storage

  This role enables you to destroy storage. It also includes all the privileges associated with the discovery, create storage, and modify storage roles.

Generate the user with a role

After you've selected the configuration options for your environment, click **Add** and ONTAP creates the user and role. The name of the generated role is a concatenation of the following values:

- Constant prefix value defined in the JSON file (for example "OTV_10")
- Product capability you selected
- List of the privilege sets.

Example

```
OTV_10_VSC_Discovery_Create
```

The new user will be added to the list on the page "Users and roles". Note that both HTTP and ONTAPI user login methods are supported.

Deploy ONTAP tools for VMware vSphere

Quick start for ONTAP tools for VMware vSphere

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

Initially, you'll deploy ONTAP tools for VMware vSphere as a small-sized single node configuration that provides core services to support NFS and VMFS datastores. To expand your configuration for additional containers per service, enhanced resiliency, or to use vVols datastores and high availability (HA), complete this workflow first and then proceed with the expansion steps. For more information, refer to the HA deployment workflow.

Plan your deployment

Verify that your vSphere, ONTAP, and ESXi host versions are compatible with the ONTAP tools version. Allocate sufficient CPU, memory, and disk space. Based on your security rules, you might need to set up firewalls or other security tools to allow network traffic.

Ensure the vCenter Server is installed and accessible.

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

Deploy ONTAP tools for VMware vSphere

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

- Deploy ONTAP tools for VMware vSphere

Add vCenter Server instances

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

- Add vCenter Server instances

Configure ONTAP user roles and privileges

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

- Configure ONTAP user roles and privileges

5 **Configure the storage backends**

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

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

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

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

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

- Manage certificates

7 **(Optional) Configure SRA protection**

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

- Enable ONTAP tools for VMware vSphere services
- Configure SRA on the VMware Live Site Recovery appliance

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

Configure ONTAP tools for VMware vSphere to manage host cluster protection for SnapMirror active sync. Perform the ONTAP cluster and SVM peering in ONTAP systems to use SnapMirror active sync. This applies only to VMFS datastores.

- Protect using host cluster protection

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

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

- Edit the backup settings
- Recover the ONTAP tools setup

High availability deployment workflow for ONTAP tools

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

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

1 **Scale up the deployment**

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

- Change ONTAP tools for VMware vSphere configuration

2 **Enable services**

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

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

- Enable VASA Provider and SRA services

3 **Upgrade the certificates**

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

- Manage certificates

ONTAP tools for VMware vSphere requirements and configuration limits

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

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

System requirements

- **Installation package space requirements per node**
  - 15 GB for thin provisioned installations
  - 348 GB for thick provisioned installations
- **Host system sizing requirements**
  The table below shows the recommended memory for each deployment size. For high availability (HA) deployments, you need three times the appliance size listed.

Type of deployment	CPUs per node	Memory (GB) per node	Disk space (GB) thick provisioned per node
Small	9	18	350
Medium	13	26	350
Large NOTE: The large deployment is only for HA configuration.	17	34	350

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

Minimum storage and application requirements

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

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

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

Interoperability Matrix Tool

Port requirements

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

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

traffic from outside the cluster. Block inter-node ports from internet access with firewall rules.

- Internal ports: These ports communicate within the Kubernetes cluster using ClusterIP addresses. They are not exposed externally and do not need to be added to firewall rules.

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

Click to expand or collapse the port requirements table.

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

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

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

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

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

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

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

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

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

- Virtual machine Disaster Recovery (DR) is configured using synchronous, asynchronous, or strict sync policies. DR is not supported for the NVMe protocol.
- ESXi host cluster protection uses SnapMirror Active Sync, which does not support multi-vCenter deployments.
- ONTAP tools restricts only the number of ESXi hosts and datastores based on deployment size. There are

no restrictions on the number of vCenter Servers that can be connected to ONTAP tools.

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

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

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

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

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

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

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

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

Pre-deployment requirements for ONTAP tools

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

Requirements	Your status
vSphere version, ONTAP version, and ESXi host version are compatible with the ONTP tools version.	□ Yes □ No
vCenter Server environment is set up and configured	□ Yes □ No
Browser cache is deleted	□ Yes □ No
You have the parent vCenter Server credentials	□ Yes □ No
You have the login credentials for the vCenter Server instance, to which the ONTAP tools for VMware vSphere will connect post-deployment for registration	□ Yes □ No
The domain name on which the certificate is issued is mapped to the virtual IP address in a multi-vCenter deployment where custom CA certificates are mandatory.	□ Yes □ No
You have run the nslookup check on the domain name to check if the domain is getting resolved to the intended IP address.	□ Yes □ No
The certificate is created with the domain name and the ONTAP tools IP address.	□ Yes □ No
ONTAP tools application and internal services are reachable from the vCenter Server.	□ Yes □ No
When using multi-tenant SVMs, you have an SVM management LIF on each SVM.	□ Yes □ No

Deployment worksheet

For single node deployment

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

Requirement	Your value
IP address for the ONTAP tools application. This is the IP address for accessing the ONTAP tools web interface (load balancer)	
ONTAP tools virtual IP address for internal communication. This IP address is used for internal communication in a setup with multiple ONTAP tools instances. This IP address should not be same as the IP address for the ONTAP tools application.(The Kubernetes Control Plane)	

Requirement	Your value
DNS hostname for the ONTAP tools management node	
Primary DNS server	
Secondary DNS server	
DNS search domain	
IPv4 address for the ONTAP tools management node. It is a unique IPv4 address for the node management interface on the management network.	
Subnet mask for the IPv4 address	
Default gateway for the IPv4 address	
IPv6 address (optional)	
IPv6 prefix length (optional)	
Gateway for the IPv6 address (optional)	

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

For High availability (HA) deployment

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

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

Network firewall configuration

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

ONTAP storage settings

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

following settings:

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

Deploy ONTAP tools

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

Before you begin

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

Consider the following before creating a content library:

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

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

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

Follow these steps to create a content library:

1. Download the file that contains the binaries (*.ova*) and signed certificates for ONTAP tools for VMware vSphere from the NetApp Support Site.
2. Log in to the vSphere client
3. Select the vSphere client menu and select **Content libraries**.
4. Select **Create** on the right of the page.
5. Provide a name for the library and create the content library.
6. Go to the content library you created.
7. Select **Actions** in the right of the page and select **Import item** and import the OVA file.

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

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

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

Steps

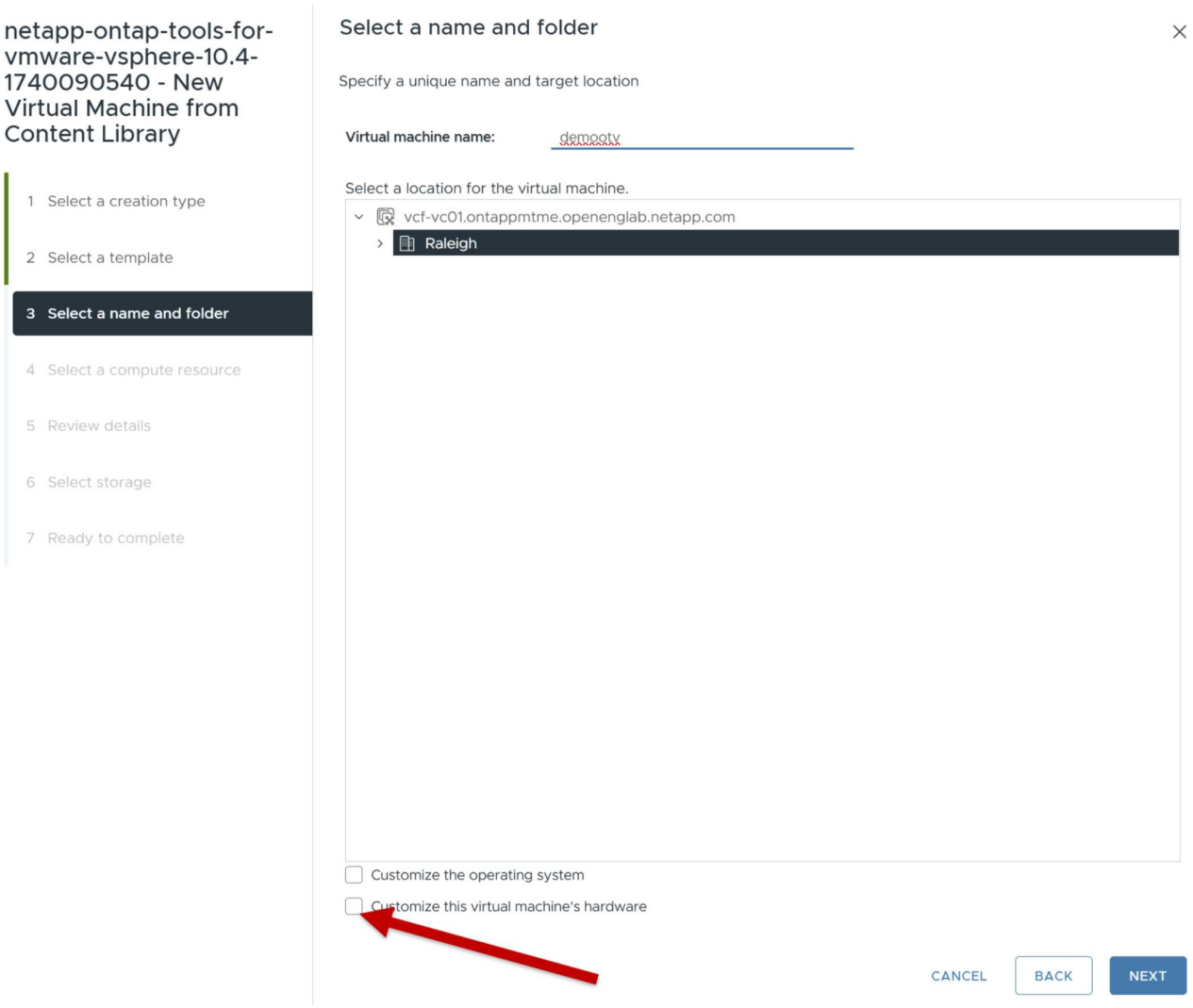
1. Download the file that contains the binaries (*.ova*) and signed certificates for the ONTAP tools for VMware vSphere from the NetApp Support Site. If you have imported the OVA into the content library, you can skip this step and proceed with the next step.
2. Log in to the vSphere server.
3. Go to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

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

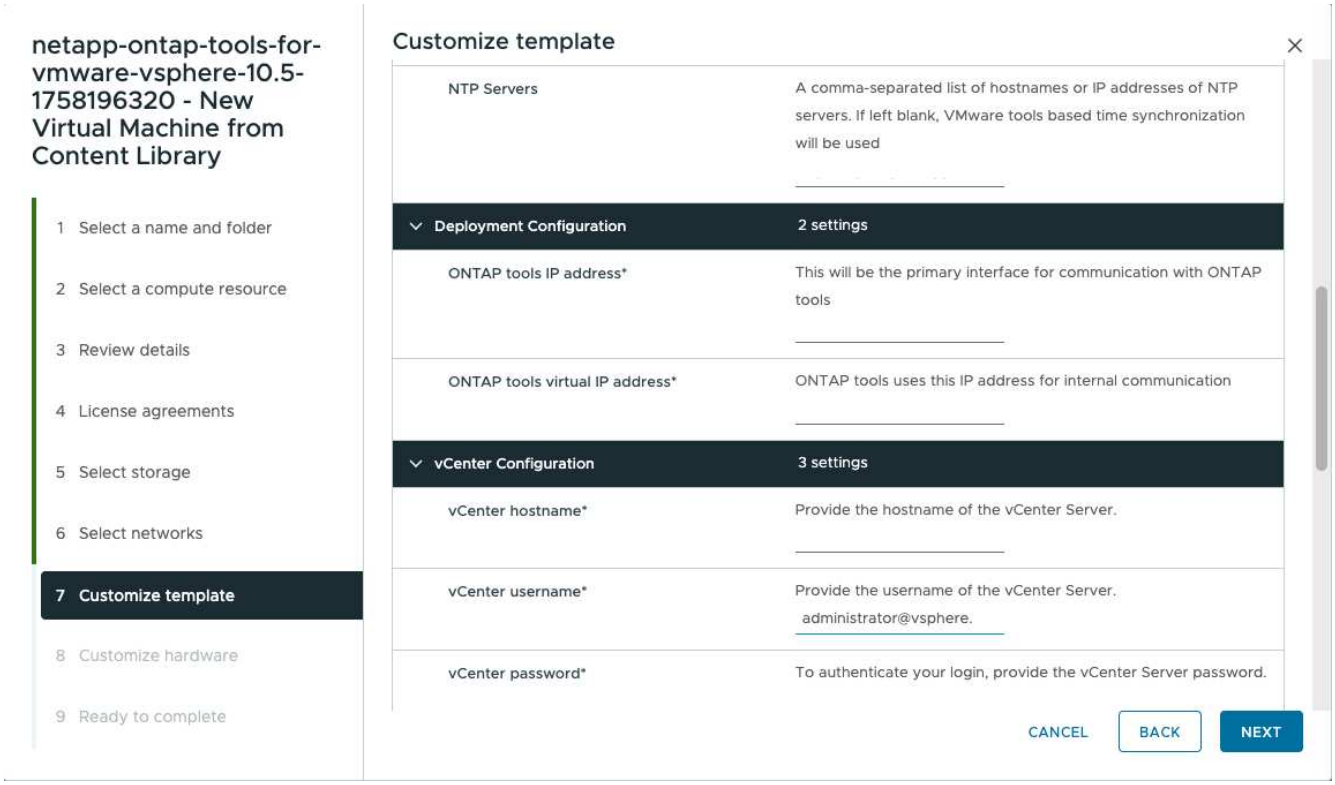
4. You can deploy the OVA from the content library or from the local system.

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

5. In the **Select a name and folder** field, enter the virtual machine name and choose its location.
   - If you're using the vCenter Server 8.0.3 version, Select the option **Customize this virtual machine's hardware**, which will activate an additional step called **Customize hardware** before proceeding to the **Ready to complete** window.
   - If you're using the vCenter Server 7.0.3 version, follow the steps in the **what's next?** section at the end of deployment.



6. Select a computer resource and select **Next**. Optionally, check the box to **Automatically power on deployed VM**.
7. Review the details of the template and select **Next**.
8. Read and accept the license agreement and select **Next**.
9. Select the storage for the configuration and the disk format and select **Next**.
10. Select the destination network for each source network and select **Next**.
11. In the **Customize template** window, fill in the required fields.



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

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

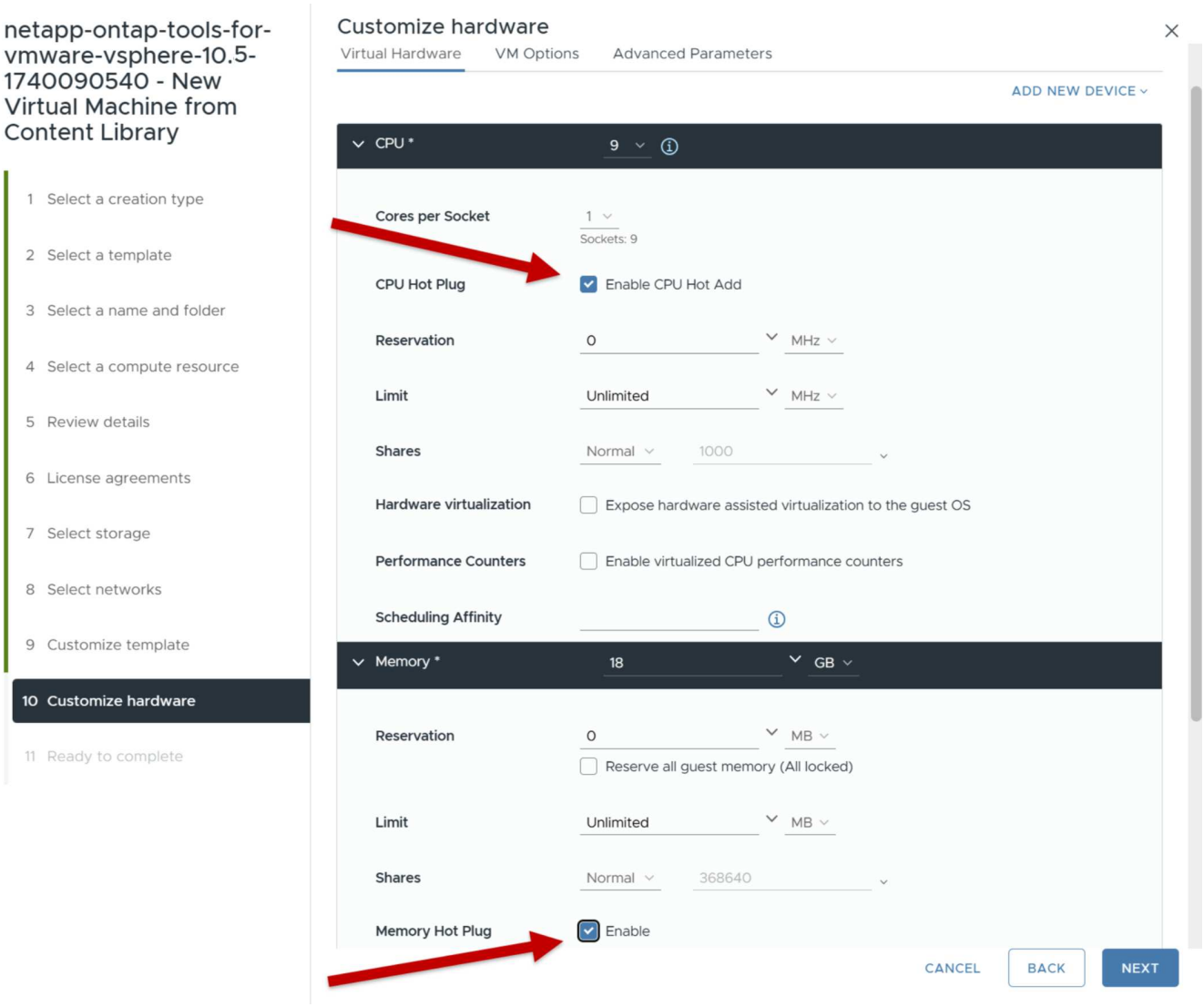
For the vCenter instance that will be managed by ONTAP tools, make sure the vCenter user account has administrator privileges.

- Host names must include letters (A-Z, a-z), digits (0-9), and hyphens (-). To configure dual stack, specify the host name mapped to the IPv6 address.

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

- ONTAP tools IP address is the primary interface for communicating with ONTAP tools.
- IPv4 is the IP address component of the node configuration, which can be utilized to enable diagnostic shell and SSH access on the node for the purposes of debugging and maintenance.

12. When using the vCenter Server 8.0.3 version, in the **Customize hardware** window, enable the **CPU hot add** and **Memory hot plug** options to allow HA functionality.



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

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

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

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

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

What's next?

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

1. Log in to the vCenter client
2. Power down the ONTAP tools node.
3. Go to the ONTAP tools for VMware vSphere virtual machine under **Inventories** and select the **Edit settings** option.

4. Under the **CPU** options, check the **Enable CPU hot add** checkbox
5. Under the **Memory** options, check the **Enable** checkbox against **Memory hot plug**.

Troubleshoot ONTAP tools deployment errors

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

Collect the log files

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

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

Steps

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

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

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

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

Steps

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

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

Deployment error codes

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

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

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

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

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

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

Deployment error code	Workflow	Resolution
049	For network and validation perl script will assign them as well shortly	-
050	Ssh Key generation failed	Restart the primary virtual machine (VM).
053	Failed installing RKE2	Either run the following and restart the primary VM or redeploy: sudo rke2-killall.sh (all VMs) sudo rke2-uninstall.sh (all VMs).
054	Failed setting kubeconfig	Redeploy
055	Failed deploying registry	If the registry pod is present, wait for the pod to be ready then restart the primary VM or else redeploy.

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

Reboot error code	**Workflow**	**Resolution**
067	Waiting for rke2-server timed out.	-
101	Failed to Reset Maint/Console user password.	-
102	Failed to Delete password file during reset Maint/Console user password.	-

103	Failed to Update New Maint/Console user password in vault.	-
088	Configuring log rotate for journald has failed.	Check the VM network settings that is compatible with the host on which the VM is hosted. You can try to migrate to another host and restart the VM.
089	Changing ownership of summary log rotate config file has failed.	Restart the VM.

Configure ONTAP tools for VMware vSphere

Add vCenter Server instances to ONTAP tools

Add vCenter Server instances to ONTAP tools for VMware vSphere to configure, manage, and protect your virtual datastores in your vCenter Server environment. When you add multiple vCenter Server instances, Custom CA certificates are required for secure communication between ONTAP tools and each vCenter Server.

About this task

ONTAP tools integrates with vCenter Server to perform storage tasks like provisioning, snapshots, and data protection directly from the vSphere client.

Before you begin

- Ensure the vCenter Server certificate includes a valid Subject Alternative Name (SAN) extension with both DNS and IP address entries. For example:

```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

  If the certificate does not include a SAN extension, or if the SAN extension does not contain the correct DNS or IP address values, ONTAP tools operations may fail due to certificate validation errors.

- The Primary Network Identifier (PNID) of the vCenter Server must be included in the SAN details. The PNID and DNS name should be identical and resolvable in DNS.
- It is recommended to deploy vCenter Server using its fully qualified domain name (FQDN), and ensuring the SAN in the certificate includes DNS Name=machine_FQDN for optimal compatibility and support.
- For more information, refer to VMware documentation:
  - vSphere Certificate Requirements for Different Solution Paths
  - Replace vCenter Machine SSL certificate Custom Certificate Authority Signed Certificate
  - Error: Subject Alternate Name (SAN) field does not contain the PNID. Please provide a valid certificate

> If FQDN is not available, you can set the PNID to the IP address and include the IP address in the SAN. However, this is not recommended by VMware.

Steps

1. Open a web browser and go to the URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **vCenters** > **Add** to onboard the vCenter Server instances. Provide your vCenter IP address or hostname, username, password, and port details.
4. In advanced options, fetch the vCenter Server certificate automatically (authorize it) or upload it manually.

You don’t need an admin account to add vCenter instances to ONTAP tools. You can create a custom role without the admin account with limited permissions. Refer to Use vCenter Server RBAC with ONTAP tools for VMware vSphere 10 for details.

Adding a vCenter Server instance to ONTAP tools automatically triggers the following actions:

- ONTAP tools registers the vCenter client plug-in as a remote plug-in.
- Custom privileges for the plug-ins and APIs are applied to the vCenter Server instance.
- Custom roles are created to manage the users.
- The plug-in appears as a shortcut on the vSphere user interface.

Register the VASA Provider with a vCenter Server instance in ONTAP tools

Use ONTAP tools for VMware vSphere to register the VASA Provider with a vCenter Server instance. This enables storage policy-based management, vVols support, and integration with VMware Live Site Recovery appliances on ONTAP systems.

VASA Provider settings show the registration status for the selected vCenter Server.

Steps

1. Log in to the vSphere client.
2. Select **Shortcuts** > **NetApp ONTAP tools** under the plug-ins section.
3. Select **Settings** > **VASA Provider settings**. The ONTAP tools displays the VASA Provider registration status as not registered.
4. Select the **Register** button to register the VASA Provider.
5. Enter a name and credentials for the VASA Provider. The username can only contain letters, numbers, and underscores. Set the password length between 8 and 256 characters.
6. Select **Register**.
7. After a successful registration and page refresh, ONTAP tools display the registered VASA Provider’s status, name, and version.

What’s next

Verify that the onboarded VASA Provider is listed under VASA Provider from the vCenter client:

Steps

1. Go to the vCenter Server instance.
2. Log in with the administrator credentials.
3. Select **Storage Providers** > **Configure**. Verify that the onboarded VASA Provider is listed correctly.

Install the NFS VAAI plug-in using ONTAP tools

The NFS vStorage API for Array Integration (NFS VAAI) plug-in connects VMware vSphere to NFS storage arrays. Use ONTAP tools for VMware vSphere to install the VAAI plug-in. This allows the NFS storage array to handle certain storage operations instead of

ESXi hosts.

Before you begin

- Download the NetApp NFS Plug-in for VMware VAAI installation package.
- Make sure you have the ESXi host and vSphere 7.0U3 latest patch or later versions and ONTAP 9.14.1 or later versions.
- Mount an NFS datastore.

Steps

1. Log in to the vSphere client.
2. Select **Shortcuts** > **NetApp ONTAP tools** under the plug-ins section.
3. Select **Settings** > **NFS VAAI Tools**.
4. If you have already uploaded the VAAI plug-in to vCenter Server, select **Change** in **Existing version**. If you have not, select **Upload**.
5. Browse and select the `.vib` file and select **Upload** to upload the file to ONTAP tools.
6. Select **Install on ESXI host**, select the ESXi host on which you want to install the NFS VAAI plug-in, and then select **Install**.

   The vSphere Web Client shows only the ESXi hosts that can install the plug-in. You can monitor the installation progress in the recent tasks section.

7. Restart the ESXi host manually after installation.

   After you restart the ESXi host, ONTAP tools for VMware vSphere automatically detect and enable the NFS VAAI plug-in.

What's next?

After you install the NFS VAAI plug-in and reboot your ESXi host, configure the NFS export policies for VAAI copy offload. Ensure the export policy rules meet these requirements:

- The relevant ONTAP volume allows NFSv4 calls.
- The root user remains as root and NFSv4 is allowed in all junction parent volumes.
- The option for VAAI support is set on the relevant NFS server.

For more information, refer to Configure the correct NFS export policies for VAAI copy offload KB article.

Related information

Support for VMware vStorage over NFS

Enable or disable NFSv4.0

ONTAP support for NFSv4.2

Configure ESXi host settings in ONTAP tools

Configuring ESXi server multipath and timeout settings helps maintain data availability and integrity. It enables automatic failover to a backup storage path if the primary path becomes unavailable.

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 time, depending on your setup and system load. You can view the progress in the Recent Tasks panel.

Steps

1. From the VMware vSphere Web client home page, select **Hosts and Clusters**.
2. On the shortcuts page of the VMware vSphere Web client, select **NetApp ONTAP tools** under the plug-ins section.
3. Go to the **ESXi Host compliance** card 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 you want to update to use NetApp recommended settings and select **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 select **Finish**. You can track the progress in the recent task panel.

Set ESXi host values

Use ONTAP tools for VMware vSphere to set timeouts and other values on ESXi hosts for optimal performance and failover. It sets these values based on NetApp testing.

You can set the following values on an ESXi host:

HBA/CNA Adapter Settings

Sets the following parameters to default values:

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBA timeouts
- QLogic FC HBA timeouts

MPIO Settings

MPIO settings pick the best paths for NetApp storage systems. MPIO settings select the best path and use it.

For high-performance environments or when testing with a single LUN datastore, adjust the load balance setting of the round-robin (VMW_PSP_RR) path selection policy (PSP) to improve performance. Set the default IOPS value from 1000 to 1.

The MPIO settings don't apply to NVMe, NVMe/FC, and NVMe/TCP protocols.

NFS settings

Parameter	Set this value to…
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 or higher
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

Configure ONTAP user roles and privileges for ONTAP tools

Use this section to configure ONTAP user roles and privileges for storage backends with ONTAP tools for VMware vSphere and ONTAP System Manager. You can assign roles using the provided JSON files, manually create users and roles, and apply the minimum required privileges for non-admin accounts.

Before you begin

- Download the ONTAP Privileges file from ONTAP tools for VMware vSphere using *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*. After downloading the zip file, you find two JSON files. Use the ASA r2-specific JSON file when configuring an ASA r2 system.

  You can create users at the cluster level or directly at the storage virtual machines (SVMs) level. If you do not use the user_roles.json file, ensure the user has the minimum required SVM permissions.

- Log in with administrator privileges for the storage backend.

Steps

1. Extract the *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* file that you downloaded.
2. Access ONTAP System Manager using the cluster management IP address of the cluster.
3. Log in to the cluster with admin privileges. To configure a user:
   a. To configure a cluster ONTAP tools user, select **Cluster** > **Settings** > **Users and Roles** pane.
   b. To configure an 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. For non-ASA r2 systems, select users_roles.json file and for ASA r2 systems, select users_roles_ASAr2.json file.

ONTAP tools automatically populates the Product field.

f. Select the product capability as **VSC, VASA Provider and SRA** from the drop-down.

ONTAP tools automatically populates the **Role** field based on the product capability you select.

g. Enter the required username and password.

h. Select the privileges (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) the user needs, and then select **Add**.

ONTAP tools adds the new role and user. You can view privileges under the role you configured.

SVM aggregate mapping requirements

When provisioning datastores using SVM user credentials, ONTAP tools for VMware vSphere creates volumes on the aggregate specified in the datastores POST API. ONTAP prevents SVM users from creating volumes on aggregates not mapped to the SVM. Map the SVM to the required aggregates using the ONTAP REST API or CLI before creating volumes.

REST API:

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

ONTAP CLI:

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
---------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

Create ONTAP user and role manually

Create users and roles manually without the JSON file.

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

   Add the **REST API Path** and choose the access from the drop-down list.

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

This page lists the minimum privileges required for a non-admin global-scoped cluster user without a JSON file.
If a cluster is in local scope, use the JSON file to create users because ONTAP tools for VMware vSphere needs more than just the Read privileges for provisioning on ONTAP.

You can access functionality by 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/security/accounts	Read-Only	Privilege discovery
/api/security/roles	Read-Only	Privilege 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 when the cluster is added locally.
/api/network/ip/interfaces	Read-Only	Add storage backend - To identify the management LIF scope is cluster/SVM
/api/storage/availability-zones	Read-Only	SAZ discovery. Applicable to ONTAP 9.16.1 release onwards and ASA r2 systems.
/api/cluster/metrocluster	Read-Only	Gets MetroCluster status and configuration details.

Create ONTAP tools for VMware vSphere ONTAP API based cluster scoped user

Discovery, create, modify, and destroy privileges are required for PATCH operations and automatic rollback on datastores. Missing permissions might cause workflow and cleanup issues.

An ONTAP API-based user with discovery, create, modify, and destroy privileges can manage ONTAP tools workflows.

To create a cluster scoped user with all privileges mentioned above, run the following commands:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all
```

```
security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly
```

```
security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
```

```
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly
```

Additionally, for ONTAP Versions 9.16.0 and above run the following command:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

For ASA r2 systems on ONTAP Versions 9.16.1 and above run the following command:

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

Create ONTAP tools for VMware vSphere ONTAP API based SVM scoped user

Run the following commands to create an SVM scoped user with all privileges:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
```

```
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

Additionally, for ONTAP Versions 9.16.0 and above run the following command:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

To create a new API based user using the above created API based roles, run the following command:

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

Example:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

Run the following command to unlock the account and enable management interface access:

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Example:

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

Upgrade ONTAP tools for VMware vSphere 10.1 user to 10.3 user

For ONTAP tools for VMware vSphere 10.1 users with a cluster-scoped user created using the JSON file, use the following ONTAP CLI commands with user admin privileges to upgrade to the 10.3 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

For ONTAP tools for VMware vSphere 10.1 user with a SVM scoped user created using the json file, use the ONTAP CLI commands with admin user privileges to upgrade to the 10.3 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>

To enable the following commands, add the commands *vserver nvme namespace show* and *vserver nvme subsystem show* to the existing role.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Upgrade ONTAP tools for VMware vSphere 10.3 user to 10.4 user

Beginning with ONTAP 9.16.1, upgrade the ONTAP tools for VMware vSphere 10.3 user to 10.4 user.

For ONTAP tools for VMware vSphere 10.3 user with a cluster-scoped user created using the JSON file and ONTAP version 9.16.1 or above, use the ONTAP CLI command with admin user privileges to upgrade to the 10.4 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 "storage
availability-zone show" -access all
```

Add a storage backend to ONTAP tools

Use ONTAP tools for VMware vSphere to add and manage storage backends for your ESXi hosts. You can onboard clusters or SVMs, enable MetroCluster support, and validate certificates for secure connectivity. You can configure storage backends using ONTAP tools Manager or the vSphere client, monitor certificate status, and manually rediscover resources after cluster changes.

To add a storage backend locally, use cluster or SVM credentials in the ONTAP tools interface. Local storage backends are available only to the selected vCenter Server. ONTAP tools maps SVMs to the vCenter Server

for vVols or VMFS datastore management. For VMFS datastores and SRA workflows, you can use SVM credentials without mapping a cluster globally.

To add a global storage backend, use ONTAP cluster credentials in ONTAP tools Manager. Global storage backends enable discovery workflows to identify cluster resources required for vVol management. In multitenant environments, you can add an SVM user locally to manage vVols datastores.

If MetroCluster support is enabled in ONTAP, onboard both source and destination clusters as local or global storage backends.

Before you begin

Verify that the certificate includes a valid Subject Alternative Name (SAN) field. ONTAP systems use the SAN field to identify cluster and SVM management LIFs.

Using ONTAP tools Manager

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://<ONTAPtoolsIP>: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. Add the storage backend and provide the server IP address or FQDN, username, and password details.

   IPv4 and IPv6 address management LIFs are supported.

5. Fetch the ONTAP cluster certificates automatically and authorize the certificate, or manually upload it by browsing to its location.

   If needed, you can disable Subject Alternative Name (SAN) validation from the maintenance console. For instructions, see Change certificate validation flag.

6. If the storage backend you add is part of a MetroCluster configuration, ONTAP tools Manager shows a pop-up message to add the peered cluster. Select **Add** and provide the details for the MetroCluster peer storage backend.

   After the ONTAP system performs a switchover and switchback, run the ONTAP tools discovery manually.

Using vSphere client user interface

vVols datastores do not support direct addition of an SVM user through the vSphere client user interface.

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. Select **Storage Backends** from the sidebar.
4. Add the storage backend and provide the server IP address, username, password, and port details.

   You can add a storage backend using cluster-based credentials with either IPv4 or IPv6 management LIFs. To add an SVM user directly, provide SVM-based credentials along with an SVM management LIF. If a cluster is already onboarded, you cannot onboard an SVM user from that cluster again.

5. Fetch the ONTAP cluster certificates automatically and authorize the certificate, or manually upload it by browsing to its location.
6. If the added storage backend is part of the MetroCluster configuration, ONTAP tools displays the **Add MetroCluster peer** screen. Select **Add peer** to add the peer storage backend.

After the ONTAP system performs a switchover and switchback, run the ONTAP tools discovery manually.

What's next?

ONTAP tools updates the list to show the new storage backend.

ONTAP tools list the newly added storage backend on the **Storage backends** page. If a certificate expires in 30 days or less, ONTAP tools shows a warning in the certificate expiry date column. After expiry, ONTAP tools marks the storage backend as unknown because it cannot connect to the storage system.

Related information

Configuring the clusters into a MetroCluster configuration

Associate a storage backend with a vCenter Server instance in ONTAP tools

Associate a storage backend with a vCenter Server instance to enable access for all vCenter Server instances. For MetroCluster configuration, when you associate a storage backend cluster, ensure you also associate its peer cluster with the vCenter Server.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select vCenter from the sidebar.
4. Select the vertical ellipses next to the vCenter Server instance that you want to connect to the storage backends.
5. From the dropdown menu, choose the storage backend you want to associate with the selected vCenter Server instance.

Configure network access in ONTAP tools

By default, all IP addresses discovered from the ESXi host are automatically added to the export policy unless you configure network access. You can modify the export policy to allow access only from specific IP addresses. If an excluded ESXi host attempts a mount operation, the operation fails.

Steps

1. Log in to the vSphere client.
2. Select **NetApp ONTAP tools** in the shortcuts page under the plug-ins section.
3. In the left pane of ONTAP tools, go to **Settings** > **Manage Network Access** > **Edit**.

   To add multiple IP addresses, separate the list with commas, range, Classless Inter-Domain Routing (CIDR), or a combination of all three.

4. Select **Save**.

Create a datastore in ONTAP tools

When you create a datastore at the host cluster level, ONTAP tools mounts it on all destination hosts and enables the action only if you have the required privileges.

Interoperability between native datastores with vCenter Server and ONTAP tools managed datastores

Beginning with ONTAP tools for VMware vSphere 10.4, ONTAP tools creates nested igroups for datastores, with parent igroups specific to datastores and child igroups mapped to the hosts. You can create flat igroups from ONTAP System Manager and use them to create VMFS datastores without using ONTAP tools. Refer to Manage SAN initiators and igroups for more information.

After you onboard the storage and run datastore discovery, ONTAP tools changes flat igroups in VMFS datastores to nested igroups. You cannot use earlier flat igroups to create new datastores. Use the ONTAP tools interface or REST API to reuse nested igroups.

Create a vVols datastore

Beginning with ONTAP tools for VMware vSphere 10.3, you can create a vVols datastore on ASA r2 systems with space-efficiency as thin.vVol. The VASA Provider creates a container and the desired protocol endpoints while creating the vVol datastore. The VASA Provider does not assign any backing volumes to this container.

Before you begin

- Make sure root aggregates are not mapped to SVM.
- Ensure that the VASA Provider is registered with the selected vCenter.
- In the ASA r2 storage system, the SVM should be mapped to the aggregate for the SVM user.

Steps

1. Log in to the vSphere client.
2. Right-click on a host system, host cluster, or data center and select **NetApp ONTAP tools** > **Create Datastore**.
3. Select vVols **Datastore type**.
4. Enter the **Datastore name** and **Protocol** information.

   The ASA r2 system supports the iSCSI and FC protocols for vVols.

5. Select the storage VM where you want to create the datastore.
6. Under advanced options:
   - If you select the **Custom export policy**, ensure you run discovery in vCenter for all objects. It's recommended that you don't use this option.
   - You can select **Custom initiator group** name for the iSCSI and FC protocols.

   In ASA r2 storage system type SVM, storage units (LUN/namespace) aren't created because the datastore is only a logical container.

7. In the **Storage attributes** pane, you can create new volumes or use the existing volumes. However, you cannot combine these two types of volumes to create a vVols datastore.

   When creating a new volume, you can enable QoS on the datastore. By default, one volume is created for every LUN-created request. Skip this step for vVols datastores on ASA r2 storage systems.

8. Review your selection in the **Summary** pane and select **Finish**.

Create an NFS datastore

An NFS datastore connects ESXi hosts to shared storage using the NFS protocol. They are simple and flexible and are used in VMware vSphere environments.

Steps

1. Log in to the vSphere client.
2. Right-click on a host system, host cluster, or data center and select **NetApp ONTAP tools** > **Create datastore**.
3. Select NFS in the **Datastore type** field.

4. Enter the datastore name, size, and protocol information in the **Name and protocol** pane. Select **Datastore cluster** and **Kerberos authentication** in the advanced options.

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

5. Select **Platform** and **Storage VM** in the **Storage** pane.
6. If you select **Custom export policy** under the advanced options, run the discovery in vCenter for all objects. It's recommended that you don't use this option.

   You cannot create an NFS datastore using the SVM's default or root volume policy.

   - In the advanced options, the **Asymmetric** toggle button is visible only if performance or capacity is selected in the platform drop-down.
   - When you choose the **Any** option in the platform dropdown, you can see all SVMs in the vCenter. Platform and asymmetric flag do not affect visibility.

7. Select the aggregate for volume creation in the **Storage Attributes** pane. In the advanced options, choose **Space Reserve** and **Enable QoS** as required.
8. Review the selections in the **Summary** pane and select **Finish**.

ONTAP tools creates the NFS datastore and mounts it on all hosts.

Create a VMFS datastore

VMFS is a clustered file system for storing virtual machine files. Multiple ESXi hosts can access the same VM files simultaneously for vMotion and High Availability features.

On a protected cluster:

- You can create only VMFS datastores. Adding a VMFS datastore to a protected cluster automatically protects it.
- You cannot create a datastore on a data center with one or more protected host clusters.
- You cannot create a datastore on an ESXi host if the parent host cluster is protected by an "Automated Failover Duplex policy" (uniform or non-uniform configuration).
- You can create a VMFS datastore only on an ESXi host protected by an asynchronous relationship. You cannot create and mount a datastore on an ESXi host that is part of a host cluster protected by the "Automated Failover Duplex" policy.

Before you begin

- Enable services and LIFs for each protocol on the ONTAP storage side.
- Map SVM to aggregate for SVM user in the ASA r2 storage system.
- Configure the ESXi host if you're using the NVMe/TCP protocol:
  1. Review the VMware Compatibility Guide

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

  2. Check if the Network Interface Card (NIC) vendor supports ESXi NIC with the NVMe/TCP protocol.

3. Set up 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 page Enable NVMe over RDMA or NVMe over TCP Software Adapters to configure NVMe/TCP software adapters. For the 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're using the NVME/FC protocol, perform the following steps to configure the ESXi host:
  1. If not already enabled, 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 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.
2. Right-click on a host system, host cluster, or data center and select **NetApp ONTAP tools** > **Create Datastore**.
3. Select VMFS datastore type.
4. Enter the datastore name, size, and protocol information in the **Name and Protocol** pane.
   To add the new datastore to an existing VMFS cluster, select the datastore cluster in Advanced Options.
5. Select storage VM in the **Storage** pane. Provide the **Custom initiator group name** in the **Advanced options** section as required. You can choose an existing igroup for the datastore or create a new igroup with a custom name.

   When NVMe/FC or NVMe/TCP protocol is selected, a new namespace subsystem is created and is used for namespace mapping. ONTAP tools creates the namespace subsystem 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 the **Storage** pane.
6. From the **storage attributes** pane:
   a. Select **Aggregate** from the drop-down options.

   For ASA r2 storage systems, the **Aggregate** option is not shown because storage is disaggregated. When you choose an ASA r2 storage system type SVM, the storage attributes page shows the options for enabling QoS.

b. ONTAP tools creates a storage unit (LUN/Namespace) with a thin space reserve based on the selected protocol.

> Beginning in ONTAP 9.16.1, ASA r2 storage systems support up to 12 nodes per cluster.

c. Select the **Performance service level** for ASA r2 storage systems with 12 nodes SVM that is a heterogeneous cluster. This option is unavailable if the selected SVM is a homogeneous cluster or uses an SVM user.

   'Any' is the default performance service level (PSL) value. This setting creates the storage unit using the ONTAP balanced placement algorithm. However, you can select the performance or extreme option as required.

d. Select **Use existing volume**, **Enable QoS** options as required, and provide the details.

> In the ASA r2 storage type, volume creation or selection doesn't apply to storage unit creation(LUN/Namespace). Therefore, these options aren't shown.

> You cannot use the existing volume to create a VMFS datastore with NVMe/FC or NVMe/TCP protocol. Create a new volume for the VMFS datastore.

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

> If you create the datastore on a protected cluster, you can see a read-only message: "The datastore is being mounted on a protected Cluster."

Result

ONTAP tools creates the VMFS datastore and mounts it on all the hosts.

Protect datastores and virtual machines

Protect a host cluster in ONTAP tools

ONTAP tools for VMware vSphere manages the 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.

Before you begin

Make sure you meet these requirements before you protect a host cluster:

- The host cluster contains datastores from a single SVM only.
- Datastores on the host cluster aren't mounted on hosts outside the cluster.
- Datastores mounted on the host cluster are VMFS datastores with iSCSI or FC protocol. You can't use vVols, NFS, or VMFS datastores with NVMe/FC and NVMe/TCP protocols.
- Datastores based on FlexVol/LUN volumes mounted on a host are not part of any consistency group.
- Datastores based on FlexVol/LUN volumes mounted on a host are not part of any SnapMirror relationships.
- The host cluster contains at least one datastore.

Steps

1. Log in to the vSphere client.
2. Right-click on a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. In the protect cluster window, the system automatically fills in the datastore type and source storage virtual machine (VM) details. Select the datastores link to view the protected datastores.
4. Select **Add Relationship**.
5. 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 the SnapMirror relationship as an AutomatedFailOverDuplex type policy, you must add the target storage VM as storage backend to the same vCenter where ONTAP tools for VMware vSphere is deployed.

   In the AutomatedFailOverDuplex policy type, there are uniform and non-uniform host configurations. When you select the **uniform host configuration** toggle button, the host initiator group configuration is implicitly replicated on the target site. For more information, refer to Key concepts and terms.
6. If you choose to have a non-uniform host configuration, select the host access (source/target) for each host inside that cluster.
7. Select **Add**.
8. You can edit the host cluster protection using the **Modify host cluster protection** operation. You can edit or delete the relationships using the ellipsis menu options.
9. Select the **Protect** button.

   The system creates a vCenter task with job ID details and shows its progress in the recent tasks panel. This is an asynchronous task; the user interface shows only the request submission status and does not

wait for the task to complete.

10. To view the protected host clusters, go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**. Select a consistency group to view its capacity, associated datastores, and child consistency groups.

If you need to remove protection within one hour of creation, run storage discovery first.

Related information

VMware vSphere Metro Storage Cluster (vMSC)

Protect using SRA protection

Configure SRA in ONTAP tools to protect datastores

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

Before you begin

- You should have set up your vCenter Server instance and configured ESXi host.
- You should have deployed ONTAP tools for VMware vSphere.
- You should have downloaded the SRA Adapter `.tar.gz` file from the NetApp Support Site.
- You should have the same custom SnapMirror schedules on both source and destination ONTAP clusters before you run the SRA workflows.
- Enable ONTAP tools for VMware vSphere services to enable the SRA capability.

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.

After a failover, actions such as expand, mount, and delete might not be available for datastores. Perform datastore discovery to refresh and display the appropriate context menu actions.

After each reprotect operation, you must perform storage discovery on both sites.

In a new setup with SRA protection, always run a test failover. Skipping the test failover might cause the reprotect operation to fail.

In a fan-out configuration, after a SnapMirror Active Sync failover where the SnapMirror source changes to site B for Automated Failover Duplex and Asynchronous SnapMirror, run a test failover between sites B and C. Skipping this step may result in a failed reprotect operation.

Related information

Configure disaster recovery for NFS datastores using VMware Site Recovery Manager

Configure SRA in ONTAP tools 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

Before you begin

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

- VMware Live Site Recovery: The VMware site provides installation documentation for VMware Live Site Recovery.

  About VMware Live Site Recovery

- SRA: Install the adapter 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 and Fibre Channel 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

Before you begin

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

- VMware Live Site Recovery: You can find installation documentation for VMware Live Site Recovery on the VMware site - About VMware Live Site Recovery
- SRA: Install the adapter 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 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. Do not use the NFS hostname in the **NFS Addresses** field.

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 in ONTAP tools 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
`StorageProvider.resignatureTimeout`	Increase the value of the setting from 900 seconds to 12000 seconds.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Set a high value (For example: 99999)

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

Refer to Change Storage Provider Settings for more information on modifying 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 don't need to wait for the maximum timeout to be reached. Most commands finish within the set maximum timeout interval.

Refer to Change Storage Settings for modifying SAN Provider settings.

Configure SRA on the VMware Live Site Recovery appliance using ONTAP tools

After deploying the VMware Live Site Recovery appliance, configure the Storage Replication Adapter (SRA) to enable disaster recovery management.

Configuring SRA on the VMware Live Site Recovery appliance saves the ONTAP tools for VMware vSphere credentials within the appliance, enabling communication between VMware Live Site Recovery and SRA.

Before you begin

- Download the *.tar.gz* file from the NetApp Support Site.
- Enable SRA services in ONTAP tools Manager. For more information, refer the Enable services section.

- Add vCenter Servers to the ONTATP tools for VMware vSphere appliance. For more information, refer the Add vCenter Servers section.
- Add storage backends to ONTAP tools for VMware vSphere. For more information, refer the Add storage backends section.

> If you have applied the vCenter certificate patch from ONTAP tools, update the vCenter configuration in the VMware Live Site Recovery appliance using the (:5480) port. For instructions, refer to Reconfigure the Site Recovery Manager Appliance.

Steps

1. On the VMware Live Site Recovery appliance screen, select **Storage Replication Adapter** > **New Adapter**.
2. Upload the *.tar.gz* file to VMware Live Site Recovery.
3. Log in to the VMware Live Site Recovery appliance using an administrator account through an SSH client such as PuTTY.
4. Switch to the root user using the command: `su root`
5. Run the command `cd /var/log/vmware/srm` to go 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>`
   - Provide the password in single quotes so the Perl script treats special characters as part of the password, not as delimiters.
   - You can set the application (VASA Provider/SRA) username and password in ONTAP tools Manager when enabling these services for the first time. Use these credentials to register SRA with VMware Live Site Recovery.
   - To locate the vCenter GUID, go to the vCenter Server page in ONTAP tools Manager after adding your vCenter instance. Refer to Add vCenter Servers section.
9. Rescan the adapters to confirm that the updated details appear on the VMware Live Site Recovery Storage Replication Adapters page.

Results

A confirmation message appears indicating that the storage credentials have been saved.
You can now use SRA to communicate with the SRA server using the specified IP address, port, and credentials.

Update SRA credentials in ONTAP tools

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.

Before you begin

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 protected and recovery sites in ONTAP tools

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

When you add a new datastore, you can include it in the existing datastore group or add a new datastore and create a new volume or consistency group for protection. After adding a new datastore to a protected consistency group or volume, update SnapMirror and perform storage discovery on both the protected and recovery sites. You can run discovery manually or on a schedule to ensure the new datastore is detected and protected.

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) supports fan-out with one sync relationship of type Automated Failover Duplex and async relationship SnapMirror on consistency group. However, fan-out with two async SnapMirror on consistency group or fan-out SnapMirrors on Volume is not supported. Vault type SnapMirror relationships are not considered within these fan-out restrictions.

Before you begin

- 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. On the vSphere Client home page, double-click the **Site Recovery** icon and then select **Sites**.

2. Select **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 select **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 select **Finish**.
5. If prompted, select **Yes** to accept the security certificates.

Result

The **Objects** dialog box displays both the protected and recovery sites.

Configure protection groups

Before you begin

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 select **Site Recovery** > **Protection Groups**.
2. In the **Protection Groups** pane, select **New**.
3. Specify a name and description for the protection group, direction and select **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 select **Next**.

   All the virtual machines on the replication group are added to the protection group.
6. You can select either the existing recovery plan or create a new one by selecting **Add to new recovery plan.**
7. In the Ready to complete tab, review the details of the protection group that you created, and then select **Finish**.

Configure protected and recovery site resources

Configure network mappings in ONTAP tools

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

Before you begin

You should have connected the protected and recovery sites.

Steps

1. Log in to vCenter Server and select **Site Recovery** > **Sites**.
2. Select your protected site and select **Manage**.
3. Select **Network Mappings** > **New** in the manage tab to create a new network mapping.
4. In the Create Network Mapping wizard, do the following:
   a. Select **Automatically Prepare Mappings for Networks with Matching Names** and select **Next**.
   b. Select the required data center objects for the protected and recovery sites and select **Add Mappings**.
   c. Select **Next** after mappings are created successfully.
   d. Select the object used earlier to create reverse mapping, then select **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 in ONTAP tools

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

Before you begin

You should have connected the protected and recovery sites.

Steps

1. Log in to vCenter Server and select **Site Recovery** > **Sites**.
2. Select your protected site and select **Manage**.
3. Select **Folder Mappings** > **Folder** icon in the Manage tab to create a new folder mapping.
4. In the Create Folder Mapping wizard, perform the following:
   a. Select **Automatically Prepare Mappings for Folders with Matching Names** and select **Next**.
   b. Select the required data center objects for the protected and recovery sites and select **Add Mappings**.
   c. Select **Next** after mappings are created successfully.
   d. Select the object used earlier to create reverse mapping and then select **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 in ONTAP tools

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.

Before you begin

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 select **Site Recovery** > **Sites**.
2. Select your protected site and select **Manage**.
3. Select **Resource Mappings** > **New** in the manage tab to create a new resource mapping.
4. In the Create Resource Mapping wizard, perform the following:
   a. Select **Automatically Prepare Mappings for Resource with Matching Names** and select **Next**.
   b. Select the required data center objects for the protected and recovery sites and select **Add Mappings**.
   c. Select **Next** after mappings are created successfully.
   d. Select the object used earlier to create reverse mapping and then select **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 in ONTAP tools

Configure a placeholder datastore to reserve space in the vCenter inventory at the recovery site for protected virtual machines (VMs). Placeholder datastores require minimal capacity, because placeholder VMs are small and typically use only a few hundred kilobytes.

Before you begin

- Ensure that the protected and recovery sites are connected.
- Verify that resource mappings have been configured.

Steps

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

> Placeholder datastores may reside on local or remote storage, but they don’t require replication.

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

Configure SRA using the array manager in ONTAP tools

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).

Before you begin

- 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, select **Array Managers** > **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're connecting to a cluster, you should enter the cluster management LIF.
      - If you're 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 VMware vSphere.
      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 connecting to a cluster, specify the SVM name in the **SVM name** field, or leave it blank to manage all SVMs in the cluster.
   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. Select **Next**.
4. Verify that the array is discovered and displayed at the bottom of the Add Array Manager window and select **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 in ONTAP tools

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.

Before you begin

- 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.
- You should have the same SnapMirror policies and schedules on source and destination sites.

Steps

1. Log in to your vCenter Server.
2. Go 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”.

Fan-out protection in ONTAP tools

In a fan-out protection scenario, the consistency group is double protected with synchronous relationship on the first destination ONTAP cluster and with asynchronous relationship on the second destination ONTAP cluster.
The create, edit, and delete SnapMirror active sync protection workflows maintain the synchronous protection. VMware Live Site Recovery appliance failover and reprotect workflows maintain the asynchronous protection.

Fan-out is not supported for SVM user.

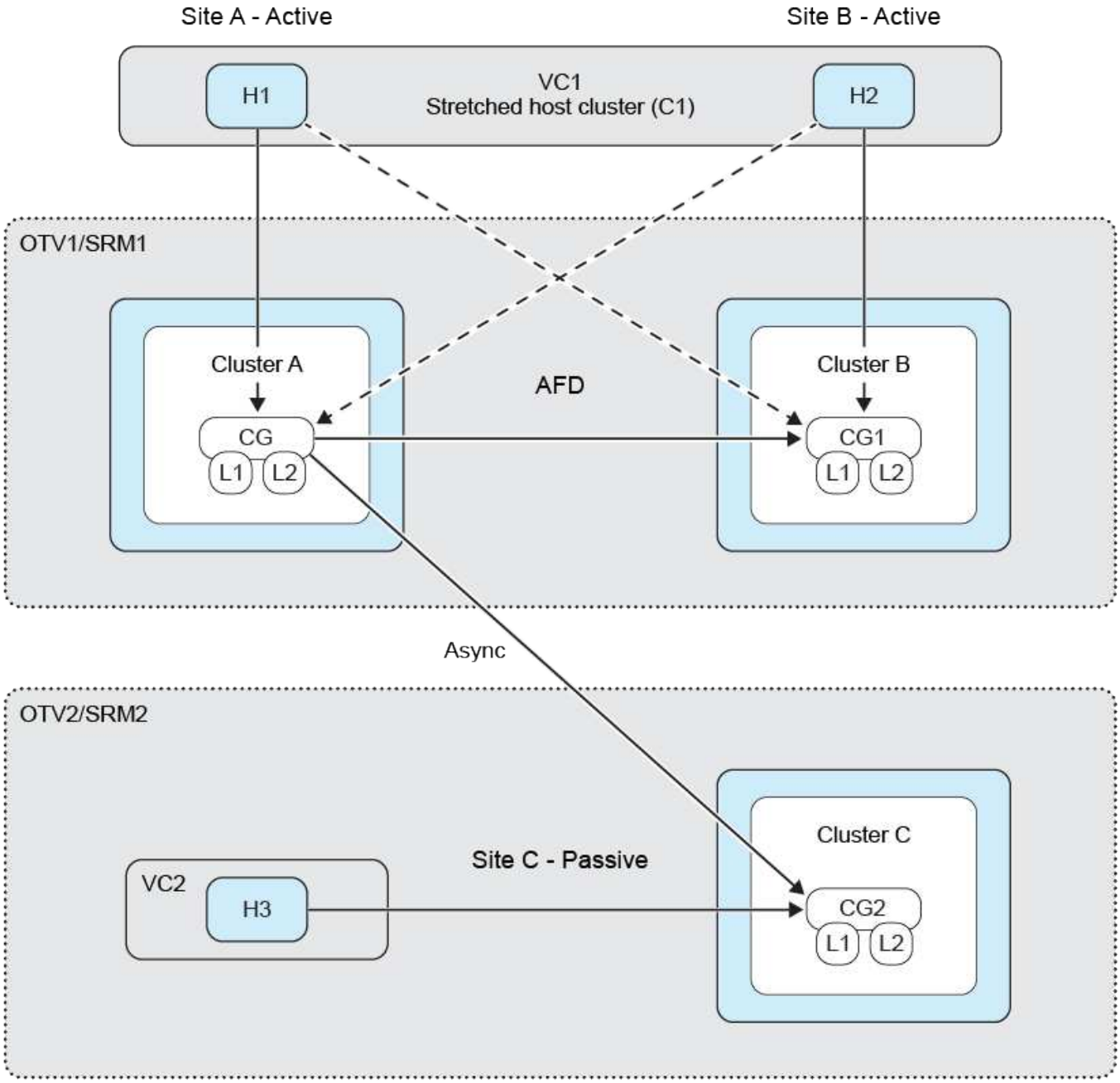
To set up fan-out protection, peer the three site clusters and SVMs.

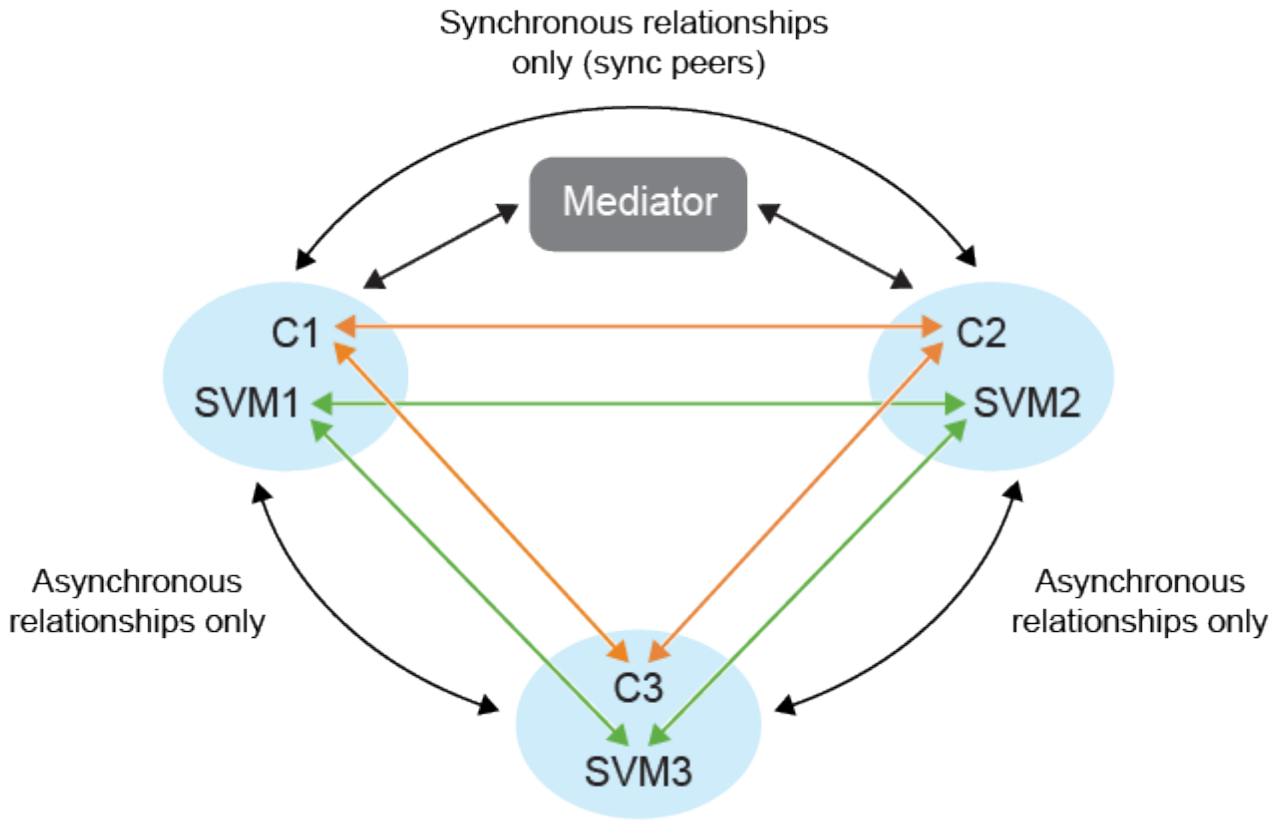
Example:

If	then

• Source consistency group is on cluster c1 and SVM svm1 • First destination consistency group is on cluster c2 and SVM svm2 and • Second destination consistency group is on cluster c3 and SVM svm3	• The cluster peering on source ONTAP cluster will be (C1, C2) and (C1, C3). • The cluster peering on first destination ONTAP cluster will be (C2, C1) and (C2, C3) and • The cluster peering on second destination ONTAP cluster will be (C3, C1) and (C3, C2). • SVM peering on source SVM will be (svm1, svm2) and (svm1, svm3). • SVM peering on first destination SVM will be (svm2, svm1) and (svm2, svm3) and • SVM peering on second destination svm will be (svm3, svm1) and (svm3, svm2).

The following diagram shows the fan-out protection configuration:


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
AFD
Cluster B
CG
L1
L2
CG1
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2



Steps

1. Select a new place holder datastore. The placeholder datastore selection criteria for phased protection are:
   - Do not place the placeholder datastore in the host cluster you are protecting.
   - If you need to include the placeholder datastore in the host cluster, add it to VMware Live Site Recovery appliance before setting up SnapMirror active sync protection. With this setup, you can leave the placeholder datastore out of protection.

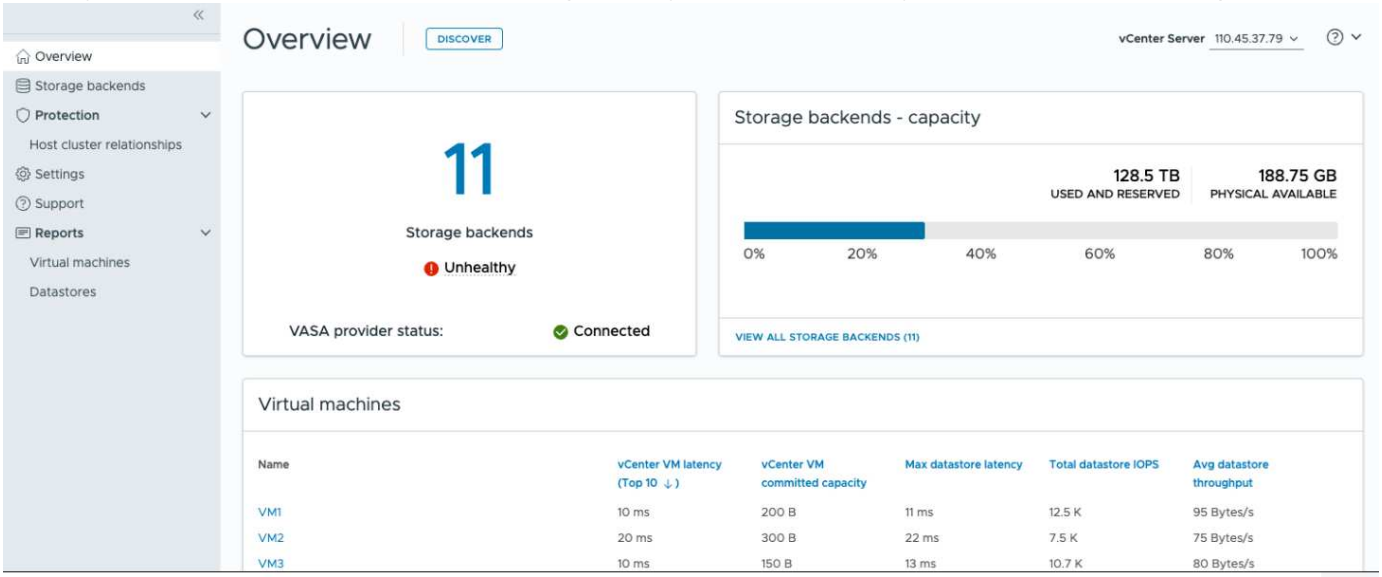
     For more information, refer to Select a Placeholder Datastore
2. Add datastore to the host cluster protection by following Modify protected host cluster. Add both asynchronous and synchronous policy types.

Manage ONTAP tools for VMware vSphere

Learn about the ONTAP tools dashboard

Selecting the ONTAP tools for VMware vSphere plug-in icon from the shortcuts section in the vCenter client opens the overview page. This dashboard provides a summary of the ONTAP tools for VMware vSphere plug-in.

In Enhanced Linked Mode (ELM), the vCenter Server dropdown appears. Choose a vCenter Server to view its data. The dropdown is available in all listing views of the plug-in.
When you select a vCenter Server on one page, it stays the same when you switch tabs in the plug-in.



From the overview page, you can run the **Discovery** action. The discovery action detects newly added or updated storage backends, hosts, datastores, and protection status or relationships at the vCenter level. Run on-demand discovery without waiting for the scheduled discovery.

The **Discovery** action button is enabled only if you have the required privilege to perform the discovery action.

After the discovery request is submitted, you can track the progress of the action in the recent tasks panel.

The dashboard has several cards showing different elements of the system. The following table shows the different cards and what they represent.

Card	Description

Status	The Status card shows the number of storage backends and the overall health status of the storage backends and the VASA Provider. Storage backends status shows **Healthy** when all the storage backends status is normal and it shows **Unhealthy** if any one of the storage backends has an issue (Unknown/Unreachable/Degraded status). Select the tool tip to open the status details of the storage backends. You can select any storage backend for more details. **Other VASA Provider states** link shows the current state of the VASA Provider that is registered in the vCenter Server.
Storage Backends - Capacity	This card shows the aggregated used and available capacity of all storage backends for the selected vCenter Server instance. In case of ASA r2 storage systems, the capacity data is not shown because it is a disaggregated system.
Virtual machines	This card shows the top 10 VMs sorted by performance metric. You can select 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.
Datastores	This card shows the top 10 datastores sorted by a performance metric. You can select 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.
ESXi Host compliance card	This card shows if all ESXi hosts (for the selected vCenter) follow the recommended NetApp host settings by group or category. You can select **Apply Recommended Settings** link to apply the recommended settings. You can select the compliant status of the hosts to see the list of hosts.

How ONTAP tools manages igroups and export policies

Initiator groups (igroups) are tables of FC protocol host World Wide Port Name (WWPNs) or iSCSI host qualified node names. You can define igroups and map them to LUNs to control which initiators have access to LUNs.

In ONTAP tools for VMware vSphere 9.x, igroups were created and managed in a flat structure, where each datastore in vCenter was associated with a single igroup. This model limited flexibility and reuse of igroups

across multiple datastores.
ONTAP tools for VMware vSphere introduces nested igroups, where each datastore in vCenter is associated with a parent igroup, while each host is linked to a child igroup under that parent. You can define custom parent igroups with user-defined names for reuse across datastores to make igroup management easier.
Understand the igroup workflow to manage LUNs and datastores in ONTAP tools for VMware vSphere. Different workflows generate varying igroup configurations, as shown in the following examples:

> The names mentioned are for illustration purposes only and don't refer to real igroup names. ONTAP tools managed igroups use the prefix "otv_". Custom igroups can be given any name.

Term	Description
DS<number>	Datastore
iqn<number>	Initiator IQN
host<number>	Host MoRef
lun<number>	LUN ID
<DSName>Igroup<number>	Default (ONTAP tools-managed) parent igroup
<Host-Moref>Igroup<number>	Child igroup
CustomIgroup<number>	User-defined custom parent igroup
ClassicIgroup<number>	Igroup used in ONTAP tools 9.x versions.

Example 1:

Create datastore on a single host with one initiator

Workflow: [Create] DS1 (lun1): host1 (iqn1)

Result:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)

ONTAP creates the parent igroup DS1Igroup for DS1 and maps the child igroup host1Igroup to lun1. The system always maps LUNs to child igroups.

Example 2:

Mount existing datastore to an additional host

Workflow: [Mount] DS1 (lun1): host2 (iqn2)

Result:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

ONTAP tools for VMware vSphere create a child igroup host2Igroup and add it to the existing parent igroup DS1Igroup.

Example 3:

Unmount a datastore from a host

Workflow: [Unmount] DS1 (lun1): host1 (iqn1)

Result:

- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

ONTAP tools for VMware vSphere remove host1Igroup from the hierarchy. The system does not explicitly delete child igroups. It deletes them under these two conditions:

- If no LUNs are mapped, the ONTAP system deletes the child igroup.
- A scheduled cleanup job removes the dangling child igroups with no LUN mappings.
  These scenarios only apply to ONTAP tools-managed igroups, not custom-created ones.

Example 4:

Delete datastore

Workflow: [Delete] DS1 (lun1): host2 (iqn2)

Result:

- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

Parent and child igroups are removed unless another datastore reuses the parent igroup. Child igroups are not explicitly deleted

Example 5:

Create multiple datastores under a custom parent igroup

Workflow:

- [Create] DS2 (lun2): host1 (iqn1), host2 (iqn2)
- [Create] DS3 (lun3): host1 (iqn1), host3 (iqn3)

Result:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

CustomIgroup1 is created for DS2 and reused for DS3. Child igroups are created or updated under the shared parent, with each child igroup mapping to its relevant LUNs.

Example 6:

Delete one datastore under a custom parent igroup.

Workflow: [Delete] DS2 (lun2): host1 (iqn1), host2 (iqn2)

Result:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun3)
  - host3Igroup → (iqn3: lun3)
- Even though CustomIgroup1 is not reused, it is not deleted.
- If no LUNs are mapped, the ONTAP system deletes host2Igroup.
- host1Igroup is not deleted because it is mapped to lun3 of DS3.
  Custom igroups are never deleted, regardless of the reuse status.

Example 7:
Expand vVols datastore (Add Volume)

Workflow:

Before expansion:

[Expand] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

After expansion:

[Expand] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

A new LUN is created and mapped to the existing child igroup host4Igroup.

Example 8:
Shrink vVols datastore (Remove Volume)

Workflow:

Before Shrink:

[Shrink] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

After Shrink:

[Shrink] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

The specified LUN (lun5) is unmapped from the child igroup. The igroup remains active as long as it has at least one mapped LUN.

Example 9:
Migration from ONTAP tools 9 to 10 (igroup normalization)

Workflow

ONTAP tools for VMware vSPhere 9.x versions don’t support hierarchical igroups. During migration to 10.3 or above versions, igroups must be normalized into the hierarchical structure.

Before migration:

[Migration] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7)
→ ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

ONTAP tools 9.x logic allows multiple initiators per igroup without enforcing one-to-one host mapping.

After migration:

[Migration] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7)
→ ClassicIgroup1:
otv_ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

During migration:

- A new parent igroup (ClassicIgroup1) is created.
- The original igroup is renamed with otv_ prefix and becomes a child igroup.

This ensures compliance with the hierarchical model.

Related topics

About igroups

Export policies

Export policies control NFS datastore access and client permissions in ONTAP tools for VMware vSphere. Export policies are created and managed in ONTAP systems and can be used with NFS datastores to enforce access control. Each export policy consists of rules that specify the clients (IP addresses or subnets) that are allowed access and the permissions granted (read-only or read-write).

When you create an NFS datastore in ONTAP tools for VMware vSphere, you can select an existing export policy or create a new one. The export policy is then applied to the datastore, ensuring only authorized clients can access it.

When you mount an NFS datastore on a new ESXi host, ONTAP tools for VMware vSphere adds the host’s IP address to the existing export policy associated with the datastore. This allows the new host to access the datastore without creating a new export policy.

When you delete or unmount an NFS datastore from an ESXi host, ONTAP tools for VMware vSphere removes the host’s IP address from the export policy. If no other hosts are using that export policy, it will be deleted. When you delete an NFS datastore, ONTAP tools for VMware vSphere removes the export policy associated with that datastore if it is not reused by any other datastores. If the export policy is reused, it keeps the host IP address and does not change.
When you delete the datastores, the export policy unassigns the host IP address and assigns a default export policy, so that the ONTAP systems can access them if required.

Assigning the export policy differs when it is reused across different datastores. When you reuse the export policy, you can append the policy with the new host IP address. When you delete or unmount a datastore that uses a shared export policy, the policy will not be deleted. It remains unchanged, and the host IP address is not removed, because it is shared with the other datastores. Reusing export policies is not recommended, because it can lead to access and latency issues.

Related topics

Create an export policy

How ONTAP tools manages igroups

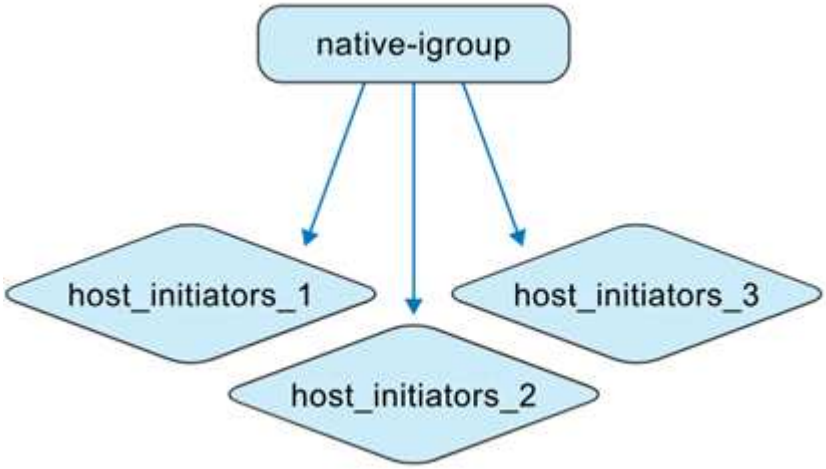
If you manage both ONTAP tools VMs and ONTAP storage systems, it is important to understand how igroups behave, especially when moving datastores from environments not managed by ONTAP tools to those that are. This page explains how igroups are updated during this process.

ONTAP tools for VMware vSphere 10.4 and later version automatically creates and maintains ONTAP and vCenter objects to simplify datastore management in VMware datacenter environments.

ONTAP tools for VMware vSphere interprets igroups in two different contexts:

Non-ONTAP tools managed igroups

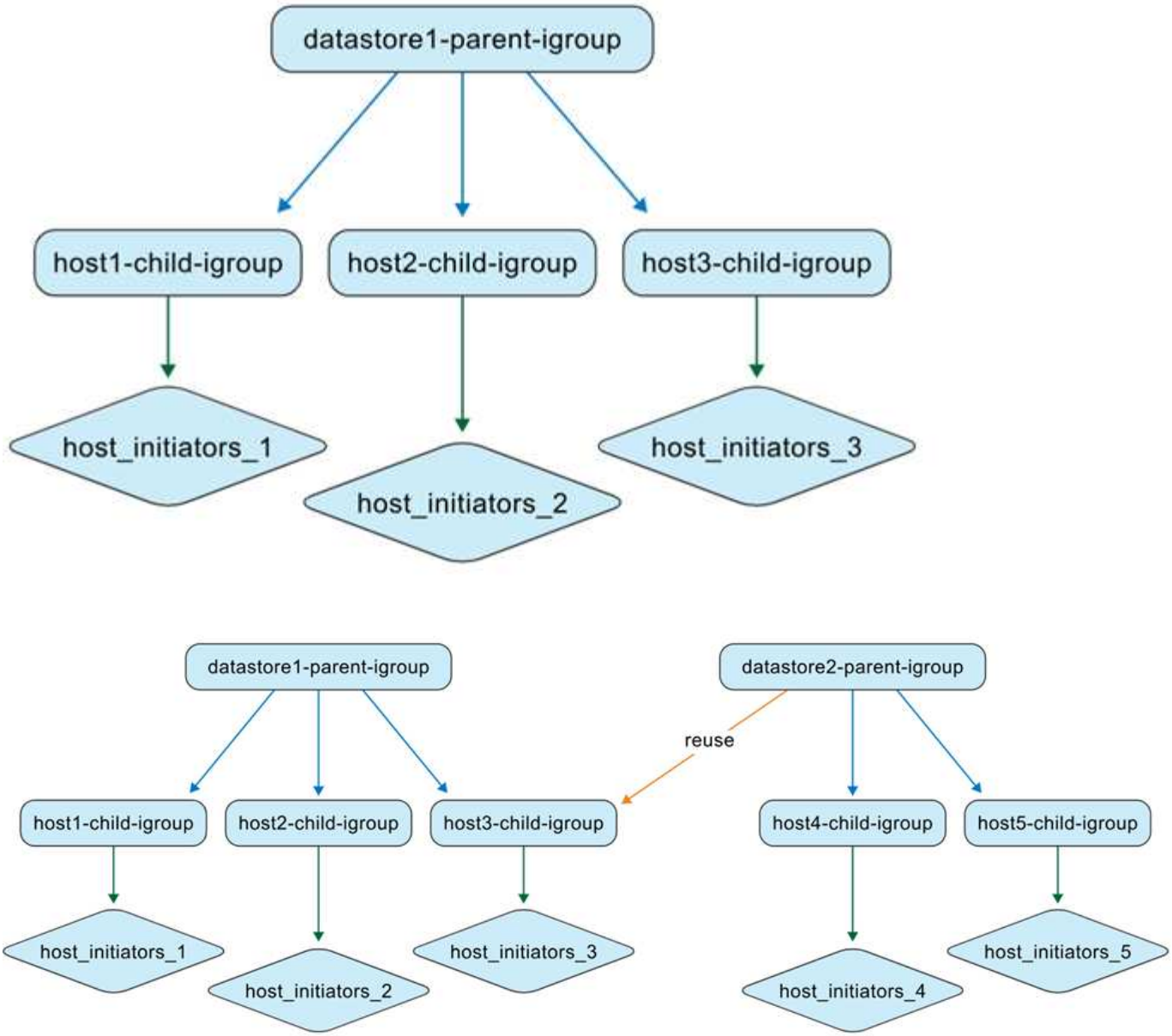
As a storage administrator, you can create igroups on the ONTAP system as flat or nested structures. The illustration shows a flat igroup created in the ONTAP system.



ONTAP tools managed igroups

When you create datastores, ONTAP tools for VMware vSphere automatically creates igroups using a nested structure for easier LUN mapping.

For example, when datastore1 is created and mounted on hosts 1, 2, and 3, and a new datastore (datastore2) is created and mounted on hosts 3, 4, and 5, ONTAP tools reuses the host-level igroup for efficient management.



Here are some cases for ONTAP tools for VMware vSphere supported igroups.

When you create a datastore with default igroup settings

When you create a datastore and leave the igroup field blank (default setting), ONTAP tools automatically generates a nested igroup structure for that datastore. The parent igroup at the datastore level is named using the pattern: otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>. Each host-level child igroup follows the pattern: otv_<hostMoref>_<vcguid>. You can view the association between parent (datastore-level) and child (host-level) igroups in the **Parent Initiator Group** section of the ONTAP storage interface.

With the nested igroup approach, LUNs are mapped only to the child igroups. vCenter Server inventory then displays the new datastore.

When you create a datastore with a custom igroup name

During datastore creation in ONTAP tools, you can enter a custom igroup name instead of selecting from the dropdown. ONTAP tools then creates a parent igroup at the datastore level using your specified name. If the same host is used for multiple datastores, the existing host-level (child) igroup is reused. As a result, the LUN

for the new datastore is mapped to this existing child igroup, which might now be associated with multiple parent igroups (one for each datastore). You can see the new datastore with the custom igroup name in the vCenter Server interface.

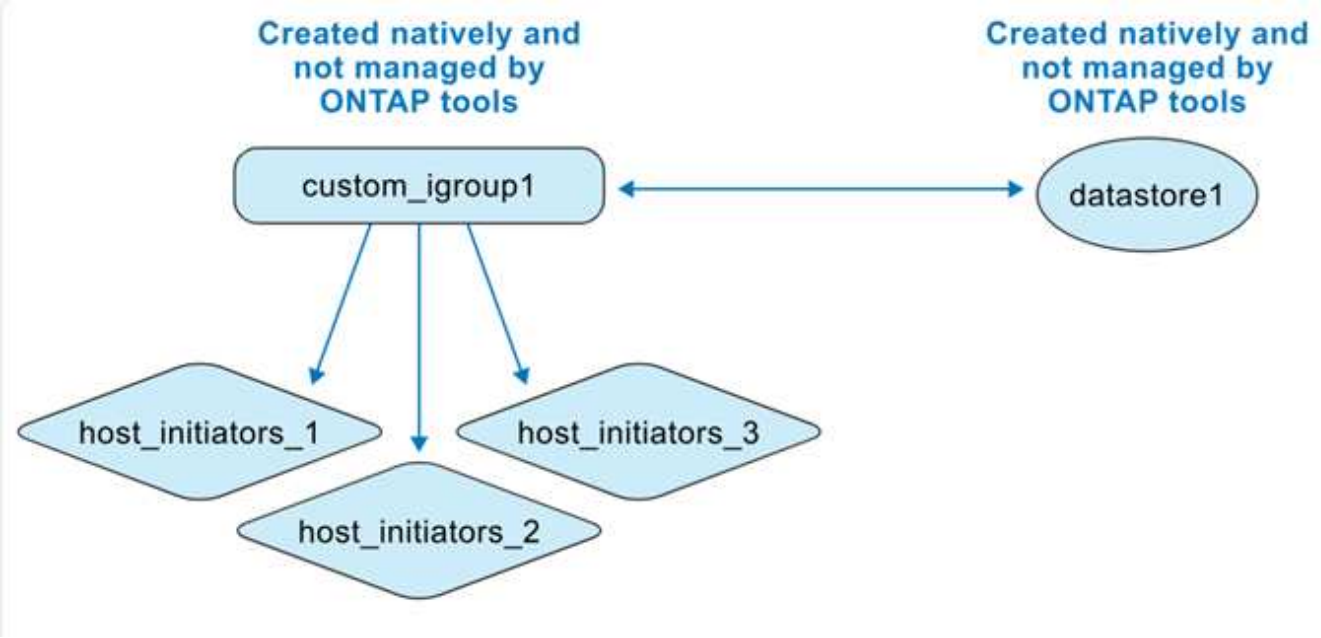
When you reuse the igroup name during datastore creation

When creating a datastore using the ONTAP tools user interface, you can choose an existing custom parent igroup from the drop-down list. After reusing the parent igroup to create another datastore, the ONTAP systems user interface shows this association. The new datastore also appears in the vCenter Server user interface.

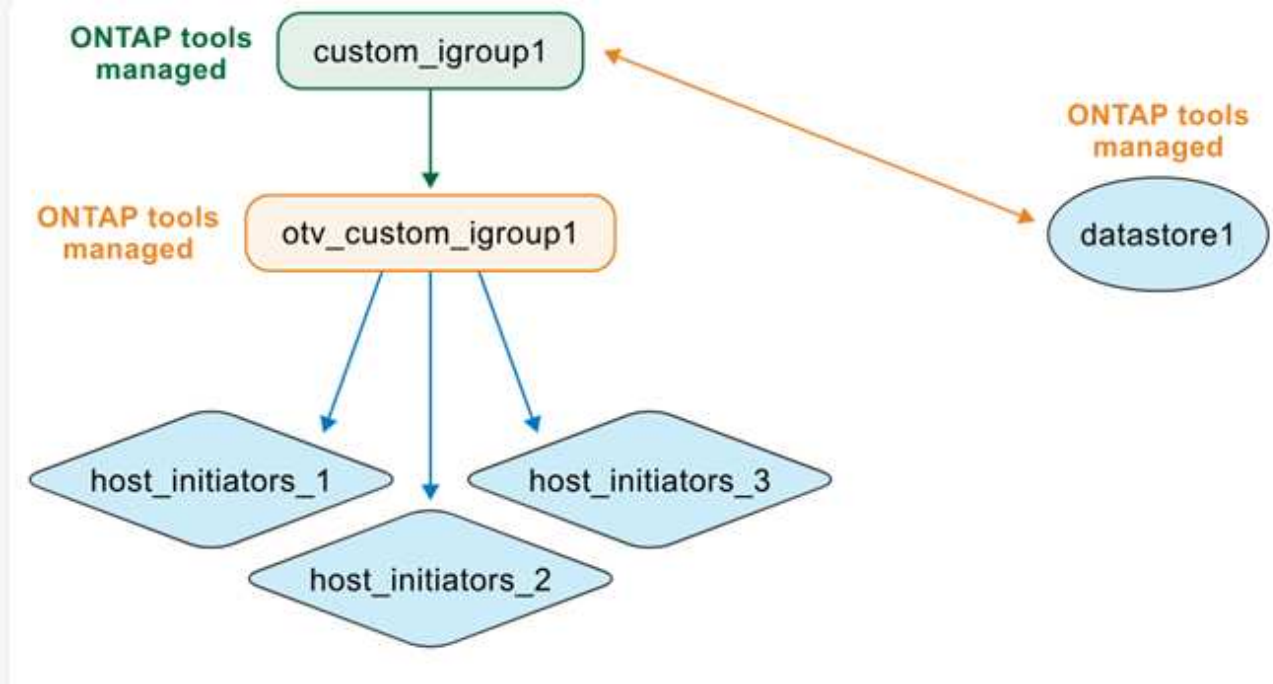
This operation can also be performed using the API. To reuse an existing igroup during datastore creation, specify the igroup UUID in the API request payload.

When you create a datastore and igroup natively from ONTAP and vCenter

If you create the igroup and datastore directly in ONTAP systems and VMware environments, ONTAP tools does not manage these objects at first. This creates a flat igroup structure.



To manage an existing datastore and igroup with ONTAP tools, you should perform a datastore discovery. ONTAP tools identifies and registers the datastore and igroup, and converts them to a nested structure in its database. A new parent igroup is created using the custom name, while the existing igroup is renamed with the "otv_" prefix and becomes the child igroup. The initiator mappings remain unchanged. Only igroups mapped to datastores are converted during discovery. After this, the igroup structure looks like the illustration below.



After you run datastore discovery in ONTAP tools, ONTAP tools converts the flat igroup to a nested structure. ONTAP tools then manages the igroup, renaming it with the 'otv_' prefix. The LUN remains mapped to the same igroup throughout this process.

How ONTAP tools reuse igroups created natively

You can create a datastore in ONTAP tools using an igroup that was first created in ONTAP systems, after ONTAP tools manages it. These igroups appear in the custom initiator group name drop-down list. The new LUN for the datastore is then mapped to the corresponding normalized child igroup, such as "otv_NativeIgroup1".

ONTAP tools for VMware vSphere does not detect or use igroups created in ONTAP system that are not managed by ONTAP tools or linked to a datastore.

Learn about the ONTAP tools Manager user interface

ONTAP tools for VMware vSphere supports multi-tenancy, enabling management of multiple vCenter Server instances.

ONTAP tools Manager is a web-based console for managing ONTAP tools for VMware vSphere, vCenter Server instances, storage backends, and appliance configuration such as High Availability (HA) and node scaling.

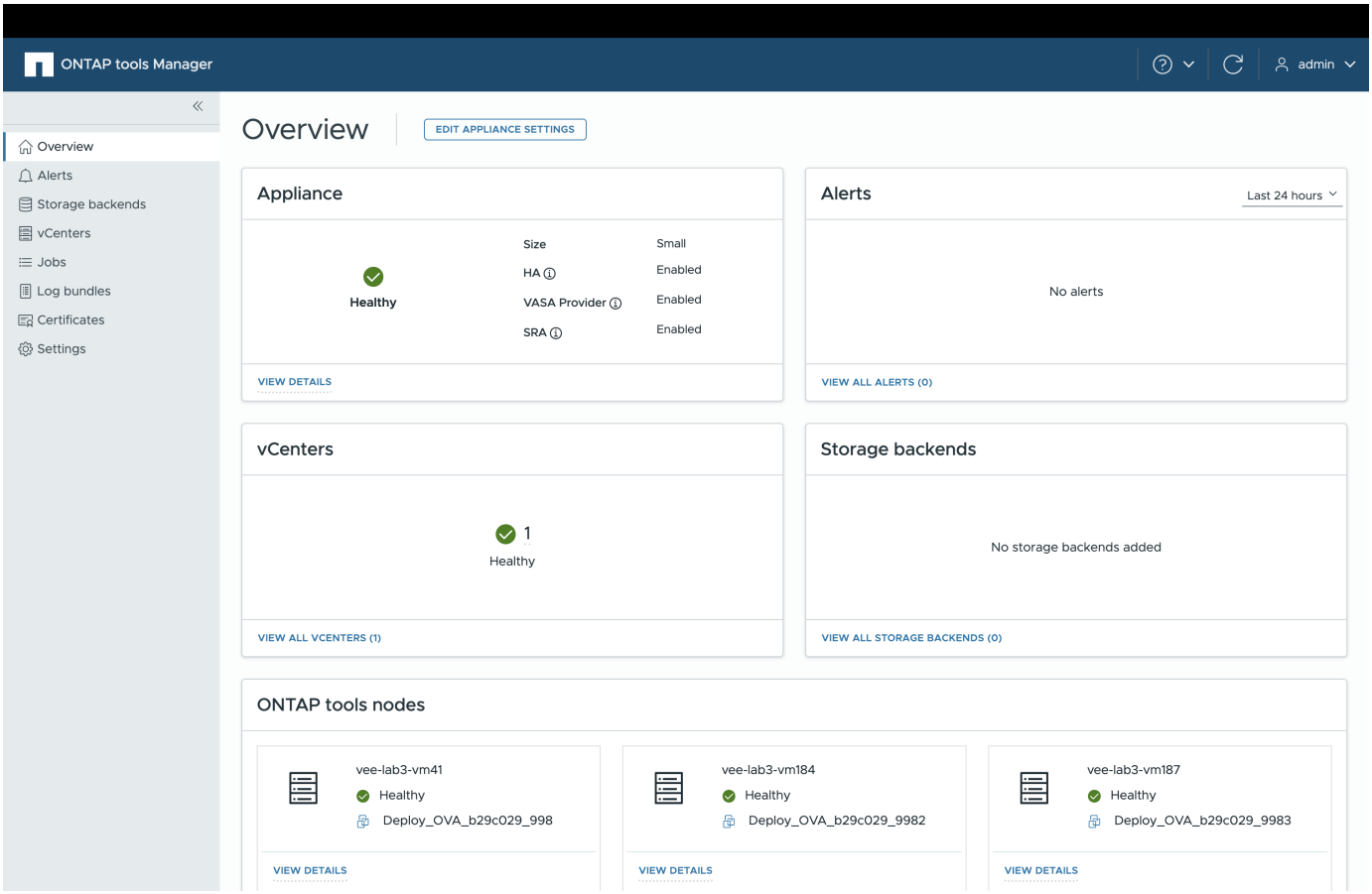
ONTAP tools Manager provides the following capabilities:

- Manage alerts - View and filter alerts generated by ONTAP tools for VMware vSphere.
- Manage storage backends - Add and manage ONTAP storage clusters, and map them to vCenter Server instances globally.
- Manage vCenter Server instances - Add and manage vCenter Server instances within ONTAP tools.
- Monitor jobs - Monitor and debug asynchronous jobs initiated from both the ONTAP tools plug-in interface and ONTAP tools Manager interface. You can filter jobs by time period, adjust page size, and view job

details, including errors and sub-tasks. Click a failed status for error details. For jobs with sub-tasks, expand the row to view descriptions and statuses. For sub-jobs use the job's drilldown to view the details.

- Download log bundles - Collect log files to troubleshoot ONTAP tools for VMware vSphere.
- Manage certificates - Replace the self-signed certificate with a custom CA certificate, and renew or refresh certificates for VASA Provider and ONTAP tools.
- Reset passwords - Change the password for the VASA Provider and SRA.
- Manage appliance settings - Configure the ONTAP tools appliance, including enabling HA and scaling up node sizes.

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



Card	Description
Appliance card	The Appliance card shows the overall status of the ONTAP tools appliance, configuration details, and the status of enabled services. To view more information, select the **View details** link. If you change an appliance setting, the card shows the job status and details until the change is complete.

Card	Description
Alerts card	The Alerts card shows ONTAP tools alerts categorized by type, including HA node-level alerts. You can view detailed alerts by clicking the count hyperlink, which takes you to the alerts page filtered by the selected alert type.
vCenters card	The vCenters card shows the health status of all vCenter Server instances managed by ONTAP tools. You can view details for each vCenter by selecting the corresponding link, which navigates to a page with more information about the selected instance.
Storage backends card	The Storage backends card shows the health and connectivity status of all ONTAP storage clusters configured in ONTAP tools. You can view details for each storage backend by selecting the corresponding link, which navigates to a page with more information about the selected cluster.
ONTAP tools nodes card	The ONTAP tools nodes card shows all nodes in the appliance, including node name, VM name, status, and network information. Select **View details** to see more details for a specific node. [NOTE] In a non-HA configuration, only a single node appears. In an HA configuration, three nodes are displayed.

Manage ONTAP tools Manager settings

Edit ONTAP tools AutoSupport settings

When configuring ONTAP tools for VMware vSphere for the first time, AutoSupport is enabled by default. It sends messages to technical support 24 hours after it is enabled.

Disable AutoSupport

When you disable AutoSupport, you no longer receive proactive support and monitoring.

> It is recommended to keep AutoSupport enabled, as it helps accelerate problem detection and resolution. Even when AutoSupport is disabled, the system continues to collect and store information locally, but it doesn't send reports over the network.

Steps

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

4. Deselect the **AutoSupport** option and save the changes.

Update AutoSupport proxy URL

Update the AutoSupport proxy URL so the AutoSupport feature routes data through the proxy server for secure transmission.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Settings** from the sidebar.
4. Select the **Settings** > **Telemetry** > **Edit** option.
5. Enter a valid **Proxy URL** and save the changes.

   If you disable AutoSupport, the proxy URL is also disabled.

Add NTP servers to ONTAP tools

Enter the NTP server details to synchronize the time clocks of the ONTAP tools appliance.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Settings** > **NTP server** > **Edit** option.
4. Enter the comma-separated fully qualified domain name (FQDN), IPv4, or IPv6 addresses.

   Refresh to screen to see the updated values.

Reset VASA Provider and SRA credentials in ONTAP tools

If you forget your VASA Provider or SRA credentials, you can reset them to a new password using the ONTAP tools Manager interface. The new password must be between 8 and 256 characters long.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Settings** > **VASA Provider / SRA credentials** > **Reset Password** option.
4. Enter the new password and confirm it.

5. Select **Save** to apply the changes.

Edit ONTAP tools backup settings

Beginning with ONTAP tools for VMware vSphere 10.5, the backup feature is enabled by default and a backup is created every 10 minutes. You can disable the backup or edit the frequency of the backup.

Do not disable the backup because it prevents ONTAP tools from maintaining low RPO. Disabling the backup doesn't delete the existing backup files.
You can change the frequency of the backup to a value between 10 and 60 minutes.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Settings** > **Backup** > **Edit** option.
4. In the edit window, you can disable the backup or edit the backup frequency.

Enable ONTAP tools services

You can change the administrator password using ONTAP tools Manager to enable services like VASA Provider, import of vVols configuration, and disaster recovery (SRA) using ONTAP tools Manager.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Edit Appliance Settings** in the overview section.
4. In the **Services** section, you can enable optional services like VASA Provider, import of vVols configuration, and disaster recovery (SRA) as needed.

   When enabling the services for the first time, you must create the VASA Provider and SRA credentials. These are used to register or enable the VASA Provider and SRA services on the vCenter Server. The username can only contain letters, numbers, and underscores. Password length should be between 8 and 256 characters.

   Before disabling any optional services, ensure that the vCenter Servers managed by ONTAP tools don't use them.

   The **Allow import of vVols configuration** option is shown only when the VASA Provider service is enabled. This option enables vVols data migration from ONTAP tools 9.xx to ONTAP tools 10.5.

Change ONTAP tools appliance settings

Use ONTAP tools Manager to scale up the ONTAP tools for VMware vSphere configuration, either by increasing the number of nodes or by enabling High Availability (HA). By default, the ONTAP tools for VMware vSphere appliance is deployed as a single-node, non-HA configuration.

Before you begin

- Ensure that your OVA template has the same OVA version as Node 1. Node 1 is the default node where the ONTAP tools for VMware vSphere OVA is initially deployed.
- Ensure the CPU hot add and memory hot plug are enabled.
- In the vCenter Server, set the Disaster Recovery Service (DRS) automation level to partially automated. After deploying HA, revert it to fully automated.
- Node hostnames in the HA setup should be in lowercase.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select the **Edit Appliance Settings** in the overview section.
4. In the **Configuration** section, scale up the node size and enable HA configuration. Use vCenter Server credentials to make changes.

   In HA configuration, you can change content library details. Provide the password for each edit.

   > In ONTAP tools for VMware vSphere, you're only allowed to increase the node size; you cannot reduce the node size. In a non-HA setup, only a medium-size configuration is supported. In an HA setup, medium and large configurations are supported.

5. Use the HA toggle button to enable the HA configuration. On the **HA settings** page, ensure that:
   - The content library belongs to the same vCenter Server where the ONTAP tools node VMs run. vCenter Server credentials are used to validate and download the OVA template for appliance changes.
   - The virtual machine hosting the ONTAP tools is not directly deployed on an ESXi host. The VM should be deployed on a cluster or a resource pool.

     > After HA configuration is enabled, you cannot revert to a non-HA single node configuration.

6. In the **HA settings** section of the **Edit Appliance Settings** window, you can enter the details of Nodes 2 and 3. ONTAP tools for VMware vSphere supports three nodes in HA setup.

   > ONTAP tools pre-fill most input options with Node 1 network details to simplify the workflow. You can edit the input data before going to the wizard's last page.
   > You can enter IPv6 address details for the other two nodes only when the IPv6 address is enabled on the ONTAP tools management node.

Ensure that an ESXi host contains only one ONTAP tools VM. The inputs are validated each time you move to the next window.

7. Review the details in the **Summary** section and **Save** the changes.

What's next?

The **Overview** page shows the deployment's status. You can also track the edit appliance settings job status from the jobs view by using the job ID.

If HA deployment fails and the new node status is 'New,' delete the new VM in vCenter before trying to enable HA again.

The **Alerts** tab on the left panel lists alerts for ONTAP tools for VMware vSphere.

Add VMware vSphere hosts to ONTAP tools

Add new VMware vSphere hosts to ONTAP tools for VMware vSphere to manage and protect datastores on the hosts.

Steps

1. Add a host to your VMware vSphere cluster following the workflow on page: How to Add an ESX Host to Your vSphere Cluster by Using the Quickstart Workflow
2. After adding the host, go to the ONTAP tools main menu and select **Discover** in the overview panel. Wait for the discovery process to finish. Alternatively, you can wait for the scheduled host discovery to complete.

Result

The new host is now discovered and managed by ONTAP tools for VMware vSphere. You can proceed to manage the datastore on the new host.

Related topics

- Mount a vVols datastore on new hosts.
- Mount NFS and VMFS datastore on new hosts.

Manage datastores

Mount NFS and VMFS datastores in ONTAP tools

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

When you add a new ESXi host using the Add an ESX Host to Your vSphere Cluster workflow, wait for the scheduled host discovery to complete before it shows up in ONTAP tools. Alternatively, you can manually run discovery from the NetApp ONTAP tools overview screen.

About this task

- Some right-click actions are disabled or unavailable depending on the vSphere client version 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.

- vSphere disables the mount datastore option when the host cluster is protected with uniform configurations.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the left navigation pane, select the data centers containing the hosts.
3. To mount NFS/VMFS datastores on a host or a host cluster, right-click and select **NetApp ONTAP tools** > **Mount Datastores**.
4. Select the datastores that you want to mount and select **Mount**.

What's next?

You can track the progress in the recent task panel.

Related topic

Add new VMware vSphere hosts

Unmount NFS and VMFS datastores in ONTAP tools

The Unmount datastore action removes an NFS or VMFS datastore from ESXi hosts. It is available for datastores discovered or managed by ONTAP tools for VMware vSphere.

Steps

1. Log in to the vSphere client.
2. Right-click on a NFS or VMFS datastore object and select **Unmount datastore**.

   The vSphere client opens a dialog box and lists the ESXi hosts that mount the datastore.
   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 user interface 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 exiting protection setting might result in partial protection. Refer to Modify protected host cluster to enable complete protection.

What's next?

You can track the progress in the recent tasks panel.

Mount a vVols datastore in ONTAP tools

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.

When you add a new ESXi host using the Add an ESX Host to Your vSphere Cluster workflow, wait for the scheduled host discovery to complete before it shows up in ONTAP tools. Alternatively, you can manually run discovery from the NetApp ONTAP tools overview screen.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the navigation pane, select the data center 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 select **Mount**.

The recent task panel displays the progress.

Related topic

Add new VMware vSphere hosts

Resize NFS and VMFS datastores in ONTAP tools

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 increase the size of NFS and VMFS datastores. A FlexVol volume in these datastores cannot shrink below its current size but can grow up to 120%.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the navigation pane, select the data center 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, enter a new size for the datastore and select **OK**.

Expand vVols datastores in ONTAP tools

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

Expand vVols datastore operation is not applicable for ASA r2 system-based vVols datastores.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the navigation pane, select the data center 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. Follow the on-screen instructions to make your selection.

5. In the **Summary** window, review the selections and select **Expand**.
   You can track the progress in the recent tasks panel.

Shrink a vVols datastore in ONTAP tools

This page explains how to remove volumes from a vVols datastore.

Use the remove storage from datastore action on any vVols datastore managed by ONTAP tools in vCenter Server.

You cannot remove storage from a volume if it contains vVols; the remove option will be disabled for such volumes. When removing volumes from the datastore, you also have the option to delete the selected volumes from ONTAP storage.

> The shrink vVols datastore operation is not supported for vVols datastores based on ASA r2 systems.

Steps

1. From the vSphere Client home page, select **Hosts and Clusters**.
2. In the navigation pane, select the data center that contains the datastore.
3. Right-click on the vVol datastore and select **NetApp ONTAP tools** > **Remove storage from datastore**.
4. Select volumes that don't have vVols and select **Remove**.

   > The option to select the volume on which 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 select **Delete**.

Delete datastores in ONTAP tools

This page describes how to delete NFS, VMFS, or vVols datastores using ONTAP tools in the vCenter Server.

When you delete a datastore, the following actions are performed depending on the datastore type:

- The vVol container is unmounted.
- If the igroup is not in use, iqn is removed from the igroup.
- The vVol container is deleted.
- Flex volumes are left on the storage array.

You can delete the datastore only if no vVols are present on the selected datastore.

Steps

1. Log in to the vSphere client.
2. Right-click on a host system, a host cluster, or a data center and select **NetApp ONTAP tools** > **Delete datastore**.

You cannot delete a datastore used by virtual machines. Move virtual machines to another datastore before deleting. You cannot delete the volume if it is part of a protected host cluster.

a. In the case of an NFS or VMFS datastore, a dialog box appears with the list of VMs using the datastore.
b. If no virtual machines are associated with a VMFS datastore, you see a confirmation dialog. If host cluster protection is enabled and an AFD relationship exists, you can clean up secondary storage elements.
c. For protected VMFS datastores on ASA r2 systems, remove protection before deleting. Beginning with ONTAP 9.17.1 and ONTAP tools for VMware vSphere 10.5, you can delete a protected datastore. If it is the only datastore in the protection group, host cluster protection removes automatically.
d. For vVols datastores, you can delete the datastore only if there are no vVols present. The **Delete datastore** dialog box includes an option to remove volumes from the ONTAP cluster.
e. For vVols datastores on ASA r2 systems, you cannot delete the backing volumes from ONTAP using the **Delete datastore** option.

3. To delete the backing volumes on ONTAP storage, select **Delete volumes on ONTAP cluster**.

For VMFS datastores on unified ONTAP storage that are part of a protected host cluster, you cannot delete the volume from the ONTAP cluster.

When you delete an NFS, VMFS, or vVols datastore, parent igroups remain on the ONTAP system. Child igroups that are not mapped to any LUNs are deleted automatically. ONTAP tools perform a daily cleanup to remove unmapped default parent igroups. Delete the custom parent igroups manually in ONTAP. ONTAP tools cannot reuse stale parent igroups.

ONTAP storage views for datastores in ONTAP tools

ONTAP tools for VMware vSphere shows the ONTAP storage side view of the datastores and their volumes in the configure tab.

Steps

1. From the vSphere client, go to the datastore.
2. Select the **Configure** tab in the right pane.
3. Select **NetApp ONTAP tools** > **ONTAP Storage**. The view changes by datastore type. See the table below:

Datastore type	Information available
NFS datastore	The **Storage details** page contains storage backends, aggregate, and volume information. The **NFS details** page contains data related to the NFS datastore.

VMFS datastores	The **Storage details** page contains storage backend, aggregate, volume, and storage availability zone (SAZ) details. The **Storage unit details** page contains details of the storage unit.
vVols datastores	Lists all the volumes. You can expand or remove storage from the ONTAP storage pane. ONTAP tools do not support this view for ASA r2 system-based vVols datastores.

Virtual machine storage view in ONTAP tools

The storage view shows the list of vVols that the virtual machine creates.

> This view applies to VMs with at least one disk from an ONTAP tools for VMware vSphere managed vVols datastore.

Steps

1. From the vSphere Client go to the virtual machine.
2. Select 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 in ONTAP tools

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.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, go to **Settings** > **Threshold Settings** > **Edit**.
4. In the **Edit Threshold** window, provide the desired values in the **Nearly Full** and **Full** fields and select **Save**.
   You can restore the threshold values to the recommended defaults: 80 for Nearly Full and 90 for Full.

Manage storage backends in ONTAP tools

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 immediately. For MetroCluster configurations, run ONTAP tools discovery manually after a switchover.

Follow the steps below to discover the storage backends.

Steps

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, go to **Storage Backends** and select a storage backend.
4. Select the vertical ellipses menu and select **Discover storage**

You can track the progress in the recent tasks panel.

Modify storage backends

You can modify the storage backend credentials or the port name. You can also modify the storage backend for global ONTAP clusters using ONTAP tools Manager.
If the certificate will expire in 30 days or less, ONTAP tools shows a warning. Modify the storage backend and upload the new certificate from the ONTAP administrator.

When you modify the storage backend, ONTAP tools for VMware vSphere performs a discovery of the storage backend to update the storage details.

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

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, go to **Storage Backends** and select a storage backend.
4. Select 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.

Modify global ONTAP clusters with ONTAP tools Manager as follows.

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select storage backends from the sidebar.
4. Select the Storage Backend you want to modify.
5. Select 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 must remove all datastores attached to the storage backend before you remove it.
Follow the steps below to remove a storage backend.

1. Log in to the vSphere client.
2. In the shortcuts page, select **NetApp ONTAP tools** under the plug-ins section.
3. In the left pane of ONTAP tools, go to **Storage Backends** and select a storage backend.
4. Select the vertical ellipses menu and select **Remove**. Ensure that the storage backend doesn't 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://<ONTAPtoolsIP>: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. Select 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 that you added, but not on the individual child SVM under the cluster.

Select the parent cluster or child to view the component summary. For the parent cluster, use the actions dropdown to discover storage, modify, or remove the storage backend.

The summary page provides the following details:

- Status of the storage backend
- Capacity information
- Basic information about the VM
- Certificate details such as the certificate status and the expiry date.
- Network information like the IP address and port of the network. For the child SVM, the information is the same as the parent storage backend.
- Privileges allowed and restricted for the storage backend. For the child SVM, the information is the same as the parent storage backend. ONTAP tools show privileges only on the cluster-based storage backends. If you add SVM as the storage backend, privileges information is not shown.
- The ASA r2 system cluster drill-down view doesn't include local tiers tab when the disaggregated property is set as "true" for the SVM or the cluster.
- For ASA r2 SVM systems, the capacity portlet is not shown. The capacity portal is required only when the disaggregated property is set as "true" for the SVM or the cluster.
- For ASA r2 SVM systems, basic information section shows the platform type.

The interface tab provides detailed information about the interface.

The local tiers tab provides detailed information about the aggregate list.

Manage vCenter Server instances in ONTAP tools

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

Dissociate storage backends with the 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 with a storage backend.

Steps

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

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://<ONTAPtoolsIP>: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. Select the vertical ellipses against the vCenter Server that you want to modify and select **Modify**.
5. In the **Modify vCenter** window, enter the username, password, and port details.
6. Upload the certificate and select **Modify**.

Remove a vCenter Server instance

Remove all storage backends from the vCenter Server before removing it.

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

4. Select the vertical ellipses against the vCenter Server that you want to remove and select **Remove**.

> After 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.

Renew vCenter Server certificate

ONTAP tools notifies you when the vCenter certificate is nearing expiration or has expired. After renewing the vCenter certificate, upload the new certificate to ONTAP tools using the following steps:

1. Log in to the ONTAP tools remote diagnostics shell.
2. Obtain the renewed vCenter certificate from the diagnostics shell:

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p'
```

3. Ensure the certificate is in Base 64 ASCII format and includes the beginning and ending lines, for example:

```
---{}BEGIN CERTIFICATE{}---
MIIFUzCCA7ugAwIBAgIJANOgLapcl5oSMA0GCSqGSIb3DQEBCwUAMIGJMQwwCgYD
VQQDDAN2YzExFDASBgoJkiaJk/IsZAEZFgRkZW1vMRUwEwYKCZImiZPyLGQBGRYF
bG9jYWwxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRwwGgYDVQQK
DBN2YzEuZGVtby5uZXRhcHAuY29tMQwwCgYDVQQLDANMT0QwHhcNMjQwNDA1MTgw
NTE4WhcNMjYwNDA1MTgwNTE4WjBzMRwwGgYDVQQDDBN2YzEuZGVtby5uZXRhcHAu
Y29tMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJ
UGFsbyBBbHRvMQ8wDQYDVQQKDAZOZXRBcHAxDDAKBgNVBAsMA0xPRDCCAaIwDQYJ
KoZIhvcNAQEBBQADggGPADCCAYoCggGBALU8OCWMtA2gvIC/OTw/7xucvPVuM+b8
DhzvNpQ2phjfr6ctEhbntPpqPdu+t2CKK7l0mzg3D9cJ/rvMvdDDXr0tgaD1oi2u
ZDW0CaF0QhLOpNfRXMoogBZ66csEhViAy3CHTcOse770mA/PyoHgrCPZngVlZIiQ
TIWpdQMbEEzFIkrLfC70UW2MzfublrsH7Dn/kOu/iCSlVJWixKf7SmZtVQ5ZxBTD
UlJSiqoX1eRXGyunArEvrIpOY9kkKXUElm3hGnk/ZmiuBJ+HqUYqYW+H+7vE3lKa
6NEqDX+tZotxTx2bXMjeiIWU30ZbshgeXlIG9qc49clBoC9iGjavhctOcaXg/W3h
dLKK5ds3rpRERgMg6VMkrfiqAJuiq+b3sTvXMAul/3hL7hz5QABAE/hP4ZvIHV02
WWDQRLiuVFAcDAyvCrO9Irx0Gk1RyRShKYakdWxZ3hhMdLuGq0yvRXqo1Ib94zwO
JfBJHjFToA/GqwromZgiTzJkKq5xbN8MFwIDAQABo4HSMIHPMAsGA1UdDwQEAwIF
4DA7BgNVHREENDAygRVlbWFpbEBkZW1vLm5ldGFwcC5jb22HBMCoAB+CE3ZjMS5k
ZW1vLm5ldGFwcC5jb20wHQYDVR0OBBYEFJ0V0zY+JRpFrEt31ovAY4BLFXmAMB8G
A1UdIwQYMBaAFENf6fRxWF3OJQNTPIdUpK6kjA78MEMGCCsGAQUFBwEBBDcwNTAz
BggrBgEFBQcwAoYnaHR0cHM6Ly92YzEuZGVtby5uZXRhcHAuY29tL2FmZC92ZWNz
L2NhMA0GCSqGSIb3DQEBCwUAA4IBgQBaDfk7GBM4vmhzYCqGrr6KB+h3qeTJ+Y0Y
5nIPRP1HucawDQ8QTay605ddJ8gFGoxkOQDn9tdXWXGjnTRFOT8R+Hw/nUfVSiDP
sYienb16copzUNwtqh+m9Ifow74Gf+ulRzEC0EAVO1X/nTEYH6NKM6Wy7y7F8g5J
lrpM3JY90ZChMqHO3Av/88rbErfQ/gU1brJ3u9Gks4e20Z7Ff312ZKhWRuJDlN2Z
0tc/gp90N9GxaVvELovq/pdjaZ8xiXCxa6piicrJd9WnqMH1gmxP2PIBDxMDBWBG
gwsfs5H7VG9MJYks6lViNsGclo0EwEdF0MfoB3JtsWpPWq6+jBua0Jm7/aFCU+Ht
mykr0gaV7muegoiBQuDma4EkAI31D7ZlUgJQaw157NTk4RW3TFcbtViBHJkM54Hr
iVm0cl+2BZNi/QTMh/MkWV2dYXJ3NuNlqqfzFY+bUfkzkR4SneMk0HX3joNNYDJv
siO7bL+k/Pxql27NVIhuCoVJAlcI7ak=
---{}END CERTIFICATE{}---
```

4. Copy the output and save it as a text file with a `.pem` extension on your desktop.
5. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
6. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
7. Select the applicable vCenter Server instance from the sidebar
8. Select the vertical ellipses against the vCenter Server that you want to modify and select **Modify**.
9. In the **Modify vCenter** window, enter the username, password, and port details.
10. Upload the certificate and select **Modify**.

Related information

Configure remote diagnostic access

Manage ONTAP tools certificates

A self-signed certificate is generated for ONTAP tools and VASA Provider by default during deployment. You can use the ONTAP tools Manager interface to renew this certificate or replace it with a custom CA certificate. In multi-vCenter deployments, using custom CA certificates is required.

Before you begin

You should have the following before you begin:

- The domain name mapped to the virtual IP address.
- Successful nslookup of the domain name, confirming it resolves to the correct IP address.
- Certificates created with the domain name and the ONTAP tools IP address.

> A ONTAP tools IP address should map to a fully qualified domain name (FQDN). Certificates should contain the same FQDN mapped to the ONTAP tools IP address in subject or subject alternative names.

> You cannot switch from a CA-signed to a self-signed certificate.

Upgrade ONTAP tools certificate

ONTAP tools tab shows details like certificate type (self-signed/CA signed) and domain name. During deployment, self-signed certificate is generated by default. You can renew the certificate or upgrade the certificate to CA.

Steps

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

   You can renew the certificate if it has expired or is nearing its expiration date. The renew option is available when the certificate type is CA-signed. In the pop-up window, provide the server certificate, private key, root CA, and intermediate certificate details.

   The system will be offline until the certificate is renewed, and you will be logged out of the ONTAP tools Manager interface.

4. To upgrade the self-signed certificate to custom CA certificate, select **Certificates** > **ONTAP tools** > **Upgrade to CA** option.
   a. In the pop-up window, upload the server certificate, server certificate private key, root CA certificate, and intermediate certificate files.
   b. Enter the FQDN of the Load Balancer IP for which you generated this certificate and upgrade the certificate.

   The system will be offline until the upgrade is complete, and you will be logged out of the ONTAP tools Manager interface.

Upgrade VASA Provider certificate

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 manage multiple vCenter Server instances and want to enable vVols capability on them, you need to change the self-signed certificate to a custom CA certificate.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with the ONTAP tools for VMware vSphere administrator credentials you provided during deployment.
3. Select **Certificates** > **VASA Provider** or **ONTAP tools** > **Renew** to renew the certificates.
4. Select **Certificates** > **VASA Provider** or **ONTAP tools** > **Upgrade to CA** to upgrade the self-signed certificate to custom CA certificate.
   a. In the pop-up window, upload the server certificate, server certificate private key, root CA certificate, and intermediate certificate files.
   b. Enter the FQDN of the Load Balancer IP for which you generated this certificate and upgrade the certificate.

The system will be offline until the upgrade is complete, and you will be logged out of the ONTAP tools Manager interface.

Access ONTAP tools for VMware vSphere maintenance console

Learn about the ONTAP tools maintenance console

The maintenance console for ONTAP tools for VMware vSphere enables you to manage application, system, and network settings. You can update administrator and maintenance passwords, generate support bundles, configure log levels, manage TLS settings, and enable remote diagnostics.

After deploying ONTAP tools for VMware vSphere, if the maintenance console is not accessible, install the VMware tools from the vCenter Server. Log in using the `maint` username and the password set during deployment. Use **nano** to edit files in the 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 select  , the maintenance console starts.

Console Menu	Options
Application Configuration	1. Display server status summary 2. Change LOG level for ONTAP tools services 3. Change cert validation flag
System Configuration	1. Reboot virtual machine 2. Shutdown virtual machine 3. Change 'maint' user password 4. Change time zone 5. Increase jail disk size (/jail) 6. Upgrade 7. Install VMware Tools

Network Configuration	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	1. Access diagnostic shell 2. Enable remote diagnostic access 3. Provide vCenter credentials for backup 4. Take backup

Configure remote diagnostic access for ONTAP tools

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

Before you begin

Enable the VASA Provider extension for your vCenter Server instance.

About this task

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

- you’re 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 expires at midnight the next day.
  - You log in as a diag user again using SSH.

Steps

1. From the 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 ONTAP tools nodes

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

Before you begin

Enable the VASA Provider extension for your vCenter Server instance.

About this task

Repeat this procedure on each node before upgrading.

Steps

1. From the 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 vCenter Server credentials in ONTAP tools

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

Before you begin

You need to have maintenance user login credentials.

About this task

If you changed vCenter Server credentials after deployment, update them using this procedure.

Steps

1. From the 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 `8` to change vCenter credentials.

Change certificate validation flag in ONTAP tools

By default, the certificate validation flag is enabled (set to true). You can set the ONTAP storage backend certificate validation flag to false if you need to bypass SAN certificate checks. This setting is not applicable to vCenter Server certificates.

Before you begin

You need to have maintenance user login credentials.

Steps

1. From the vCenter Server, open a console to ONTAP tools.
2. Log in as the maintenance user.

3. Enter `1` to select **Application Configuration** menu.
4. Enter `3` to change cert validation flag.

   The maintenance console shows the certificate validation flag status and prompts you to change it.

5. Enter 'y' to toggle the flag or 'n' to cancel.

When you enable the certificate validation flag (set to true), ONTAP tools checks that all storage backends use certificates with a Subject Alternative Name (SAN). If any backend uses a certificate without a SAN, you cannot enable certificate validation. Before enabling this flag, verify that all storage backends use SAN-based certificates. If you disable the certificate validation flag (set to false), ONTAP tools bypasses certificate validation for all configured storage backends.

ONTAP tools reports

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, the interface displays all the disk-related datastore information.

The datastores report lists ONTAP tools for VMware vSphere discovered or recognized datastores that use any ONTAP storage, with performance metrics.

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

Manage virtual machines

Virtual machine migration and cloning considerations for ONTAP tools

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

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 you migrate the virtual machine to a different FlexVol volume, the system updates the metadata file for that volume 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 doesn't support virtual machines cloned to a VM template.

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

Refer to Creating a Virtual Machine for Cloning for more details.

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're expected to delete memory snapshot before enabling protection for the virtual machine.

For a Windows VM with the ASA r2 storage type, a snapshot of the virtual machine is read-only.
When you power on the VM, VASA Provider creates a LUN from the read-only snapshot and enables IOPS.
When you power off the VM, VASA Provider deletes the LUN and disables IOPS.

Migrate virtual machines to vVols datastores in ONTAP tools

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.

Before you begin

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 select **Migrate**.
2. Select **Change storage only** and then select **Next**.
3. Select a virtual disk format, a VM Storage Policy, and a vVol datastore that matches the features of the datastore that you're migrating.
4. Review the settings and select **Finish**.

Clean up VASA configurations in ONTAP tools

To complete the VASA cleanup process, follow these steps.

It is recommended to remove any vVols datastores before starting 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.

Attach or detach a data disk from a VM in ONTAP tools

Follow these steps to attach or detach data disks from virtual machines in vSphere and manage their storage resources.

Attach a data disk to a virtual machine

Attach a data disk to a virtual machine to add more storage.

Steps

1. Log in to the vSphere client.
2. Right-click on a virtual machine in the inventory and select **Edit Settings**.
3. On the **Virtual Hardware** tab, select **Existing hard disk**.
4. Select the virtual machine where the disk exists.
5. Select the disk you want to attach and select the **OK** button.

Result

The hard disk appears in the Virtual Hardware devices list.

Detach a data disk from the virtual machine

Detach a data disk from a virtual machine when you don't need it anymore. The disk is not deleted; it stays on the ONTAP storage system.

Steps

1. Log in to the vSphere client.
2. Right-click on a virtual machine in the inventory and select **Edit Settings**.
3. Move your pointer over the disk and select **Remove**.

The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files aren't deleted.

Related information

Add a New Hard Disk to a Virtual Machine

Add an Existing Hard Disk to a Virtual Machine

Discover storage systems and hosts in ONTAP tools

When ONTAP tools for VMware vSphere is launched in the vSphere Client for the first time, it automatically discovers ESXi hosts, their associated LUNs and NFS exports, as well as the NetApp storage systems that own these resources.

Before you begin

- Ensure all ESXi hosts are powered on and connected.
- Ensure all storage virtual machines (SVMs) to be discovered are running, and each cluster node has 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 existing ones to get the latest capacity and setup details. You can also change ONTAP tools for VMware vSphere credentials for storage system access.

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 on the required data center and select **NetApp ONTAP tools** > **Update Host Data** .

   In the **Confirm** dialog box, confirm your choice.

3. Select the discovered storage controllers that have the status `Authentication Failure` and select **Actions** > **Modify**.
4. Fill in the required information in the **Modify Storage System** dialog box.
5. 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

Use the ONTAP tools dashboard in VMware vSphere to identify configuration issues, select ESXi hosts, review NetApp recommended settings, and apply them.

Before you begin

The ESXi host systems portlet displays issues with ESXi host settings. Select an issue to view the host name or IP address.

Steps

1. Log in to the vSphere client.
2. In the shortcuts page, select **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 use NetApp recommended host settings and select **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 select **Finish**.
   You can track the progress in the recent task panel.

Related information

Configure ESXi host settings

Manage passwords

Change ONTAP tools Manager password

You can change the administrator password using ONTAP tools Manager.

Steps

1. Launch ONTAP tools Manager from a web browser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in with your ONTAP tools for VMware vSphere administrator credentials.
3. Select 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 and new passwords. The user interface screen shows the password requirements.
5. Select **Change** to apply the changes.

Reset ONTAP tools Manager password

If you forget the ONTAP tools Manager password, you can restore administrator access by using a reset token generated from the ONTAP tools for VMware vSphere maintenance console.

Steps

1. Open a web browser and navigate to `https://<ONTAPtoolsIP>:8443/virtualization/ui/` to access ONTAP tools Manager.

2. On the login page, select **Reset password**.
3. Generate a password reset token using the ONTAP tools for VMware vSphere maintenance console:
   a. Log in to the vCenter Server and open the maintenance console.
   b. Enter `2` to select **System Configuration**.
   c. Enter `3` to select **Change 'maint' user password**.
4. In the password reset dialog, enter the reset token, username, and new password.
5. Select **Reset** to update the credentials.
6. Log in to ONTAP tools Manager with the new password.

Reset application user password in ONTAP tools

Follow these steps to reset the application user password needed for SRA and VASA Provider registration with vCenter Server using ONTAP tools for VMware vSphere.

Steps

1. Open a web browser and navigate to: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Log in using the administrator credentials configured during ONTAP tools deployment.
3. From the sidebar, select **Settings**.
4. On the **VASA/SRA credentials** page, select **Reset password**.
5. Enter and confirm the new password.
6. Select **Reset** to apply the new password.

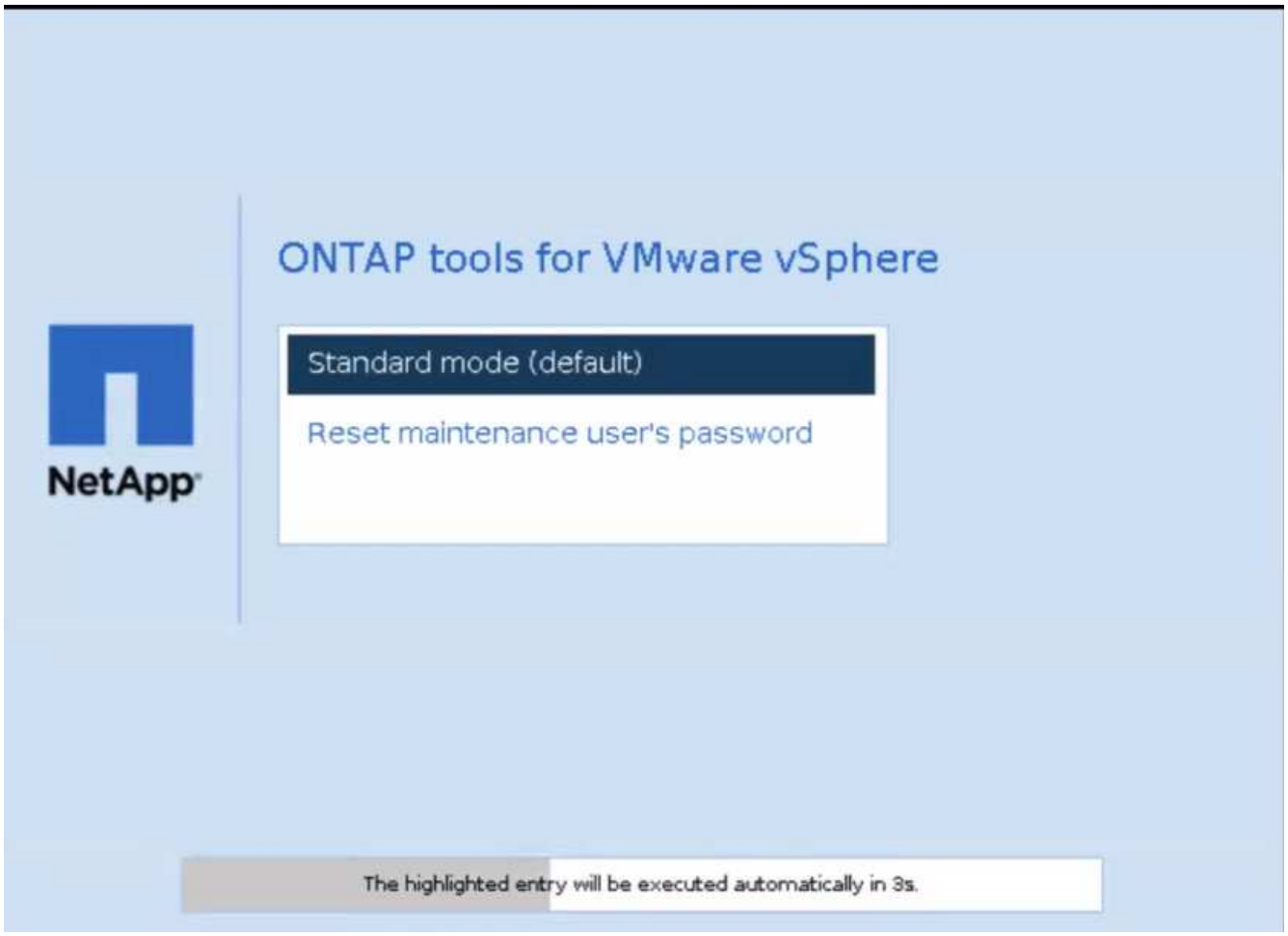
Reset the ONTAP tools maintenance console password

During guest OS restart operation, GRUB menu displays an option to reset maintenance console user password.
Use this option to update the maintenance console user password on the VM. After you reset the password, 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.

> For ONTAP tools for VMware vSphere HA deployment, you should change the maintenance console user password on the ONTAP tools management node, which is node1.

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 and confirm the new password. You have three attempts. The system restarts after you successfully enter the new password.
5. Press **Enter** to continue.
   The system updates the password 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 the **Restart Guest OS** option.

Manage host cluster protection

Modify a protected host cluster in ONTAP tools

You can change protection settings for a host cluster in a single workflow. The following changes are supported:

- 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.

> You need to perform storage discovery after you create, edit, or delete protection for a host cluster to reflect the changes. If you do not perform the storage discovery, the changes are reflected after the periodic storage discovery is triggered.

Monitor host cluster protection

Monitor the protection status, SnapMirror relationships, datastores, and SnapMirror status for each protected host cluster.

Steps

1. Log in to the vSphere client.
2. Go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**.

   The protection column displays an icon that shows the protection status.

3. Hover over the icon to see more details.

Add new datastores or hosts

Add hosts or create datastores on the protected cluster using the vCenter user interface.

Steps

1. Log in to the vSphere client.
2. To edit the properties of a protected cluster, you can either
   a. Go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu next to the cluster and select **Edit** or
   b. Right-click on a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. If you create a datastore in the vCenter user interface, it appears as unprotected. You can view all datastores in the cluster and their protection status in a dialog box. Select the **Protect** button to enable protection.

   > After creating a datastore in the vCenter Server user interface, select **Discover** on the overview page to show the datastore as a candidate for protection in the host cluster. The protection status updates to protected after the next periodic protection discovery.

4. If you add a new ESXi host, the protection status is shown as partially protected. Select the ellipsis menu under the SnapMirror settings and select **Edit** to set the proximity of the newly added ESXi host.

   > For Asynchronous relationships, editing is not supported in ONTAP tools because the target SVM for a tertiary site cannot be added to the same instance. To modify the relationship configuration, use System Manager or the CLI on the target SVM.

5. After making changes, select **Save**.
6. You can see the changes in the **Protect Cluster** window.

ONTAP tools creates a vCenter task, and you can track its progress in the **Recent task** panel.

Add a new SnapMirror relationship

Steps

1. Log in to the vSphere client.
2. To edit the properties of a protected cluster, you can either
   a. Go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu against the cluster and select **Edit** or
   b. Right-click on 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. Select **Protect**.

   You can see the changes in the **Protect Cluster** window.

ONTAP tools creates a vCenter task, and you can track its progress in the **Recent task** panel.

Delete an existing SnapMirror relationship

To delete an SnapMirror asynchronous relationship, ensure that the secondary site SVM or cluster is added as a storage backend in ONTAP tools for VMware vSphere.
You cannot delete all SnapMirror relationships at once. Deleting a relationship also removes the corresponding relationship from the ONTAP cluster.
When you delete an Automated Failover Duplex SnapMirror relationship, the system unmaps the destination datastores and deletes the consistency group, LUNs, volumes, and igroups from the destination ONTAP cluster.

When you delete the relationship, the system rescans the secondary site to remove the unmapped LUN as an active path from the hosts.

Steps

1. Log in to the vSphere client.
2. To edit the properties of a protected cluster, you can either
   a. Go to **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, select the ellipsis menu against the cluster and select **Edit** or
   b. Right-click on a host cluster and select **NetApp ONTAP tools** > **Protect Cluster**.
3. Select the ellipsis menu under the SnapMirror settings and select **Delete**.
   - If you delete an asynchronous policy type-based relationship of a protected host cluster, you must manually remove the storage elements from the tertiary storage cluster. Storage elements include consistency groups, volumes (for ONTAP systems), storage units (LUNs/Namespaces), and snapshots.
   - If you delete an Automated Failover Duplex (AFD) policy-based relationship of a protected host cluster, you can choose to remove the associated storage elements on the secondary storage directly from the interface.
   - If you delete an Automated Failover Duplex (AFD) policy-based relationship and the consistency group is now hierarchical for application-level backups, a warning appears about backup impact. Confirm to proceed. After confirmation, delete the associated storage elements on the secondary storage. If you do not remove them, they remain on the secondary site.

ONTAP tools creates a vCenter task, and you can track its progress in the **Recent task** panel.

Modify an existing SnapMirror relationship

To modify an SnapMirror asynchronous relationship, ensure the secondary site SVM or cluster is added as a storage backend in ONTAP tools for VMware vSphere.
For Automated Failover Duplex SnapMirror relationships, you can update host proximity for uniform configurations or host access for non-uniform configurations.
Changing between Asynchronous and Automated Failover Duplex policy types is not supported.
You can configure proximity or access settings for newly discovered hosts in the cluster.

You cannot edit an existing SnapMirror asynchronous relationship.

Steps

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

ONTAP tools create a vCenter task. Track its progress in the **Recent task** panel.

Remove host cluster protection in ONTAP tools

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

Steps

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

   On this page, monitor protected host clusters, protection state, SnapMirror relationship, and status. Select consistency groups to view capacity, associated datastores, and child groups.

2. In the **Host cluster protection** window, select the ellipsis menu next to the cluster, and select **Remove protection**.
   - If you remove protection from a host cluster with only a SnapMirror asynchronous relationship, you must manually delete the storage elements. Storage elements include consistency groups, volumes (for ONTAP system), storage units (LUNs), and snapshots.
   - If you remove protection from a host cluster with only an automated failover duplex-based SnapMirror policy relationship and a non-hierarchical consistency group, you can delete the associated storage elements on the secondary storage directly from the same screen.
   - If you remove protection from a host cluster with both SnapMirror policies and a hierarchical consistency group for backups, a warning appears about backup impacts. Confirm to proceed. After confirmation, delete the associated storage elements on the secondary storage. If you do not clean up, the storage elements remain on the secondary site.

Recover the ONTAP tools setup

Beginning with ONTAP tools for VMware vSphere 10.5, the backup feature is enabled by default.

The datastore where you deploy ONTAP tools for VMware vSphere virtual machines stores the backup files. A folder named after the ONTAP tools IP address (dots replaced by underscores and suffixed with *OTV_backup*) keeps the two most recent backup files (*OTV_backup_1.tar.enc* and *OTV_backup_2.tar.enc*) and an info file (*OTV_backup_info.txt*) that contains the name of the latest backup.

Ensure that the new virtual machine uses the same ONTAP tools IP address and matches the initial system configuration, including enabled services, node size, and HA mode.

Steps

1. Download the backup files from the datastore of the original virtual machine to your local system.
   a. Go to the storage section and choose the datastore that contains the backup files for the virtual machine.
   b. Select the **Files** section.
   c. Download the required backup directory.
2. Power off the existing virtual machine. Then, deploy a new virtual machine using the same OVA file as the original deployment.
3. From the vCenter Server, open the maintenance console.
4. Log in as the maintenance user.
5. Enter `4` to select **Support and Diagnostics**.
6. Enter `2` to select **Enable remote diagnostic access** option and create a new password for the diagnostic access.
7. Choose a backup file from the downloaded directory. Refer to the *OTV_backup_info.txt* file to identify the latest backup.
8. Use the following command to transfer the backup file to the new virtual machine. When prompted, enter the diagnostic password.

   ```
   scp <OTV_backup_X.tar.enc>
   diag@<node_ip>:/home/diag/system_recovery.tar.enc
   ```

   don’t alter the destination path and file name (/home/diag/system_recovery.tar.enc) mentioned in the command.

9. After the backup file is transferred, log in to the diagnostic shell and run the following command:

   ```
   sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
   ```

   The logs are recorded in */var/log/post-deploy-upgrade.log* file.

After you complete the recovery, ONTAP tools restores services and vCenter objects.

Uninstall ONTAP tools

Uninstalling the ONTAP tools for VMware vSphere deletes all the data in the tools.

Steps

1. Remove or move all the virtual machines from the ONTAP tools for VMware vSphere managed datastores.
   - To remove the virtual machines, refer to Remove and reregister VMs and VM templates
   - To move them to an unmanaged datastore, refer to How to Migrate Your Virtual Machine with Storage vMotion
2. Delete datastores created on ONTAP tools for VMware vSphere.
3. If you have enabled the VASA provider, select **Settings** > **VASA Provider settings** > **Unregister** in ONTAP tools to unregister the VASA providers from all the vCenter servers.
4. Disassociate all storage backends from the vCenter Server instance. Refer to Dissociate storage backends with the vCenter Server instance.
5. Delete all storage backends. Refer to Manage storage backends.
6. Remove the SRA adapter from VMware Live Site Recovery:
   a. Log in as admin to the VMware Live Site Recovery appliance management interface using port 5480.
   b. Select **Storage Replication Adapters**.
   c. Select the appropriate SRA card, and from the drop-down menu, select **Delete**.
   d. Confirm that you know the results of deleting the adapter and select **Delete**.
7. Delete the vCenter server instances onboarded to ONTAP tools for VMware vSphere. Refer to Manage vCenter Server instances.
8. Power off the ONTAP tools for VMware vSphere VMs from the vCenter Server and delete the VMs.

What's next?

Remove FlexVol volumes

Remove FlexVol volumes after uninstalling ONTAP tools

When you use a dedicated ONTAP cluster for ONTAP tools for VMware deployment, it creates many unused FlexVol volumes. After removing ONTAP tools for VMware vSphere, you should remove the FlexVol volumes to avoid possible performance impacts.

Steps

1. Find out the ONTAP tools for VMware vSphere deployment type from the ONTAP tools management node VM.
   Run the following command to check the deployment type:
   cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol

   If it is an iSCSI deployment, delete igroups as well.

2. Get the list of FlexVol volumes.
   kubectl describe persistentvolumes | grep internalName | awk -F'=' '{print $2}'
3. Remove the VMs from the vCenter Server. Refer to Remove and reregister VMs and VM templates.
4. Delete FlexVol volumes. Refer to Delete a FlexVol volume. Enter the exact FlexVol volume name in the CLI

command to delete a volume.

5. Delete SAN igroups from the ONTAP storage system in case of iSCSI deployment. Refer to View and manage SAN initiators and igroups.

Upgrade ONTAP tools for VMware vSphere

Upgrade from ONTAP tools for VMware vSphere 10.x to 10.5

You can upgrade from ONTAP tools for VMware vSphere 10.3 or 10.4 to 10.5. However, to upgrade from ONTAP tools 10.0, 10.1, or 10.2 to 10.5, you must first upgrade to 10.3 or 10.4 before proceeding to 10.5.

- For ASA r2 systems, make sure you upgrade to ONTAP tools for VMware vSphere to 10.5 and ONTAP to 9.16.1, before setting up more storage availability zones (SAZs).
- If the upgrade from ONTAP tools for VMware vSphere 10.3 or 10.4 to 10.5 fails, you cannot roll back. Use low RPO or snapshot recovery to restore the setup. For ONTAP tools for VMware vSphere 10.2 and earlier, use zero-RPO to restore the setup.

Before you begin

- Ensure that all nodes are active.
- Ensure the ONTAP system certificate and onboarded vCenter certificates are valid for at least 5 days. If the certificates expire sooner, the upgrade fails.
- Ensure you have a fifth disk with a capacity of 100 GB on all nodes.
- Verify that the node configuration matches the specifications in the table below.

Deployment Type	CPU(Core) per node	Memory(GB) per node	Disk Space(GB) per node	Total CPU(Core)	Memory(GB)	Total Disk Space(GB)
Non-HA Small	9	18	350	9	18	350
Non-HA Medium	13	26	350	13	26	350
HA Small	9	18	350	27	54	1050
HA Medium	13	26	350	39	78	1050
HA Large	17	34	350	51	102	1050

- Ensure hot plug-in for CPU and RAM is enabled.
- Enable low RPO backup and ensure one backup is visible in vCenter Client interface. Download the backup folder before upgrade.
- Low RPO backup is recommended. However, in non-HA deployment, you can take a quiesced snapshot of the ONTAP tools virtual machine before upgrading.

  Refer to Edit Backup settings and Recover the ONTAP tools setup for more information about backup and recovery.

Steps

1. Upload ONTAP tools for VMware vSphere upgrade ISO to content library.
2. In the primary VM page, select **Actions** > **Edit Settings**. To identify the primary VM name:
   a. Enable diag shell on any node

b. Run the following command:
`grep sourceHost /opt/netapp/meta/ansible_vars.yaml`

3. Select the **content library ISO file** in the edit settings window under the **CD/DVD drive** field.
4. Select the ISO file, check the **Connected** box for the **CD/DVD drive** field, and click **OK**.
5. From the vCenter Server, open a console to ONTAP tools.
6. Log in as the maintenance user.
7. Enter **2** to select the **System Configuration** menu.
8. Enter **7** to select the **Upgrade** option.
9. Provide the vCenter credentials, when prompted. This is the vCenter instance where the ONTAP tools is hosted.

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

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

   During the upgrade, if any onboarded storage backend certificates are missing Subject Alternative Name (SAN) entries, you will receive a prompt indicating the missing SAN. If you choose to proceed without validating the SAN, the upgrade will continue, but this is not recommended because of potential security risks.

10. When you upgrade, the following actions are performed automatically:
    a. The gateway certificate is renewed with a 1-year validity period. When you remove the previous SRA adapter and upload the new 10.5 adapter, the SRA certificate validity changes from 10 years to 1 year.
    b. Remote plug-in is upgraded
    c. ONTAP and vCenter Server certificates are validated and added to ONTAP tools
    d. Backup is enabled

What's next

After upgrading to ONTAP tools for VMware vSphere 10.5:

- Monitor system alerts and plan to renew the gateway certificate before it expires in one year.
- Remove the ONTAP tools 10.4 or 10.3 SRA adapter and upload the 10.5 SRA adapter tar file.
- Run the install command after uploading SRA adapter tar. the Then, rescan the SRA adapters to update the VMware Site Recovery Storage Replication Adapters page.

After upgrading you can:

- Disable the services from the manager user interface
- Move from a non-HA setup to an HA setup
- Scale up a non-HA small configuration to a non-HA medium, or to an HA medium or large configuration.

Related information

ONTAP tools upgrade error codes

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
09	post-deploy-upgrade.pl

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

Upgrade error code	Workflow	Resolution
052	The ISO might be the same as the current version or two releases above the current version.	Use an ISO version compatible to upgrade from your current version.
068	Debian packages rollback has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
069	Failed restoring files	Use zero-RPO or snapshot based recovery and retry upgrade.
070	Failed deleting backup	-
071	Kubernetes cluster was not healthy	-

Upgrade error code	Workflow	Resolution
074	Mount ISO has failed	Check the /var/log/upgrade-run.log and retry upgrade.
075	Upgrade pre-checks has failed	Retry the upgrade.
076	Registry upgrade has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
077	Registry rollback has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
078	Operator upgrade has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
079	Operator rollback has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
080	Services upgrade has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
081	Services rollback has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
082	Deleting old images from container failed	Use zero-RPO or snapshot based recovery and retry upgrade.
083	Deleting backup has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
084	Changing JobManager back to Production failed	Follow the below steps to recover/complete the upgrade. 1. Enable Diagnostic Shell 2. Run the command: *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Check the logs at /var/log/post-deploy-upgrade.log
087	Post upgrade steps failed.	Perform the following steps to recover/complete the upgrade. 1. Enable Diagnostic Shell 2. Run *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* command 3. Check the logs at /var/log/post-deploy-upgrade.log

Upgrade error code	Workflow	Resolution
088	Configuring log rotate for journald has failed	Check the VM network settings compatible with the host on which VM is hosted. You can try to migrate the VM to another host and restart.
089	Changing ownership of summary log rotate config file has failed	Retry the upgrade.
095	OS upgrade failed	No recovery for OS upgrade. ONTAP tools services are upgraded and new pods will be running.
096	Install dynamic storage provisioner	Check the upgrade logs and retry upgrade.
097	Uninstalling services for upgrade has failed	Use zero RPO or snapshot based recovery and retry upgrade.
098	copying dockercred secret from ntv-system to dynamic storage provisioner namespace has failed	Check the upgrade logs and retry upgrade.
099	Failed to validate the new HDD addition	Add the new HDD to all the nodes in case of HA and to one node in case of non-HA deployment.
109	backing up persistent volume data has failed	Check the upgrade logs and retry upgrade.
110	restoring persistent volume data has failed	Use zero-RPO or snapshot based recovery and retry upgrade.
111	Updating etcd timeout parameters for RKE2 has failed	Check the upgrade logs and retry upgrade.
112	Uninstall dynamic storage provisioner has failed	-
113	Refresh resources on secondary nodes has failed	Check the upgrade logs and retry upgrade.
104	Restarting of secondary node has failed	Restart the nodes manually one by one
100	kernel rollback has failed	-
051	dynamic storage provisioner upgrade has failed	Check upgrade logs and retry upgrade.
056	deleting migration backup has failed	NA
090	certificate validation for storage backends and vCenter failed	Check upgrade logs and log file at /var/log/cert_validation_error.log and retry the upgrade.

Beginning with ONTAP tools for VMware vSphere 10.3 zero RPO is not supported.

Learn more about How to restore ONTAP tools for VMware vSphere if upgrade fails from version 10.0 to 10.1

Migrate ONTAP tools for VMware vSphere 9.xx to 10.5

Migrate from ONTAP tools for VMware vSphere 9.xx to 10.5

Moving the NetApp ONTAP tools for VMware vSphere setup from version 9.xx to 10.5 necessitates a migration process because of the significant product updates and enhancements across the versions.

You can migrate from ONTAP tools for VMware vSphere 9.12D1, 9.13D2, and 9.13P2 releases to ONTAP tools for VMware vSphere 10.5.

If you have NFS and VMFS datastores and no vVols datastores in your setup, simply uninstall ONTAP tools 9.xx and deploy ONTAP tools 10.5. However, if your setup contains vVols datastores, you'll have to go through a process of migrating the VASA Provider and the SRA.

The following table outlines the migration process in these two different scenarios.

If the setup has vVols datastores	If the setup contains only NFS and VMFS datastores
Steps: 1. Migrate the VASA Provider 2. Create VM storage policies	Steps: 1. Remove ONTAP tools 9.xx from your environment. Refer to How to remove OTV 9.xx from your environment NetApp Knowledge Base article. 2. Deploy and configure ONTAP tools for VMware vSphere 10.5 3. Update the SRA 4. Create VM storage policies

After migrating from ONTAP tools for VMware vSphere 9.xx to 10.5, vVols datastores using the NVMe/FC protocol become non-operational because ONTAP tools 10.5 supports the NVMe-oF protocol only with VMFS datastores.

Migrate the VASA Provider and update the SRA in ONTAP tools

Follow the steps in this section to migrate the VASA Provider from ONTAP tools for VMware vSphere 9.xx to ONTAP tools for VMware vSphere 10.5 and update the Storage Replication Adapter (SRA) on the VMware Live Site Recovery appliance.

Steps to migrate the VASA Provider

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

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

2. Deploy OVA for ONTAP tools for VMware vSphere 10.5.
3. Add the vCenter Server instance you want to migrate to ONTAP tools for VMware vSphere 10.5 release. Refer to Add a vCenter Server instance for more information.
4. Onboard the storage backend locally from the vCenter server APIs for the ONTAP tools plug-in. Refer to Add a storage backend using the vSphere client interface for more information.
5. Obtain an access token to authenticate REST API requests. Use the following example, replacing the variables with values specific to your environment.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

   Copy and save the access token returned in the response.

6. Issue the following API from Swagger or in Postman to migrate.

```
curl -X POST
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra
tion-jobs`
```

   You can access Swagger through this URL: `https://$FQDN_IP_PORT/`, for example: `https://10.67.25.33:8443/`.

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

```
curl -X POST 'https://<OTV-NG-
IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
--header 'x-auth: <auth_token>' \
--header 'Content-Type: application/json' \
--data '{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "******"
  },
  "database_password": "******"
}'
```

Request body for other release migration:

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*******"
  }
}
```

JSON output example

The system returns a job object. Save the job identifier to use it in the next step.

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

7. Use the following URI in Swagger to check the status:

```
curl
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<migra
tion_id>?includeSubJobsAndTasks=true`
```

   After the job completes, review the migration report in the job response.

8. Add the ONTAP tools for VMware vSphere storage provider to the vCenter Server.
9. Register the VASA Provider with ONTAP tools for VMware vSphere. For instructions, see Register the VASA Provider.
10. After registration, verify the name of the VASA Provider and its status in the vSphere Client under **Storage Providers**. The VASA Provider should appear online, confirming successful registration.
11. Enable VASA Provider service on ONTAP tools for VMware vSphere 10.5.
12. Stop ONTAP tools for VMware vSphere storage provider 9.10/9.11/9.12/9.13 VASA Provider service using these steps:
    a. In ONTAP tools 9.x, open the web console.
    b. Access the maintenance console.
    c. Enter `1` to select the **Application Configuration** menu.
    d. Enter `5` to stop the VASA Provider and SRA services.
    e. In the vSphere Client, navigate to **Inventory** > **Storage Providers**.
    f. Select the ONTAP tools 9.x VASA Provider from the storage backend and click **Remove**.

       After the old VASA Provider is stopped, the 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.

13. Migrated NFS and VMFS datastores appear in ONTAP tools for VMware vSphere 10.5 after the datastore discovery job, which may take up to 30 minutes. Check their visibility on the overview page.
14. Perform the patch migration using the following API in Swagger or in Postman:

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
PATCH	/api/v1

Processing type

Asynchronous

Use the following URI in Swagger:

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Curl example

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/d50073ce-35b4-4c51-9d2e-4ce66f802c35`
```

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"
}
```

The request body is empty for patch operation.

UUID is the migration UUID returned in response to the post-migrate API.

After running the patch migration API, all VMs comply with the storage policy.

What's next

After completing the migration and registering ONTAP tools 10.5 to the vCenter Server, follow these steps:

- Wait for **Discovery** to complete, and the system refreshes the certificates automatically on all the hosts.

- Wait before starting datastore and virtual machine operations. The waiting time depends on the number of hosts, datastores, and virtual machines. If you do not wait, you might see occasional failures.

After upgrading, if the virtual machine's compliance state is outdated, reapply the storage policy using the following steps:

1. Go to the datastore and select **Summary** > **VM Storage policies**.

   The system shows the compliance status under **VM storage policy compliance** as **Out-of-date**.

2. Select the Storage VM policy and the corresponding VM.
3. Select **Apply**.

   The compliance status under **VM storage policy compliance** shows as compliant.

Related information

- Learn about ONTAP tools for VMware vSphere 10 RBAC
- Upgrade from ONTAP tools for VMware vSphere 10.x to 10.5

Steps to update the storage replication adaptor(SRA)

Before you begin

In the recovery plan, the protected site refers to the location where the VMs are currently running, while the recovery site is where the VMs will be recovered. The VMware Live Site Recovery appliance interface displays the state of the recovery plan with details about the protected and the recovery sites. In the recovery plan, the CLEANUP and REPROTECT buttons are disabled, whereas the TEST and RUN buttons remain enabled. This indicates that the site is prepared for data recovery. Before migrating the SRA, verify that one site is in the protected state and the other is in the recovery state.

Don't begin migration if the failover has been completed but the re-protection is pending. Ensure that the re-protection process is completed before proceeding with the migration. If a test failover is in progress, clean up the test failover and start the migration.

1. Follow these steps to delete the ONTAP tools SRA adapter for VMware vSphere 9.xx in VMware Site Recovery:
   a. Go to VMware Live Site Recovery configuration management page
   b. Go to the **Storage Replication Adapter** section.
   c. From the ellipsis menu select **Reset configuration**.
   d. From the ellipsis menu select **Delete**.
2. Perform these steps on both protection and recovery sites.
   a. Enable ONTAP tools for VMware vSphere services
   b. Configure ONTAP tools for VMware vSphere 10.5 SRA adapter using the steps in Configure SRA on the VMware Live Site Recovery appliance.
   c. On the VMware Live Site Recovery interface, run **Discover Arrays** and **Discover Devices**. Confirm devices display as before migration.

Automate using the REST API

Learn about the ONTAP tools REST API

ONTAP tools for VMware vSphere 10 is a set of tools for virtual machine lifecycle management. It includes a robust REST API you can use as part of your automation processes.

REST web services foundation

Representational State Transfer (REST) is a style for creating distributed web applications including the design of web services APIs. It establishes a set of technologies for exposing server-based resources and managing their states.

Resources and state representation

Resources are the foundational components of a REST web services application. There are two important initial tasks when designing a REST API:

- Identify the system or server-based resources
- Define the resource states and associated state transition operations

Client applications can display and change the resource states through well-defined message flows.

HTTP messages

Hypertext Transfer Protocol (HTTP) is the protocol used by the web services client and server to exchange messages about the resources. It follows the CRUD model based on the generic operations create, read, update, and delete. The HTTP protocol includes request and response headers as well as response status codes.

JSON data formatting

While there are several message formats available, the most popular option is JavaScript Object Notation (JSON). JSON is an industry standard for representing simple data structures in plain text and is used to transfer state information describing the resources and desired actions.

Security

Security is an important aspect of a REST API. In addition to the Transport Layer Security (TLS) protocol used to protect the HTTP traffic over the network, the ONTAP tools for VMware vSphere 10 REST API also uses access tokens for authentication. You need to acquire an access token and use it on subsequent API calls.

Support for asynchronous requests

The ONTAP tools for VMware vSphere 10 REST API performs most requests synchronously, returning a status code when the operation is complete. It also supports asynchronous processing for tasks that require a longer time to complete.

ONTAP tools Manager environment

There are several aspects of the ONTAP tools Manager environment you should consider.

Virtual machine

ONTAP tools for VMware vSphere 10 is deployed using the vSphere remote plug-in architecture. The software,

including support for the REST API, runs in a separate virtual machine.

ONTAP tools IP address

ONTAP tools for VMware vSphere 10 exposes a single IP address which provides a gateway to the capabilities of the virtual machine. You need to provide the address during initial configuration and it's assigned to an internal load balancer component. The address is used by the ONTAP tools Manager user interface as well as to access the Swagger documentation page and REST API directly.

Two REST APIs

In addition to the ONTAP tools for VMware vSphere 10 REST API, the ONTAP cluster has its own REST API. ONTAP tools Manager uses the ONTAP REST API as a client to perform storage related tasks. It's important to keep in mind these two APIs are separate and distinct. For more information, refer to ONTAP automation.

ONTAP tools REST API implementation details

While REST establishes a common set of technologies and best practices, the exact implementation of each API can vary based on the design choices. You should be familiar with how the ONTAP tools for VMware vSphere 10 REST API is designed before using it.

The REST API includes several resource categories such as vCenters and Aggregates. Review the API reference for more information.

How to access the REST API

You can access the ONTAP tools for VMware vSphere 10 REST API through the ONTAP tools IP address along with the port. There are several parts to the complete URL, including:

- ONTAP tools IP address and port
- API version
- Resource category
- Specific resource

You must configure the IP address during initial setup, while the port remains fixed at 8443. The first part of the URL is consistent for each ONTAP tools for VMware vSphere 10 instance; only the resource category and specific resource change between endpoints.

The IP address and port values in the examples below are for illustration purposes only. You need to change these values for your environment.

Example to access authentication services

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

This URL can be used to request an access token using the POST method.

Example to list the vCenter servers

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

This URL can be used to request a list of the defined vCenter server instances using the GET method.

HTTP details

The ONTAP tools for VMware vSphere 10 REST API uses HTTP and related parameters to act on the resource instances and collections. Details of the HTTP implementation are presented below.

HTTP methods

The HTTP methods or verbs supported by the REST API are presented in the table below.

Method	CRUD	Description
GET	Read	Retrieves object properties for a resource instance or collection. This is considered a list operation when used with a collection.
POST	Create	Creates a new resource instance based on the input parameters.
PUT	Update	Updates an entire resource instance with the supplied JSON request body. Key values that aren’t user-modifiable are preserved.
PATCH	Update	Requests a set of selected changes in the request be applied to the resource instance.
DELETE	Delete	Deletes an existing resource instance.

Request and response headers

The following table summarizes the most important HTTP headers used with the REST API.

Header	Type	Usage notes
Accept	Request	This is the type of content the client application can accept. Valid values include '*/*` or `application/json`.
x-auth	Request	Contains an access token identifying the user issuing the request through the client application.
Content-Type	Response	Returned by the server based on the `Accept` request header.

HTTP status codes

The HTTP status codes used by the REST API are described below.

Code	Meaning	Description
200	OK	Indicates success for calls that don’t create a new resource instance.
201	Created	An object has been successfully created with a unique identifier for the resource instance.
202	Accepted	The request has been accepted and a background job created to perform the request.
204	No content	The request was successful although no content was returned.
400	Bad request	The request input is not recognized or is inappropriate.
401	Unauthorized	The user is not authorized and must authenticate.

Code	Meaning	Description
403	Forbidden	Access is denied due to an authorization error.
404	Not found	The resource referred to in the request doesn't exist.
409	Conflict	An attempt to create an object failed because the object already exists.
500	Internal error	A general internal error occurred at the server.

Authentication

Authentication of a client to the REST API is performed using an access token. The relevant characteristics of the token and authentication process include:

- The client must request a token using ONTAP tools Manager admin credentials (username and password).
- Tokens are formatted as a JSON Web Token (JWT).
- Each token expires after 60 minutes.
- API requests from a client must include the token in the `x-auth` request header.

Refer to Your first REST API call for an example of requesting and using an access token.

Synchronous and asynchronous requests

Most REST API calls complete quickly and therefore run synchronously. That is, they return a status code (such as 200) after a request has been completed. Requests that take longer to complete run asynchronously using a background job.

After issuing an API call that runs asynchronously, the server returns a 202 HTTP status code. This indicates the request has been accepted but not yet completed. You can query the background job to determine its status including success or failure.

Asynchronous processing is used for several types of long running operations, including datastore and vVol operations. Refer to the job manager category of the REST API at the Swagger page for more information.

Make your first ONTAP tools REST API call

You can issue an API call using curl to get started with the ONTAP tools for VMware vSphere 10 REST API.

Before you begin

You should review the required information and parameters needed in the curl examples.

Required information

You need the following:

- ONTAP tools for VMware vSphere 10 IP address or FQDN as well as the port
- Credentials for the ONTAP tools Manager admin (username and password)

Parameters and variables

The curl examples presented below include Bash style variables. You can set these variables in the Bash

environment or manually update them before issuing the commands. If you set the variables, the shell will substitute the values into each command before it's executed. The variables are described in the table below.

Variable	Description
$FQDN_IP_PORT	The fully qualified domain name or IP address of the ONTAP tools Manager along with the port number.
$MYUSER	Username for the ONTAP tools Manager account.
$MYPASSWORD	Password associated with the ONTAP tools Manager username.
$ACCESS_TOKEN	The access token issued by the ONTAP tools Manager.

The following commands and output at the Linux CLI illustrate how a variable can be set and displayed:

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

Step 1: Acquire an access token

You need to acquire an access token to use the REST API. An example of how to request an access token is presented below. You should substitute in the appropriate values for your environment.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

Copy and save the the access token provided in the response.

Step 2: Issue the REST API call

After you have an access token, you can use curl to issue a REST API call. Include the access token acquired in the first step.

Curl example

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

The JSON response includes a list of the VMware vCenter instances configured to the ONTAP tools Manager.

ONTAP tools REST API reference

The ONTAP tools for VMware vSphere 10 REST API reference contains details about all the API calls. This reference is helpful when developing automation applications.

You can access the ONTAP tools for VMware vSphere 10 REST API documentation online through the Swagger user interface. You need the IP address or FQDN of the ONTAP tools for VMware vSphere 10 gateway service as well as the port.

Steps

1. Type the following URL into your browser substituting the appropriate IP address and port combination for the variable and press **Enter**.

   `https://$FQDN_IP_PORT/`

   Example

   `https://10.61.25.33:8443/`

2. As an example of an individual API call, scroll down to the **vCenters** category and select **GET** next to the endpoint `/virtualization/api/v1/vcenters`

Legal notices

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 10.5