NetApp

ONTAP tools for VMware vSphere Documentation

ONTAP tools for VMware vSphere 9.11

NetApp
February 12, 2024

Table of Contents

ONTAP tools for VMware vSphere Documentation

Release notes

Provides important information about this release of ONTAP tools for VMware vSphere, including fixed issues, known issues, cautions, and limitations.

For more information, see the ONTAP tools for VMware vSphere 9.11 Release Notes.

Concepts

ONTAP tools Overview

The ONTAP tools for VMware vSphere provides end-to-end life cycle management for virtual machines in VMware environments that use NetApp storage systems. It simplifies storage and data management for VMware environments by enabling administrators to directly manage storage within the vCenter Server.

With vSphere 6.5, VMware introduced a new HTML5-based client called vSphere Client. The 9.6 and later releases of ONTAP tools support only vSphere Client. The ONTAP tools integrates with vSphere Client and enables you to use single sign-on (SSO) services. In an environment with multiple vCenter Server instances, each vCenter Server instance that you want to manage must have its own registered instance of VSC.

Each component in ONTAP tools provides capabilities to help manage your storage more efficiently.

Virtual Storage Console (VSC)

VSC enables you to perform the following tasks:

- Add storage controllers, assign credentials, and set up permissions for storage controllers of VSC, that both SRA and VASA Provider can leverage

- Provision datastores

- Monitor the performance of the datastores and virtual machines in your vCenter Server environment

- Control administrator access to the vCenter Server objects by using role-based access control (RBAC) at two levels:

  - vSphere objects, such as virtual machines and datastores

    These objects are managed by using the vCenter Server RBAC.

  - ONTAP storage

    The storage systems are managed by using ONTAP RBAC.

- View and update the host settings of the ESXi hosts that are connected to NetApp storage

VSC provisioning operations benefit from using the NFS Plug-in for VMware vStorage APIs for Array Integration (VAAI). The NFS Plug-in for VAAI is a software library that integrates the VMware Virtual Disk Libraries that are installed on the ESXi host. The VMware VAAI package enables the offloading of certain tasks from the physical hosts to the storage array. You can perform tasks such as thin provisioning and hardware acceleration at the array level to reduce the workload on the ESXi hosts. The copy offload feature and space reservation feature improve the performance of VSC operations.

The NetApp NFS Plug-in for VAAI is not shipped with VSC. But you can download the plug-in installation package and obtain the instructions for installing the plug-in from the NetApp Support Site.

VASA Provider

VASA Provider for ONTAP uses VMware vSphere APIs for Storage Awareness (VASA) to send information about storage used by VMware vSphere to the vCenter Server. ONTAP tools has VASA Provider integrated

with VSC. VASA Provider enables you to perform the following tasks:

- Provision VMware Virtual Volumes (vVols) datastores
- Create and use storage capability profiles that define different storage service level objectives (SLOs) for your environment
- Verify for compliance between the datastores and the storage capability profiles
- Set alarms to warn you when volumes and aggregates are approaching the threshold limits
- Monitor the performance of virtual machine disks (VMDKs) and the virtual machines that are created on vVols datastores

If you are using ONTAP 9.6 or earlier, then VASA Provider communicates with the vCenter Server by using VASA APIs and communicates with ONTAP by using NetApp APIs called ZAPIs. To view the vVols dashboard for ONTAP 9.6 and earlier, you must have installed and registered OnCommand API Services with your vCenter Server. If you are using ONTAP 9.7 and later versions, then you do not require OnCommand API Services to be registered with VASA Provider to view the vVols dashboard.

> ⓘ For ONTAP 9.6 and earlier, VASA Provider requires a dedicated instance of OnCommand API Services. One instance of OnCommand API Services cannot be shared with multiple VASA Provider instances.

Storage Replication Adapter (SRA)

When SRA is enabled and used in conjunction with VMware Site Recovery Manager (SRM), you can recover the vCenter Server datastores and virtual machines in the event of a failure. SRA enables you to use array based replication (ABR) for protected sites and recovery sites for disaster recovery in the event of a failure.

Related information

NetApp Support

VASA Provider configurations for vVols

You can use VASA Provider for ONTAP to create and manage VMware Virtual Volumes (vVols). You can provision, edit, mount, and delete a vVols datastore. You can also add storage to the vVols datastore or remove storage from the vVols datastore. to provide greater flexibility. You can provision and manage every virtual machine and the related VMDK.

A vVols datastore consists of one or more FlexVol volumes within a storage container (also called "backing storage"). A virtual machine can be spread across one vVols datastore or multiple vVols datastores.

While you can create a vVols datastore that has multiple FlexVol volumes, all of the FlexVol volumes within the storage container must use the same protocol (NFS, iSCSI, or FCP) and the same storage virtual machines (SVMs).

You do not require detailed knowledge of the underlying storage. For example, you do not have to identify a specific FlexVol volume to contain the storage. After you add FlexVol volumes to the vVols datastore, the storage container manages the storage requirements and prevents any situations during VM provisioning where VMware provisioned to a backing volume with no capacity.

> ⓘ It is a good practice to include multiple FlexVol volumes in a vVols datastore for performance and flexibility. Because FlexVol volumes have LUN count restrictions that limit the number of virtual machines, including multiple FlexVol volumes allows you to store more virtual machines in your vVols datastore.

As part of the setup process, you must specify a storage capability profile for the vVols datastore that you are creating. You can select one or more VASA Provider storage capability profiles for a vVols datastore. You can also specify a default storage capability profile for any vVols datastores that are automatically created in that storage container.

VASA Provider creates different types of vVols during virtual machine provisioning or VMDK creation, as required.

- **Config**

  VMware vSphere uses this vVols datastore to store configuration information.

  In SAN (block) implementations, the storage is a 4 GB LUN.

  In an NFS implementation, this is a directory containing VM config files such as the vmx file and pointers to other vVols datastores.

- **Data**

  This vVols contains operating system information and user files.

  In SAN implementations, this is a LUN that is the size of the virtual disk.

  In an NFS implementation, this is a file that is the size of the virtual disk.

  For every NFS data vVols that is provisioned on ONTAP clusters 9.8 and above, all the VMDK files are registered for monitoring performance metrics like IOPS, Throughput, and Latency.

- **Swap**

  This vVols is created when the virtual machine is powered on and is deleted when the virtual machine is powered off.

  In SAN implementations, this is a LUN that is the size of the virtual memory.

  In an NFS implementation, this is a file that is the size of the virtual memory.

- **Memory**

  This vVols is created if the memory snapshots option is selected when creating VM snapshot.

  In SAN implementations, this is a LUN that is the size of the virtual memory.

  In an NFS implementation, this is a file that is the size of the virtual memory.

Configure disaster recovery setup

You can create and manage the disaster recovery setup in your vCenter Server along with VMware's Site Recovery Manager (SRM).

VASA Provider now comes built-in with the capabilities of Storage Replication Adapter (SRA). If you have configured vVols datastores in your datacenter, then for recovery of vVols datastores, you do not need to install SRA separately for disaster recovery. In Site Recovery Manager (SRM), you must pair the protected and recovery sites. After the site pairing has occurred, the next part of the SRM configuration involves setting up an array pair which enables SRM to communicate with storage system to discover devices and device replication. Before you can configure the array pair, you must first create a site pair in SRM.

This release of ONTAP tools provides you with an option to use synchronous SnapMirror configuration for disaster recovery.

> ⓘ VMware Site Recovery Manager (SRM) does not use SRA for managing disaster recovery of vVols datastores. Instead VASA Provider is used for replication and failover control of vVols datastores on ONTAP 9.7 and later clusters.

Enable Storage Replication Adapter

Role based access control

Overview of role-based access control in ONTAP tools

vCenter Server provides role-based access control (RBAC) that enables you to control access to vSphere objects. In ONTAP® tools for VMware vSphere, vCenter Server RBAC works with ONTAP RBAC to determine which VSC tasks a specific user can perform on objects on a specific storage system.

To successfully complete a task, you must have the appropriate vCenter Server RBAC permissions. During a task, VSC checks a user's vCenter Server permissions before checking the user's ONTAP privileges.

You can set the vCenter Server permissions on the root object (also known as the root folder). You can then refine the security by restricting child entities that do not need those permissions.

Components of vCenter Server permissions

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

The vCenter Server has the following components:

* One or more privileges (the role)

  The privileges define the tasks that a user can perform.

* A vSphere object

  The object is the target for the tasks.

* A user or group

  The user or group defines who can perform the task.

As the following diagram illustrates, you must have all three elements in order to have a permission.

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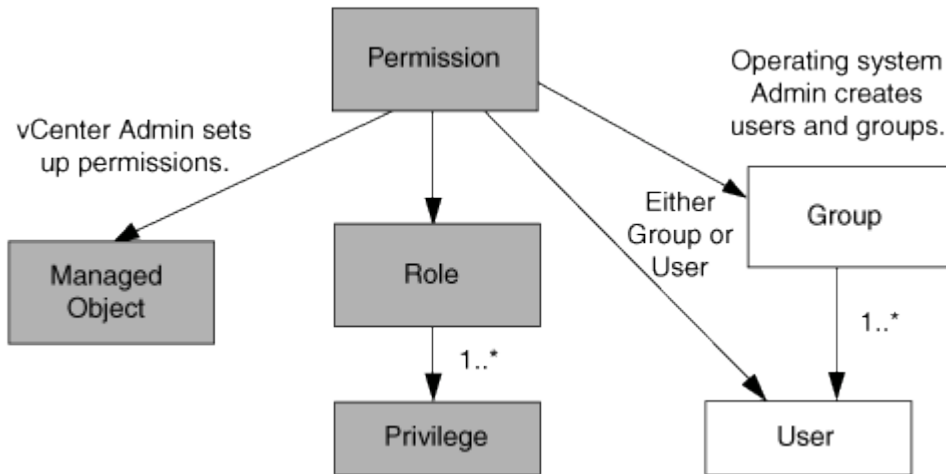
Privileges

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

- Native vCenter Server privileges

  These privileges come with the vCenter Server.

- VSC-specific privileges

  These privileges are defined for specific VSC tasks. They are unique to VSC.

VSC tasks require both VSC-specific privileges and vCenter Server native privileges. These privileges constitute the "role" for the user. A permission can have multiple privileges. These privileges are for a user that is logged into the vCenter Server.

> ⓘ To simplify working with vCenter Server RBAC, VSC provides several standard roles that contain all the VSC-specific and native privileges that are required to perform VSC tasks.

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

Privilege	Roles	Tasks
NetApp ONTAP tools Console > View	• VSC Administrator • VSC Provision • VSC Read-Only	All the VSC and VASA Provider specific tasks require the View Privilege.

NetApp Virtual Storage Console > Policy Based Management > Management or privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > Management	VSC Administrator	VSC and VASA Provider tasks related to storage capability profiles and threshold settings.

vSphere objects

Permissions are associated with vSphere objects, such as the vCenter Server, ESXi hosts, virtual machines, datastores, datacenters, and folders. You can assign permissions to any vSphere object. Based on the permission that is assigned to a vSphere object, the vCenter Server determines who can perform which tasks on that object. For VSC specific tasks, permissions are assigned and validated only at the root-folder level (vCenter Server) and not on any other entity. Except for VAAI plugin operation, where permissions are validated against the concerned ESXi .

Users and groups

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

> (i) These vCenter Server permissions apply to VSC vCenter users, not to VSC administrators. By default, VSC administrators have full access to the product and do not require permissions assigned to them.

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

Key points about assigning and modifying permissions for vCenter Server

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

Assigning permissions

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

Where you assign a permission determines the VSC tasks that a user can perform.

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

In these cases, you can set up a permission so that it is inherited by the child entities. You can also assign other permissions to the child entities. The permission assigned to a child entity always overrides the permission inherited from the parent entity. This means that you can permissions to a child entity as a way to

restrict the scope of a permission that was assigned to a root object and inherited by the child entity.

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

Permissions and non-vSphere objects

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

For example, any permission that includes a privilege such as the VSC privilege "Add/Modify/Skip storage systems" must be assigned at the root object level.

Modifying permissions

You can modify one permission at any time.

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

Standard roles packaged with ONTAP tools

To simplify working with vCenter Server privileges and role-based access control (RBAC), Virtual Storage Console (VSC) provides standard VSC roles that enable you to perform key VSC tasks. There is also a read-only role that enables you to view VSC information, but not perform any tasks.

The standard VSC roles have both the required VSC-specific privileges and the native vCenter Server privileges that are required for users to perform VSC tasks. In addition, the roles are set up so that they have the required privileges across all supported versions of the vCenter Server.

As an administrator, you can assign these roles to users as required.

> ⓘ When you upgrade VSC to the latest version, the standard roles are automatically upgraded to work with the new version of VSC.

You can view the VSC standard roles by clicking **Roles** on the vSphere Client Home page.

The roles that VSC provides enable you to perform the following tasks:

Role	Description
VSC Administrator	Provides all of the native vCenter Server privileges and VSC-specific privileges that are required to perform all VSC tasks.
VSC Read-only	Provides read-only access to VSC. These users cannot perform any VSC actions that are access-controlled.

VSC Provision	Provides all of the native vCenter Server privileges and VSC-specific privileges that are required to provision storage. You can perform the following tasks: • Create new datastores • Destroy datastores • View information about storage capability profiles

Guidelines for using VSC standard roles

When you work with standard ONTAP tools for VMware vSphere roles, there are certain guidelines you should follow.

You should not directly modify the standard roles. If you do, VSC will overwrite your changes each time you upgrade VSC. The installer updates the standard role definitions each time you upgrade VSC. Doing this ensures that the roles are current for your version of VSC as well as for all supported versions of the vCenter Server.

You can, however, use the standard roles to create roles that are tailored to your environment. To do this, you should copy the VSC standard role and then edit the copied role. By creating a new role, you can maintain this role even when you restart or upgrade the VSC Windows service.

Some of the ways that you might use the VSC standard roles include the following:

• Use the standard VSC roles for all VSC tasks.

   In this scenario, the standard roles provide all the privileges a user needs to perform the VSC tasks.

• Combine roles to expand the tasks a user can perform.

   If the standard VSC roles provide too much granularity for your environment, you can expand the roles by creating higher-level groups that contain multiple roles.

   If a user needs to perform other, non-VSC tasks that require additional native vCenter Server privileges, you can create a role that provides those privileges and add it to the group also.

• Create more fine-grained roles.

   If your company requires that you implement roles that are more restrictive than the standard VSC roles, you can use the VSC roles to create new roles.

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

Privileges required for VSC tasks

Different ONTAP tools for VMware vSphere tasks require different combinations of privileges specific to Virtual Storage Console (VSC) and native vCenter Server privileges.

Information about the privileges required for VSC tasks is available in the NetApp Knowledgebase article 1032542.

Product-level privilege required by ONTAP tools for VMware vSphere

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

The following information describes the VSC product-level View privilege:

Privilege	Description	Assignment level
View	You can access the VSC GUI. This privilege does not enable you to perform tasks within VSC. To perform any VSC tasks, you must have the correct VSC-specific and native vCenter Server privileges for those tasks.	The assignment level determines which portions of the UI you can see. Assigning the View privilege at the root object (folder) enables you to enter VSC by clicking the NetApp icon. You can assign the View privilege to another vSphere object level; however, doing that limits the VSC menus that you can see and use. The root object is the recommended place to assign any permission containing the View privilege.

Permissions for ONTAP storage systems and vSphere objects

ONTAP role-based access control (RBAC) enables you to control access to specific storage systems and to control the actions that a user can perform on those storage systems. In ONTAP® tools for VMware vSphere, ONTAP RBAC works with vCenter Server RBAC to determine which Virtual Storage Console (VSC) tasks a specific user can perform on the objects on a specific storage system.

VSC uses the credentials (user name and password) that you set up within VSC to authenticate each storage system and to determine which storage operations can be performed on that storage system. VSC uses one set of credentials for each storage system. These credentials determine which VSC tasks can be performed on that storage system; in other words, the credentials are for VSC, not for an individual VSC user.

ONTAP RBAC applies only to accessing storage systems and performing VSC tasks that are related to storage, such as provisioning virtual machines. If you do not have the appropriate ONTAP RBAC privileges for a specific storage system, you cannot perform any tasks on a vSphere object that is hosted on that storage system. You can use ONTAP RBAC in conjunction with the VSC-specific privileges to control which VSC tasks a user can perform:

- Monitoring and configuring storage or vCenter Server objects residing on a storage system
- Provisioning vSphere objects residing on a storage system

Using ONTAP RBAC with the VSC-specific privileges provides a storage-oriented layer of security that the

storage administrator can manage. As a result, you have more fine-grained access control than what either ONTAP RBAC alone or vCenter Server RBAC alone supports. For example, with vCenter Server RBAC, you can allow vCenterUserB to provision a datastore on NetApp storage while preventing vCenterUserA from provisioning datastores. If the storage system credentials for a specific storage system do not support the creation of storage, then neither vCenterUserB nor vCenterUserA can provision a datastore on that storage system.

When you initiate a VSC task, VSC first verifies whether you have the correct vCenter Server permission for that task. If the vCenter Server permission is not sufficient to allow you to perform the task, VSC does not have to check the ONTAP privileges for that storage system because you did not pass the initial vCenter Server security check. As a result, you cannot access the storage system.

If the vCenter Server permission is sufficient, VSC then checks the ONTAP RBAC privileges (your ONTAP role) that are associated with the storage system credentials (the user name and password) to determine whether you have sufficient privileges to perform the storage operations that are required by that VSC task on that storage system. If you have the correct ONTAP privileges, you can access the storage system and perform the VSC task. The ONTAP roles determine the VSC tasks that you can perform on the storage system.

Each storage system has one set of ONTAP privileges associated with it.

Using both ONTAP RBAC and vCenter Server RBAC provides the following benefits:

- Security

  The administrator can control which users can perform which tasks at a fine-grained vCenter Server object level and at a storage system level.

- Audit information

  In many cases, VSC provides an audit trail on the storage system that enables you to track events back to the vCenter Server user who performed the storage modifications.

- Usability

  You can maintain all of the controller credentials in one place.

Recommended ONTAP roles when using ONTAP tools for VMware vSphere

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

To create new user roles, you must log in as an administrator on storage systems running ONTAP. You can create ONTAP roles using one of the following:

- ONTAP System Manager 9.8P1 or later

  Configure user roles and privileges

- RBAC User Creator for ONTAP tool (if using ONTAP 9.6 or earlier)

  RBAC User Creator tool for VSC, VASA Provider and Storage Replication Adapter 7.0 for VMware vSphere

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

with the role.

As a security measure, the VSC-specific ONTAP roles are ordered hierarchically. This means that the first role is the most restrictive role and has only the privileges that are associated with the most basic set of VSC storage operations. The next role includes both its own privileges and all of the privileges that are associated with the previous role. Each additional role is less restrictive with regard to the supported storage operations.

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

1. Discovery

   This role enables you to add storage systems.

2. Create Storage

   This role enables you to create storage. This role also includes all of the privileges that are associated with the Discovery role.

3. Modify Storage

   This role enables you to modify storage. This role also includes all of the privileges that are associated with the Discovery role and the Create Storage role.

4. Destroy Storage

   This role enables you to destroy storage. This role also includes all of the privileges that are associated with the Discovery role, the Create Storage role, and the Modify Storage role.

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

How to configure ONTAP role-based access control for ONTAP tools for VMware vSphere

You must configure ONTAP role-based access control (RBAC) on the storage system if you want to use role-based access control with ONTAP tools for VMware vSphere. You can create one or more custom user accounts with limited access privileges with the ONTAP RBAC feature.

VSC and SRA can access storage systems at either the cluster level or the storage virtual machine (SVM)SVM level. If you are adding storage systems at the cluster level, then you must provide the credentials of the admin user to provide all of the required capabilities. If you are adding storage systems by directly adding SVM details, you must be aware that the "vsadmin" user does not have all of the required roles and capabilities to perform certain tasks.

VASA Provider can access storage systems only at the cluster level. If VASA Provider is required for a particular storage controller, then the storage system must be added to VSC at the cluster level even if you are using VSC or SRA.

To create a new user and to connect a cluster or an SVM to ONTAP tools, you should perform the following:

- Create a cluster administrator or an SVM administrator role

    ℹ️ You can use one of the following to create these roles:

    ◦ ONTAP System Manager 9.8P1 or later

    [Configure user roles and privileges]

    ◦ RBAC User Creator for ONTAP tool (if using ONTAP 9.6 or earlier)

    [RBAC User Creator tool for VSC, VASA Provider and Storage Replication Adapter 7.0 for VMware vSphere]

- Create users with the role assigned and the appropriate application set using ONTAP

    You require these storage system credentials to configure the storage systems for VSC. You can configure storage systems for VSC by entering the credentials in VSC. Each time you log in to a storage system with these credentials, you will have permissions to the VSC functions that you had set up in ONTAP while creating the credentials.

- Add the storage system to VSC and provide the credentials of the user that you just created

VSC roles

VSC classifies the ONTAP privileges into the following set of VSC roles:

- Discovery

    Enables the discovery of all of the connected storage controllers

- Create Storage

    Enables the creation of volumes and logical unit number (LUNs)

- Modify Storage

    Enables the resizing and deduplication of storage systems

- Destroy Storage

    Enables the destruction of volumes and LUNs

VASA Provider roles

You can create only Policy Based Management at the cluster level. This role enables policy-based management of storage using storage capabilities profiles.

SRA roles

SRA classifies the ONTAP privileges into a SAN or NAS role at either the cluster level or the SVM level. This enables users to run SRM operations.

VSC performs an initial privilege validation of ONTAP RBAC roles when you add the cluster to VSC. If you have added a direct SVM storage IP, then VSC does not perform the initial validation. VSC checks and

enforces the privileges later in the task workflow.

Configure high availability for ONTAP tools

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

The ONTAP tools relies on the VMware vSphere High-availability (HA) feature and vSphere fault tolerance (FT) feature to provide high availability. High-availability (HA) solution provides for rapid recovery from outages caused by:

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

No additional configuration is required for ONTAP tools to provide high availability. Only the vCenter Server and ESXi hosts must be configured with the VMware vSphere HA feature or the vSphere FT feature based on their requirements. Both HA and FT require clustered hosts together with shared storage. FT has additional requirements and limitations.

In addition to the VMware vSphere HA solution and vSphere FT solution, ONTAP tools also helps keep the ONTAP tools services running at all times. The ONTAP tools watchdog process periodically monitors all three services, and restarts them automatically when any kind of failure is detected. This helps to prevent application failures.

> ⓘ vCenter HA is not supported by ONTAP tools.

VMware vSphere HA

You can configure your vSphere environment where ONTAP tools for VMware vSphere is deployed for high availability (HA). The VMware HA feature provides failover protection from hardware failures and operating system failures in virtual environments.

The VMware HA feature monitors virtual machines to detect operating system failures and hardware failures. When a failure is detected, the VMware HA feature restarts the virtual machines on the other physical servers in the resource pool. Manual intervention is not required when a server failure is detected.

The procedure to configure VMware HA depend on the version of your vCenter Server. For example, you can use the following reference link and select the required vCenter Server version to view the steps to configure VMware HA.

VMware vSphere Documentation: Creating and Using vSphere HA Clusters

VMware vSphere Fault Tolerance

The VMware vSphere Fault Tolerance (FT) feature provides high availability (HA) at a higher level and enables you to protect virtual machines without any loss of data or connections. You must enable or disable vSphere FT for ONTAP tools from your vCenter Server.

Ensure your vSphere license supports FT with the number of vCPUs needed for ONTAP tools in your environment (at least 2 vCPUs; 4 vCPUs for large scale environments).

vSphere FT enables virtual machines to operate continuously even during server failures. When vSphere FT is enabled on a virtual machine, a copy of the primary virtual machine is automatically created on another host (the secondary virtual machine) that is selected by Distributed Resource Scheduler (DRS). If DRS is not enabled, the target host is selected from the available hosts. vSphere FT operates the primary virtual machine and secondary virtual machine in lockstep mode, with each mirroring the execution state of the primary virtual machine to the secondary virtual machine.

When there is a hardware failure that causes the primary virtual machine to fail, the secondary virtual machine immediately picks up where the primary virtual machine stopped. The secondary virtual machine continues to run without any loss of network connections, transactions, or data.

Your system must meet the CPU requirements, virtual machine limit requirements, and licensing requirements for configuring vSphere FT for your vCenter Server instance.

The procedure to configure HA depend on the version of your vCenter Server. For example, you can use the following reference link and select the required vCenter Server version to view the steps to configure HA.

VMware vSphere Documentation: Fault Tolerance Requirements, Limits, and Licensing

MetroCluster configurations supported by ONTAP tools

The ONTAP tools for VMware vSphere supports environments that use MetroCluster IP and FC configurations for ONTAP. Most of this support is automatic. However, you might notice a few differences when you use a MetroCluster environment with VSC and VASA Provider.

> ⓘ SRA does not support MetroCluster configurations.

MetroCluster configurations and VSC

You must ensure that VSC discovers the storage system controllers at the primary site and the secondary site. Typically, VSC automatically discovers storage controllers. If you are using a cluster management LIF, then it is a good practice to verify that VSC has discovered the clusters at both sites. Otherwise, you can manually add the storage controllers to VSC. You can also modify the user name and password pairs that VSC uses to connect to the storage controllers.

When a switchover occurs, the SVMs on the secondary site take over. These SVMs have the "-mc" suffix appended to their names. If a switchover operation occurs while you are performing operations such as provisioning a datastore, the name of the SVM where the datastore resides is changed to include the "-mc" suffix. This suffix is dropped when the switchback occurs, and the SVMs on the primary site resume control.

> ⓘ If you have added direct SVMs with MetroCluster configuration to VSC, then after switchover, the change in the SVM name (the addition of the "-mc" suffix) is not reflected. All other switchover operations continue to execute normally.

When a switchover or switchback occurs, VSC might take a few minutes to automatically detect and discover the clusters. If this happens while you are performing a VSC operation such as provisioning a datastore, you might experience a delay.

MetroCluster configurations and VASA Provider

VASA Provider automatically supports environments that use MetroCluster configurations. The switchover is transparent in VASA Provider environments. You cannot add direct SVMs to VASA Provider.

> ⓘ VASA Provider does not append the "-mc" suffix to the names of the SVMs on the secondary site after a switchover.

Deploy and upgrade ONTAP tools

Deployment workflow for new users of ONTAP tools for VMware vSphere

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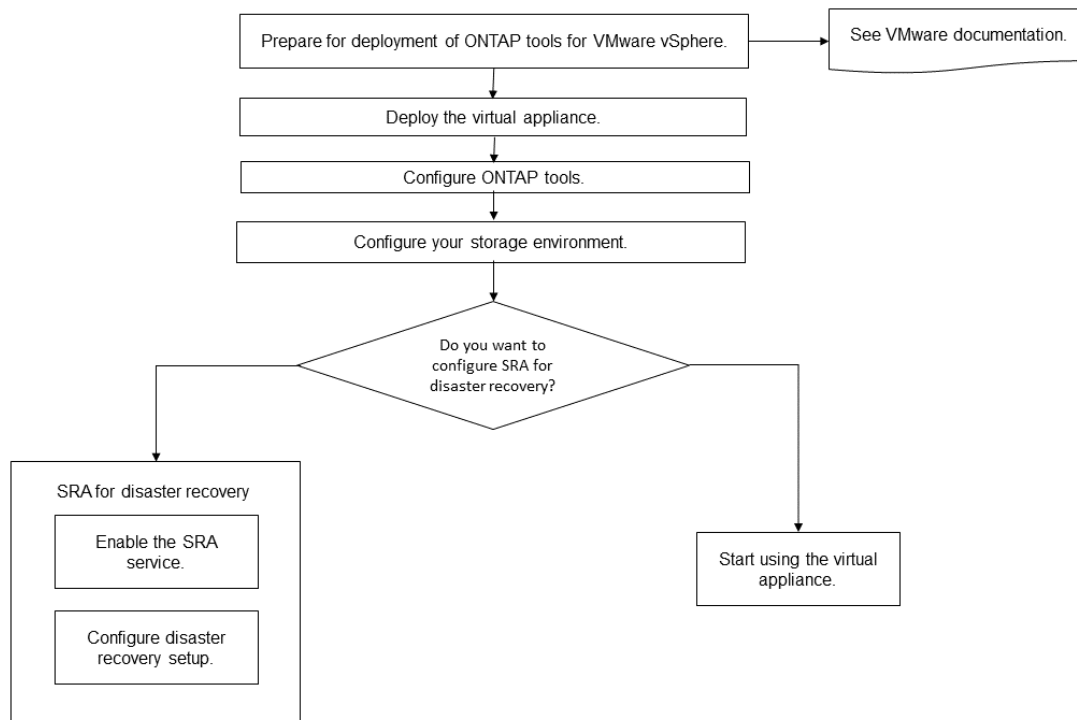
Deployment workflow for existing users of ONTAP tools

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

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

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

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

Set IPv4 or IPv6 using the preferences file

In many cases, you might not need to migrate configuration data. However, if you have customized the

preferences files earlier, you might want to review them and make similar changes to the newly deployed ONTAP tools. You can add the storage systems to the newly deployed ONTAP tools and specify the credentials as you add them.

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

If you are upgrading from SRA 4.0 or earlier:

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

  Upgrade to the latest release of ONTAP tools

* If you are using SRA 2.1 or 3.0, you should first make note of existing site configuration details.

  Installation and Setup Guide for Storage Replication Adapter 4.0 for ONTAP has the detailed instructions in the "Upgrade Overview" section. These SRA releases also use the VASA Provider, so you must unregister VASA Provider and then deploy the latest version of ONTAP tools. The previous release of the server (`.ova`) can be removed when the upgrade is complete.

For any SRA upgrade, the SRA software (the adapter on the Site Recovery Manager server, installed by the `.msi` file) should be removed from the Site Recovery Manager server. You can use the Windows system control panel to uninstall the software and then install the latest SRA software on the SRA server using the `.msi` file.

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

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

To upgrade from ONTAP tools 9.10 and later releases, run the virtual appliance 9.7P1 or later. Upgrading from an earlier version prior to 9.7P1 of the virtual appliance is not supported.

If you are going to deploy the latest release of ONTAP tools, you must see the topic `Requirements for deploying the ONTAP tools`. The topic `Upgrading to the latest release of ONTAP tools` has information on performing an in-place upgrade.

Related information

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

VMware Cloud Foundation mode of deployment for ONTAP tools

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

The VCF mode enables you to create containers for your storage without the need for a vCenter Server. VASA

Provider is enabled by default after the deployment of ONTAP tools in VCF mode. After the deployment is complete, you can add storage systems and create containers using REST APIs. A new API is introduced to generate the *appliance-api-token* that authenticates API calls. Some of the existing APIs are modified to include the *appliance-api-token* header.

The APIs available for VCF deployment mode are:

API	HTTP method	New/modified	Section header
/1.0/admin/containers	GET	New	Container
/1.0/admin/containers	POST	New	Container
/1.0/vcf/user/login	POST	New	User Authentication
/1.0/admin/storage-systems	GET	Modified	Storage Systems
/1.0/admin/storage-systems	POST	Modified	Storage Systems
/2.0/storage/clusters/discover	POST	Modified	Storage Systems
/2.0/storage/capability-profiles	GET	Modified	Storage Capability Profile
/2.0/tasks/{id}	GET	Modified	Task

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

| Storage object	API
Storage VM	api/svm/svms
Aggregate	storage/aggregates
Volume	storage/volumes

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

Container Storage capability profile	Deduplication	Compression
Platinum	Both	Both
AFF_Thick	Both	Both
AFF_Default	Both	Both
AFF_Tiering	Both	Both
AFF_Encrypted	Both	Both
AFF_Encrypted_Tiering	Both	Both
AFF_Encrypted_Min50	Both	Both
FAS_Default	Background	None
FAS_Max20	Background	None
Bronze	None	None

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

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

The VCF deployment of ONTAP tools allows only container creation workflows. If you want to use other workflows such as provisioning datastores, creating storage capability profiles, or disaster recovery, then you should register ONTAP tools with vCenter Server using the Register.html page. The limitation of ONTAP tools in VCF mode is that you cannot configure SRA for disaster recovery.
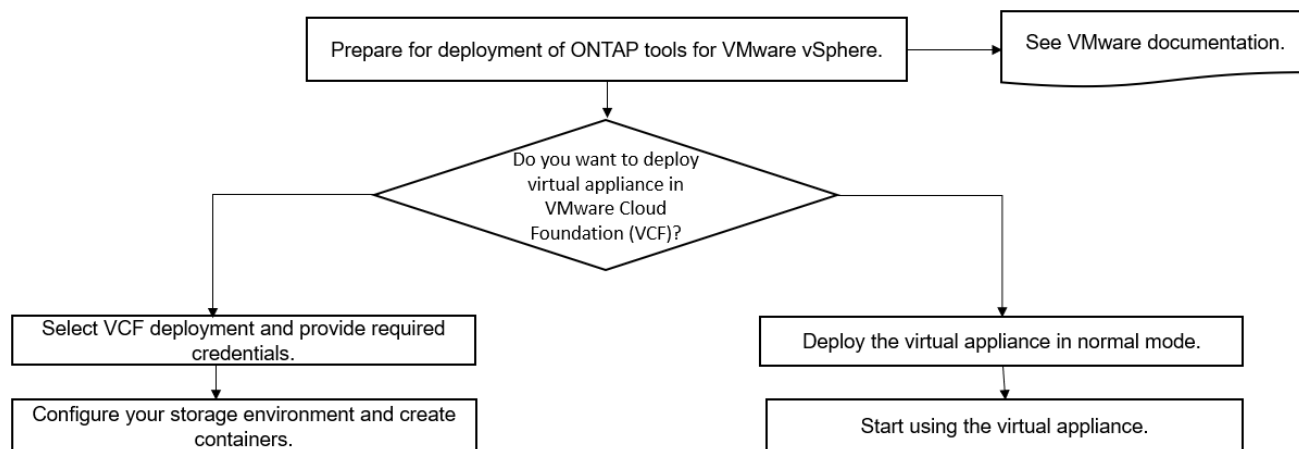
How to deploy ONTAP tools

ONTAP tools for VMware vSphere Quick Start

ONTAP tools for VMware vSphere is a single vCenter Server plug-in that includes VSC, VASA Provider and Storage Replication Adapter (SRA) extensions. VSC is recommended for all ONTAP vSphere environments as it configures ESXi host settings and provisions ONTAP storage using best practices. The VASA Provider is required for virtual volumes (vVols) support, and SRA works together with VMware Site Recovery Manager.

Preparing for installation

You deploy the plug-in as a virtual appliance, which reduces your effort of installing and registering each product separately with the vCenter Server.

Deployment requirements

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

The minimum space and host sizing requirements are:

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

You should be aware of the following licenses:

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

ONTAP tools uses the following default bidirectional TCP ports:

Additional requirements	Description column
9083	When enabled, both VASA Provider and SRA use this port to communicate with the vCenter Server. This port is also required for obtaining the TCP/IP settings.
443	Depending on how you have configured your credentials, the VMware vCenter Server and the storage systems listen for secure communications on this port.
8143	VSC listens for secure communications on this port.
7	VSC sends an echo request to ONTAP to verify reachability and is required only when adding storage system and can be disabled later.

Minimum storage and application requirements:

Storage, host, and applications	Version requirements
ONTAP	ONTAP 9.3, 9.5, 9.6, 9.7, 9.8P1 or later.
VMware vSphere, vCenter server, ESXi hosts, Site Recovery Manager (SRM), plug-in applications, and databases column 1	See the Interoperability Matrix Tool

ONTAP tools requirements

- Configure and set up your vCenter Server environment.
- Download the .ova file.
- The login credentials for your vCenter Server instance.
- Delete the browser cache to avoid any browser cache issue during the deployment of the ONTAP tools.
- Configure the default gateway to be used by the virtual appliance to respond to ICMP pings.
- A valid DNS hostname for the virtual appliance.
- Download and install OnCommand API Services for ONTAP 9.6 or earlier if you want to view the vVols dashboard.
  You do not need to register OnCommand API Services with VASA Provider if you are using ONTAP 9.7 or later.

Optional requirements for SRA

If you are deploying the virtual appliance for use with VMware Site Recovery Manager, then you must have:
* Downloaded the `.msi` file for the SRA plug-in only if you want to configure the Site Recovery Manager (SRM) disaster recovery solution. column 1
* Downloaded the `.tar.gz` file for SRA if you are using the SRM appliance.

Deploying ONTAP tools

Steps

1. Download the `.ova` file from the NetApp Support Site to a vSphere Client system to deploy the ONTAP tools.

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

2. Log in to the vSphere Web Client, select **Home** > **Host & Clusters**.

3. Right-click the required datacenter, and then click **Deploy OVF template**.

4. You can either enter the URL for the .ova file or browse to the folder where the .ova file is saved, and then click **Next**.

5. Enter the required details to complete the deployment.

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

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

Deploying SRA on SRM

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

Installing SRA on Windows SRM server

Steps

1. Download the `.msi` installer for the SRA plug-in from the NetApp Support Site.

2. Double-click the downloaded `.msi` installer for the SRA plug-in and follow the on-screen instructions.

3. Enter the IP address and password of your deployed virtual appliance to complete the installation of the SRA plug-in on the SRM server.

Uploading and configuring SRA on SRM Appliance

Steps

1. Download the `.tar.gz` file from the NetApp Support Site.

2. On the SRM Appliance screen, click **Storage Replication Adapter** > **New Adapter**.

3. Upload the `.tar.gz` file to SRM.

4. Rescan the adapters to verify that the details are updated in the SRM Storage Replication Adapters page.

5. Log in using administrator account to the SRM Appliance using the putty.

6. Switch to the root user: `su root`

7. At the log location enter command to get the docker ID used by SRA docker: `docker ps -l`

8. Login to the container ID: `docker exec -it -u srm <container id> sh`

9. Configure SRM with the ONTAP tools IP address and password: `perl command.pl -I <otv-IP> administrator <otv-password>`
   A success message confirming that the storage credentials are stored is displayed.

Updating SRA credentials

Steps

1. Delete the contents of the /srm/sra/conf directory using:

   a. `cd /srm/sra/conf`

   b. `rm -rf *`

2. Execute the perl command to configure SRA with the new credentials:

   a. `cd /srm/sra/`

   b. `perl command.pl -I <otv-IP> administrator <otv-password>`

Enabling VASA Provider and SRA

Steps

1. Log in to the vSphere web client by using the IP address that you specified during deployment.

2. Click the **OTV** icon, and enter the username and password specified during deployment, click **Sign In**.

3. In the left pane of OTV, **Settings > Administrative Settings > Manage Capabilities**, and enable the required capabilities.

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

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

Requirements for deploying the ONTAP tools

Port requirements for VSC

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

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

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

VSC uses the following default bidirectional TCP ports:

Default port number	Description
9083	When enabled, both VASA Provider and Storage Replication Adapter (SRA) use this port to communicate with the vCenter Server. This port is also required for obtaining the TCP/IP settings.
443	Depending on how you have configured your credentials, the VMware vCenter Server and the storage systems listen for secure communications on this port.
8143	VSC listens for secure communications on this port.
7	VSC sends an echo request to ONTAP to verify reachability and is required only when adding storage system and can be disabled later.

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

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

Space and sizing requirements for the ONTAP tools

Before deploying the ONTAP tools for VMware vSphere, you should be familiar with the

space requirements for the deployment package and some basic host system requirements.

- **Installation package space requirements**
  - 2.1 GB for thin provisioned installations
  - 54.0 GB for thick provisioned installations
- **Host system sizing requirements**
  - ESXi 6.5U3 or later
  - Recommended memory: 12 GB RAM
  - Recommended CPUs: 2

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

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

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

Interoperability Matrix Tool

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

Storage Replication Adapter (SRA) requires the following licenses:

- SnapMirror license

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

- FlexClone license

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

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

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

Considerations for deploying ONTAP tools

Before you deploy ONTAP tools for VMware vSphere, it is good practice to plan your deployment and decide how you want to configure ONTAP tools in your environment.

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

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

Upgrading from an existing deployment of VSC	The upgrade procedure from an existing deployment of VSC to ONTAP tools depends on the version of VSC, and whether you have deployed ONTAP tools. The deployment workflows and upgrade section has more information.
	
	Deployment workflow for existing users of ONTAP tools
	
	Best practices before an upgrade:
	
	• You should record information about the storage systems that are being used and their credentials.
	
	  After the upgrade, you should verify that all of the storage systems were automatically discovered and that they have the correct credentials.
	
	• If you modified any of the standard VSC roles, you should copy those roles to save your changes.
	
	  VSC overwrites the standard roles with the current defaults each time you restart the VSC service.

Regenerating an SSL certificate for VSC	The SSL certificate is automatically generated when you deploy the ONTAP tools. You might have to regenerate the SSL certificate to create a site-specific certificate. Regenerate an SSL certificate for Virtual Storage Console

Setting ESXi server values	Although most of your ESXi server values are set by default, it is a good practice to check the values. These values are based on internal testing. Depending on your environment, you might have to change some of the values to improve performance. • Configure ESXi server multipathing and timeout settings • ESXi host values set using ONTAP® tools for VMware vSphere
Guest operating system timeout values	The guest operating system (guest OS) timeout scripts set the SCSI I/O timeout values for supported Linux, Solaris, and Windows guest operating systems to provide correct failover behavior.

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

Considerations	Description
Requirements of role-based access control (RBAC)	VSC supports both vCenter Server RBAC and ONTAP RBAC. The account used to register VSC to vCenter Server (`https://<appliance_ip>:8143/Register.html`) must be a vCenter Server administrator (assigned to the vCenter Server administrator or administrator role). If you plan to run VSC as an administrator, you must have all of the required permissions and privileges for all of the tasks. If your company requires that you restrict access to vSphere objects, you can create and assign standard VSC roles to users to meet the vCenter Server requirements. You can create the recommended ONTAP roles by using ONTAP System Manager using the JSON file provided with the ONTAP tools. If a user attempts to perform a task without the correct privileges and permissions, the task options are grayed out. • Standard roles packaged with ONTAP tools • Permissions for ONTAP storage systems and vSphere objects
ONTAP version	Your storage systems must be running ONTAP 9.3, 9.5, 9.6, 9.7, 9.8P1 or later.

Storage capability profiles	To use storage capability profiles or to set up alarms, you must enable VASA Provider for ONTAP. After you enable VASA Provider, you can configure VMware Virtual Volumes (vVols) datastores, and you can create and manage storage capability profiles and alarms. The alarms warn you when a volume or an aggregate is at nearly full capacity or when a datastore is no longer in compliance with the associated storage capability profile.

Additional deployment considerations

You must consider few requirements while customizing the deployment ONTAP tools.

Appliance administrator user password

You must not use any spaces in the administrator password.

Appliance maintenance console credentials

You must access the maintenance console by using the "maint" user name. You can set the password for the "maint" user during deployment. You can use the Application Configuration menu of the maintenance console of your ONTAP tools to change the password.

vCenter Server administrator credentials

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

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

vCenter Server IP address

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

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

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

  Both the VSC and VASA certificates will be generated using the same type of IP address used during vCenter Server registration.

  > ⓘ IPv6 is supported only with vCenter Server 6.7 and later.

Appliance network properties

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

operation.

Deploy ONTAP tools

How to download ONTAP tools

You can download the *.ova* file for ONTAP tools for VMware vSphere from the NetApp
Support Site.

The *.ova* file includes the ONTAP tools. When the deployment is complete, all the three products are installed
in your environment. By default, VSC starts working as soon as you decide on the subsequent deployment
model and choose whether to enable VASA Provider and SRA based on your requirements.

You can download ONTAP tools from the NetApp Support Site by using the software download page.

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

How to deploy ONTAP tools

You should deploy ONTAP tools in your environment, and specify the required
parameters, to be able to use the appliance.

What you will need

- You must be running a supported release of vCenter Server.

  > (i) ONTAP tools can be registered either with a Windows deployment of vCenter Server or a
  > VMware vCenter Server Virtual Appliance (vCSA) deployment.

  Interoperability Matrix Tool

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

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

About this task

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

Steps

1. Log in to the vSphere Client.

2. Select **Home** > **Host & Clusters**.

3. Right-click the required datacenter, and then click **Deploy OVA template**.

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

Location	Action
URL	Provide the URL for the .*ova* file for ONTAP tools.
Folder	Select the .*ova* file for ONTAP tools from the saved location.

5. Enter the details to customize the deployment wizard.

   (Optional) In the Configure vCenter or Enable VCF section, select the **Enable VMware Cloud Foundation (VCF)** checkbox and provide a password for ONTAP tools credentials.
   You do not need to provide IP address but providing a password is mandatory.
   See the following for complete details.

   - Deployment customization considerations

   - VMware Cloud Foundation mode of deployment for ONTAP tools

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

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

7. Power on the ONTAP tools virtual machine, and then open a console of the virtual machine running the ONTAP tools.

8. Verify that ONTAP tools is running after the deployment is completed.

9. If ONTAP tools is not registered with any vCenter Server, use
   `` `\https://appliance_ip:8143/Register.html `` to register the VSC instance.

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

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

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

    Clear the vSphere cached downloaded plug-in packages

    ⓘ If you are using ONTAP 9.6 or earlier, then to view the vVols dashboard, you must download and install OnCommand API Services. But for ONTAP 9.7 you do not require OnCommand API Services to be registered with VASA Provider.

Related information

Enable VASA Provider for configuring virtual datastores

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

What you will need

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

About this task

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

Steps

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

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

Register OnCommand API services with ONTAP 9.6 or earlier releases

If you are using ONTAP 9.6 or earlier, then the vVols dashboard can display the details of VMware Virtual Volumes (vVols) datastores and virtual machines only if you have registered OnCommand API Services for VASA Provider to obtain data for the vVols VM and datastore reports.

What you will need

You must have downloaded OnCommand API Services 2.1 or later from the NetApp Support Site.

> ⓘ The vVols dashboard displays performance metrics only when the SAN vVols datastores and virtual machines are configured using ONTAP 9.3 or later.

Steps

1. From the ONTAP tools home page, click **Settings**.

2. Click **Manage Extension** in the Administrative Settings tab.

3. Use the Register OnCommand API Services slider to enable OnCommand API Services.

4. Enter the IP address, service port, and credentials for OnCommand API Services.

   You can also use the Manage VASA Provider Extensions dialog box for the following modifications:

   ○ To update OnCommand API Services registration when there is any change to the credentials.

   ○ To unregister OnCommand API Services when you no longer require the vVols dashboard.

   You must clear the Register OnCommand API Services checkbox to remove the OnCommand API Services registration for VASA Provider.

5. Click **Apply**.

   The vVols dashboard displays the metrics for ONTAP 9.6 or earlier SAN vVols datastores only after the registration of OnCommand API Services is complete.

Related information

NetApp Support

Install the NFS VAAI plug-in

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

What you will need

* You should have downloaded the installation package for the NFS Plug-in for VAAI (`` `.vib ``) from the NetApp Support Site.

  NetApp Support

* You should have installed ESXi host 6.5 or later and ONTAP 9.1 or later.

* You should have powered on the ESXi host and mounted an NFS datastore.

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

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

* You should have enabled the vstorage option on the storage virtual machine (SVM) by using the `vserver nfs modify -vserver vserver_name -vstorage enabled` command.

* You should have ESXi 7.0 update1 or later if you are using NetApp NFS VAAI plug-in 2.0.

Steps

1. Rename the `.vib` file that you downloaded from the NetApp Support Site to NetAppNasPlugin.vib to match the predefined name that VSC uses.

2. Click **Settings** in the ONTAP tools home page.

3. Click **NFS VAAI Tools** tab.

4. Click **Change** in the **Existing version** section.

5. Browse and select the renamed `.vib` file, and then click **Upload** to upload the file to ONTAP tools.

6. In the Install on ESXi Hosts section, select the ESXi host on which you want to install the NFS VAAI plug-in, and then click **Install**.

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

7. Reboot the ESXi host after the installation finishes.

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

Clear the vSphere cached downloaded plug-in packages

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

Steps

1. Logout from your existing vSphere web client or vSphere-UI.

2. Remove the browser cache.

3. Remove the vSphere Client cached plug-in packages. For VCSA, Perform the following:

   a. SSH into the VCSA appliance.

   b. Stop the VMware vSphere Client service:
      `service-control --stop vsphere-ui`

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

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

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

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

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

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

Upgrade ONTAP tools

Upgrade to the latest release of ONTAP tools

You can perform an in-place upgrade to the latest release of ONTAP tools from your existing 9.7P1 or later release following the instructions provided here.

What you will need

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

  Clear the vSphere cached downloaded plug-in packages

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

> (i) You can perform an in-place upgrade to the latest release of ONTAP tools only from your existing 9.7P1 or later versions. When you upgrade to 9.7.1 release of ONTAP tools and you want to use vVols replication, then you will need to setup one more vCenter Server with ONTAP tools with Site Recovery Manager (SRM) installed.

Steps

1. Mount the downloaded *.iso* file to the ONTAP tools:

   a. Click **Edit Settings** > **DVD/CD-ROM Drive**.

   b. Select **Datastore ISO** file from the drop-down list.

   c. Browse to and select the downloaded *.iso* file, and then select the **Connect at power on** checkbox.

2. Access the Summary tab of your deployed ONTAP tools.

3. Click ▶ to start the maintenance console.

4. At the "Main Menu" prompt, enter option 2 for **System Configuration**, and then enter option 8 for **Upgrade**.

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

5. If you want ONTAP tools to be registered with the vCenter Server with the IPv6 address, then you must perform the following:

   a. Unregister ONTAP tools.

   b. Register the IPv6 address of ONTAP tools to vCenter Server using the **Register** page.

   c. Regenerate VSC and VASA Provider certificates after the registration.

   > (i) IPv6 is supported only with vCenter Server 6.7 and later.

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

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

   b. Log in to the vSphere Client.

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

> ⓘ
> - If upgrading from the 7.0 version of ONTAP tools to the latest version of ONTAP tools, you must first create storage capability profiles before attempting to edit an existing VM Storage Policy or you might get an error that there are incorrect or missing values.
>
> - If upgrading from an earlier version to the latest release of ONTAP tools, it is found that the `vvol.rebalance.threshold` property is missing in the `vvol.properties file.
>
>   The default value of the property is set to 85%.
>
> - After you upgrade to the latest OTV(9.10) release that has FIPS enabled but you have a older version of vCenter where FIPS is not supported, the deployment will still work. But if you upgrade your vCenter to the latest FIPS supported version and you have an earlier version of ONTAP tools, then the deployment will work only if FIPS is disabled on the vCenter.

Upgrade Storage Replication Adapter

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

Step

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

| For…	Perform the following…
Windows	a. Log in to the SRM Windows Server. b. Uninstall existing SRA *.msi* installer from SRM Server. c. Change the system path to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\external\perl\c\bin` d. Double-click on the *.msi* installer you downloaded from NetApp support site, and follow on-screen instructions. e. Enter the IP address and password of your deployed ONTAP tools .

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

Configure ONTAP tools

Workflow for configuring ONTAP tools

Configuring ONTAP tools involves configuring your storage systems, creating a storage capability profile, provisioning the datastore, and optionally configuring SRA for disaster recovery.
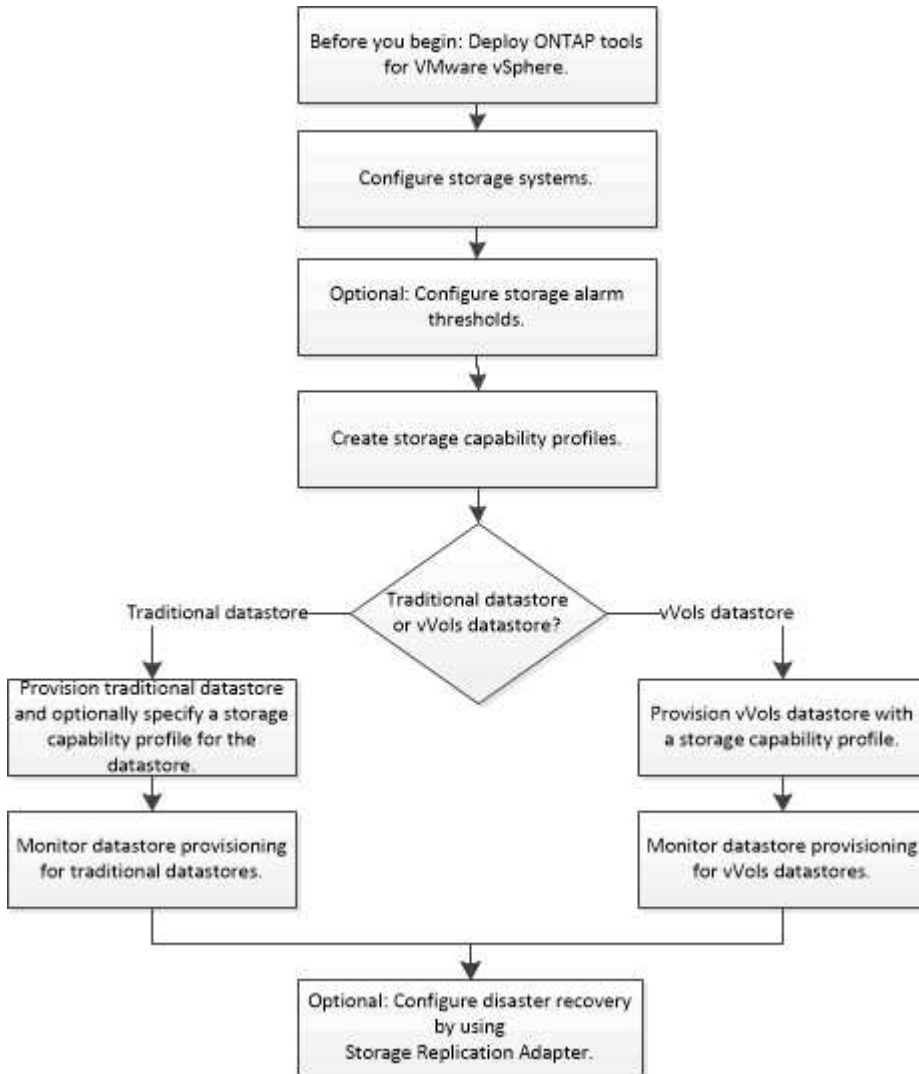
Configure ESXi settings

Configure ESXi server multipathing and timeout settings

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

About this task

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

Normal icon or the Pending Reboot icon.

Steps

1. From the VMware vSphere Web Client Home page, click **vCenter** > **Hosts**.
2. Right-click a host, and then select **Actions** > **NetApp VSC** > **Set Recommended Values**.
3. In the NetApp Recommended Settings dialog box, select the values that work best with your system.

   The standard, recommended values are set by default.
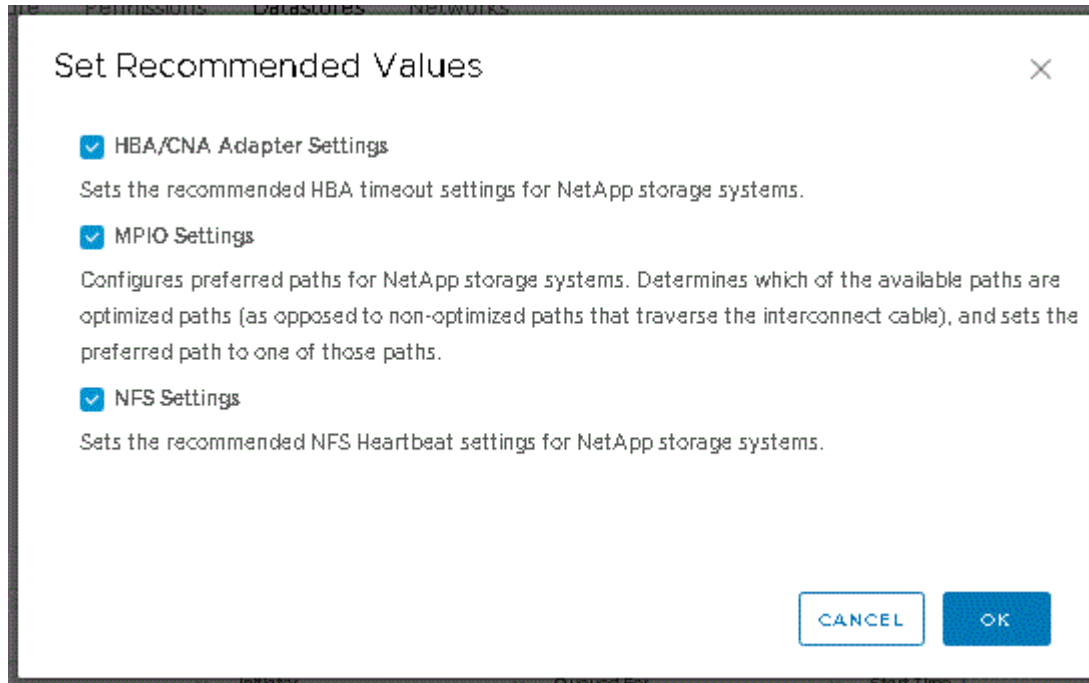
4. Click **OK**.

ESXi host values set using ONTAP tools

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

You can set the following values on an ESXi host:

ESXi advanced configuration

- **VMFS3.HardwareAcceleratedLocking**

  You should set this value to 1.

- **VMFS3.EnableBlockDelete**

  You should set this value to 0.

NFS settings

- **Net.TcpipHeapSize**

  If you are using vSphere 6.0 or later, you should set this value to 32.

- **Net.TcpipHeapMax**

  You should set this value to 512MB for vSphere 6.X releases, except for 6.5U3 and 6.7U3 releases. For vSphere 6.5U3 and 6.7U3 releases set this value to 1024MB. If you are using vSphere 7.0 or later versions, you should set this value to 1024MB.

- **NFS.MaxVolumes**

  If you are using vSphere 6.0 or later, you should set this value to 256.

- **NFS41.MaxVolumes**

  If you are using vSphere 6.0 or later, you should set this value to 256.

- **NFS.MaxQueueDepth**

  If you are using the vSphere 6.0 or later version of ESXi host, then you should set this value to 128 or higher to avoid queuing bottlenecks.

  For vSphere versions prior to 6.0, you should set this value to 64.

- **NFS.HeartbeatMaxFailures**

  You should set this value to 10 for all NFS configurations.

- **NFS.HeartbeatFrequency**

  You should set this value to 12 for all NFS configurations.

- **NFS.HeartbeatTimeout**

  You should set this value to 5 for all NFS configurations.

FC/FCoE settings

- **Path selection policy**

  You should set this value to "RR" (round robin) when FC paths with ALUA are used.

  You should set this value to "FIXED" for all other configurations.

  Setting this value to "RR" helps to provide load balancing across all of the active/optimized paths. The value "FIXED" is used for older, non-ALUA configurations and helps to prevent proxy I/O.

- **Disk.QFullSampleSize**

  You should set this value to 32 for all configurations. Setting this value helps to prevent I/O errors.

- **Disk.QFullThreshold**

You should set this value to 8 for all configurations. Setting this value helps prevent I/O errors.

- **Emulex FC HBA timeouts**

  Use the default value.

- **QLogic FC HBA timeouts**

  Use the default value.

iSCSI settings

- **Path selection policy**

  You should set this value to "RR" for all iSCSI paths.

  Setting this value to "RR" helps to provide load balancing across all of the active/optimized paths.

- **Disk.QFullSampleSize**

  You should set this value to 32 for all configurations. Setting this value helps to prevent I/O errors.

- **Disk.QFullThreshold**

  You should set this value to 8 for all configurations. Setting this value helps prevent I/O errors.

Configure guest operating systems

Configure guest operating system scripts

The ISO images of the guest operating system (OS) scripts are mounted on ONTAP® tools for VMware vSphere server. To use the guest OS scripts to set the storage timeouts for virtual machines, you must mount the scripts from the vSphere Client.

Operating System Type	60-second timeout settings	190-second timeout settings
Linux	https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout-install.iso	https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout_190-install.iso
Windows	https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout.iso	https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout_190.iso
Solaris	https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout-install.iso	https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout_190-install.iso

You should install the script from the copy of the VSC instance that is registered to the vCenter Server that manages the virtual machine. If your environment includes multiple vCenter Servers, you should select the server that contains the virtual machine for which you want to set the storage timeout values.

You should log in to the virtual machine, and then run the script to set the storage timeout values.

Set timeout values for Windows guest operating systems

The guest operating system (OS) timeout scripts set the SCSI I/O timeout settings for Windows guest operating systems. You can specify either a 60-second timeout or a 190-second timeout. You must reboot the Windows guest OS for the settings to take effect.

What you will need

You must have mounted the ISO image containing the Windows script.

Steps

1. Access the console of the Windows virtual machine, and log in to an account with Administrator privileges.

2. If the script does not automatically start, open the CD drive, and then run the `windows_gos_timeout.reg` script.

   The Registry Editor dialog is displayed.

3. Click **Yes** to continue.

   The following message is displayed:

   ```
   The keys and values contained in 'D:\windows_gos_timeout.reg' have been
   successfully added to the registry.`
   ```

4. Reboot the Windows guest OS.

5. Unmount the ISO image.

Set timeout values for Solaris guest operating systems

The guest operating system (OS) timeout scripts set the SCSI I/O timeout settings for Solaris 10. You can specify either a 60-second timeout or a 190-second timeout.

What you will need

You must have mounted the ISO image containing the Solaris script.

Steps

1. Access the console of the Solaris virtual machine, and log in to an account with root privileges.

2. Run the `solaris_gos_timeout-install.sh` script.

   For Solaris 10, a message similar to the following is displayed:

   ```
   Setting I/O Timeout for /dev/s-a - SUCCESS!
   ```

3. Unmount the ISO image.

Set timeout values for Linux guest operating systems

The guest operating system (OS) timeout scripts set the SCSI I/O timeout settings for versions 4, 5, 6, and 7 of Red Hat Enterprise Linux and versions 9, 10, and 11 of SUSE Linux Enterprise Server. You can specify either a 60-second timeout or a 190-second timeout. You must run the script each time you upgrade to a new version of Linux.

What you will need

You must have mounted the ISO image containing the Linux script.

Steps

1. Access the console of the Linux virtual machine, and log in to an account with root privileges.
2. Run the `linux_gos_timeout-install.sh` script.

   For Red Hat Enterprise Linux 4 or SUSE Linux Enterprise Server 9, a message similar to the following is displayed:

   ```
   Restarting udev... this may take a few seconds.
   ```

   ```
   Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
   ```

   For Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, and Red Hat Enterprise Linux 7 a message similar to the following is displayed:

   ```
   patching file /etc/udev/rules.d/50-udev.rules
   ```

   ```
   Hunk #1 succeeded at 333 (offset 13 lines).
   ```

   ```
   Restarting udev... this may take a few seconds.
   ```

   ```
   Starting udev: [ OK ]
   ```

   ```
   Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
   ```

   For SUSE Linux Enterprise Server 10 or SUSE Linux Enterprise Server 11, a message similar to the following is displayed:

```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```

```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev:    done
```

3. Unmount the ISO image.

Requirements for registering VSC in multiple vCenter Servers environment

If you are using ONTAP tools for VMware vSphere in an environment where a single VMware vSphere HTML5 client is managing multiple vCenter Server instances, you must register one instance of VSC with each vCenter Server so that there is a 1:1 pairing between VSC and the vCenter Server. Doing this enables you to manage all of the servers running vCenter 6.0 or later in both linked mode and non-linked mode from a single vSphere HTML5 client.

> ⓘ If you want to use VSC with a vCenter Server, then you must have set up or registered one VSC instance for every vCenter Server instance that you want to manage. Each registered VSC instance must be of the same version.

Linked mode is installed automatically during the vCenter Server deployment. Linked mode uses Microsoft Active Directory Application Mode (ADAM) to store and synchronize data across multiple vCenter Server systems.

Using the vSphere HTML5 client to perform VSC tasks across multiple vCenter Servers requires the following:

• Each vCenter Server in the VMware inventory that you want to manage must have a single VSC server registered with it in a unique 1:1 pairing.

 For example, you can have VSC server A registered to vCenter Server A, VSC server B registered to vCenter Server B, VSC server C registered to vCenter Server C, and so on.

 You **cannot** have VSC server A registered to both vCenter Server A and vCenter Server B.

 If a VMware inventory includes a vCenter Server that does not have a VSC server registered to it, but there are one or more vCenter Servers that are registered with VSC, then you can view the instances of VSC and perform VSC operations for the vCenter Servers that have VSC registered.

• You must have the VSC-specific View privilege for each vCenter Server that is registered to the single sign-on (SSO).

You must also have the correct RBAC permissions.

When you are performing a task that requires you to specify a vCenter Server, the **vCenter Server** drop-down box displays the available vCenter Servers in alphanumeric order. The default vCenter Server is always the first server in the drop-down list.

If the location of the storage is known (for example, when you use the Provisioning wizard and the datastore is on a host managed by a specific vCenter Server), the vCenter Server list is displayed as a read-only option. This happens only when you use the right-click option to select an item in the vSphere Web Client.

VSC warns you when you attempt to select an object that it does not manage.

You can filter storage systems based on a specific vCenter Server from the VSC summary page. A summary page appears for every VSC instance that is registered with a vCenter Server. You can manage the storage systems that are associated with a specific VSC instance and vCenter Server, but you should keep the registration information for each storage system separate if you are running multiple instances of VSC.

Configure the ONTAP tools preferences file

Set IPv4 or IPv6 using the preferences file

The preferences files contain settings that control ONTAP tools for VMware vSphere operations. Under most circumstances, you do not have to modify the settings in these files. It is helpful to know which preference files Virtual Storage Console (VSC) uses.

VSC has several preference files. These files include entry keys and values that determine how VSC performs various operations. The following are some of the preference files that VSC uses:

`/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml`

`/opt/netapp/vscserver/etc/vsc/vscPreferences.xml`

You might have to modify the preferences files in certain situations. For example, if you use iSCSI or NFS and the subnet is different between your ESXi hosts and your storage system, you have to modify the preferences files. If you do not modify the settings in the preferences file, datastore provisioning fails because VSC cannot mount the datastore.

There is a new option added to the preference file `kaminoprefs.xml` that you can set to enable support for IPv4 or IPv6 for all storage systems added to VSC.

- The `default.override.option.provision.mount.datastore.address.family` parameter has been added to the `kaminoprefs.xml` preference file to set a preferred data LIF protocol for datastore provisioning.

  This preference is applicable for all of the storage systems added to VSC.

- The values for the new option are `IPv4`, `IPv6`, and `NONE`.

- By default the value is set to `NONE`.

Value	Description

NONE	• Provisioning happens using the same IPv6 or IPv4 address type of data LIF as the type of cluster or SVM management LIF used for adding the storage. • If the same IPv6 or IPv4 address type of data LIF is not present in the SVM, then the provisioning happens through the other type of data LIF, if available.
IPv4	• Provisioning happens using the IPv4 data LIF in the selected SVM. • If the SVM does not have an IPv4 data LIF, then the provisioning happens through the IPv6 data LIF, if it is available in the SVM.
IPv6	• Provisioning happens using the IPv6 data LIF in the selected SVM. • If the SVM does not have an IPv6 data LIF, then the provisioning happens through the IPv4 data LIF, if it is available in the SVM.

To configure the IPv4 or IPv6 using the user interface, see the following sections:

- Add different subnets
- Enable datastore mounting across different subnets

Add different subnets

You can use the ONTAP tools interface or REST APIs to add different subnets of ESXi hosts. This enables you to either allow or restrict the subnets for datastore mount operation after provisioning storage systems. If you do not add subnets of ESXi hosts then ONTAP tools blocks datastore mount operation for those subnets.

Steps

1. Log in to your vCenter Server instance and access ONTAP tools.
2. On the homepage, click **Settings** > **Manage Subnet Access**.
3. In the Manage Subnet Access dialog box, click **Selected** option in Allowed subnets for NFS Subnets Access.
4. Enter the values for the required subnets, and then click **ADD**.
5. Select either **None** or **Selected** for Restricted subnets.
6. Repeat the above steps for iSCSI Subnets Access, and click **Apply**.

Enable datastore mounting across different subnets

If you use iSCSI or NFS and the subnet is different between your ESXi hosts and your

storage system, you have to modify the ONTAP tools for VMware vSphere preferences files. If you do not modify the preferences file, then datastore provisioning fails because Virtual Storage Console (VSC) cannot mount the datastore.

About this task

When datastore provisioning fails, VSC logs the following error messages:

`Unable to continue. No ip addresses found when cross-referencing kernel ip addresses and addresses on the controller.

Unable to find a matching network to NFS mount volume to these hosts.`

Steps

1. Log in to your vCenter Server instance.

2. Launch the maintenance console using your unified appliance virtual machine.

   [Maintenance Console of ONTAP tools for VMware vSphere](#)

3. Enter `4` to access the Support and Diagnostics option.

4. Enter `2` to access the Access Diagnostic Shell option.

5. Enter `vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml` to update the `kaminoprefs.xml` file.

6. Update the `kaminoprefs.xml` file.

If you use…	Do this…
iSCSI	Change the value of the entry key `default.allow.iscsi.mount.networks` from ALL to the value of your ESXi host networks.
NFS	Change the value of the entry key `default.allow.nfs.mount.networks` from ALL to the value of your ESXi host networks.

   The preferences file includes sample values for these entry keys.

   > ⓘ The value "ALL" does not mean all networks. The "ALL" value enables all of the matching networks, between the host and the storage system, to be used for mounting datastores. When you specify host networks, then you can enable mounting only across the specified subnets.

7. Save and close the `kaminoprefs.xml` file.

Regenerate an SSL certificate for Virtual Storage Console

The SSL certificate is generated when you install Virtual Storage Console (VSC). The distinguished name (DN) that is generated for the SSL certificate might not be a common

name (CN) that the client machines recognize. By changing the keystore and private key passwords, you can regenerate the certificate and create a site-specific certificate.

About this task

You can enable remote diagnostic using the maintenance console and generate site-specific certificate.

Virtual Storage Console: Implementing CA signed certificates

Steps

1. Log in to the maintenance console.

2. Enter `1` to access the Application Configuration menu.

3. In the Application Configuration menu, enter `3` to stop the VSC service.

4. Enter `7` to regenerate SSL certificate.

Configure storage systems

Overview of storage systems for ONTAP tools

You should add storage systems to ONTAP tools and set default credentials, if required, by using the VSC interface.

ONTAP tools for VMware vSphere provides a single mechanism to discover storage systems and to set the storage credentials. The credentials provide the ONTAP permissions that are required to enable Virtual Storage Console (VSC) users to perform tasks by using the storage systems.

Before VSC can display and manage the storage resources, VSC must discover the storage systems. As part of the discovery process, you must supply the ONTAP credentials for your storage systems. These are the privileges (or roles) that are associated with the user name and password pair that is assigned to each storage system. These user name and password pairs use ONTAP role-based access control (RBAC) and must be set up from within ONTAP. You cannot change these credentials from within VSC. You can define ONTAP RBAC roles by using ONTAP System Manager.

> ⓘ If you log in as an administrator, you automatically have all of the privileges for that storage system.

When you add a storage system to VSC, you must supply an IP address for the storage system and the user name and password pair that is associated with that system. You can set up default credentials that VSC will use during the storage system discovery process, or you can manually enter credentials when the storage system is discovered. The details of the storage system that is added to VSC are automatically pushed to the extensions that you enable in your deployment. You do not have to manually add storage to VASA Provider and Storage Replication Adapter (SRA). Both VSC and SRA support the addition of credentials at the cluster level and storage virtual machine (SVM) level. VASA Provider supports only cluster-level credentials for adding storage systems.

If your environment includes multiple vCenter Server instances, when you add a storage system to VSC from the Storage Systems page, the Add Storage System dialog box displays a vCenter Server box where you can specify to which vCenter Server instance the storage system is to be added. If you add a storage system by right-clicking a datacenter name, you do not have the option to specify a vCenter Server instance because the server is already associated with that datacenter.

Discovery happens in one of the following ways. In each case, you must supply credentials for any newly discovered storage system.

- When the VSC service starts, VSC begins its automatic background discovery process.
- You can click the REDISCOVER All button in the **Storage Systems** page, or on a host or datacenter to select it from the **Actions** menu (**Actions** > **Netapp ONTAP tools** > **Update Host and Storage Data**). You can also click **DISCOVER** on the **Getting Started** tab of the 'Overview' section.

All of the VSC features require specific permissions to perform tasks. You can limit what users can do based on the credentials that are associated with the ONTAP role. All of the users that have the same storage system user name and password pair share the same set of storage system credentials and can perform the same operations.

Set default credentials for storage systems

You can use ONTAP tools for VMware vSphere to set default credentials for a storage system in your vCenter Server.

What you will need

You must have selected the vCenter Server that you want to use for creating default credentials.

About this task

If you set up default credentials for storage systems, Virtual Storage Console (VSC) uses these credentials to log in to a storage system that VSC has just discovered. If the default credentials do not work, you must manually log in to the storage system. VSC and SRA support addition of storage system credentials at the cluster level or the SVM level. But VASA Provider will only work with cluster level credentials.

Steps

1. On the ONTAP tools Home page, click **Settings** > **Administrative Settings** > **Configure Default Credentials for Storage System**.

2. In the Storage System Default Credentials dialog box, enter the user name and password for the storage system.

   Storage controller credentials are assigned in ONTAP based on the user name and password pair. The storage controller credentials can either be the administrator account or a custom account that uses role-based access control (RBAC).

   You cannot use VSC to change the roles that are associated with the user name and password pair of the storage controller. To modify or create a new ONTAP user role for use with ONTAP tools, you can use System Manager.

   See the "Configuring user roles and privileges" section.

3. Click **OK** to save the default credentials.

If you updated the storage system credentials because a storage system reported "Authentication Failure" status, you should click the **REDISCOVER ALL** option available on the Storage Systems page. When you do this, VSC tries to connect to the storage system by using the new credentials.

Add storage systems to VSC

You can manually add storage system to Virtual Storage Console (VSC).

About this task

Each time you start Virtual Storage Console (VSC) or select the **REDISCOVER All** option, VSC automatically discovers the available storage systems.

Steps

1. Add a storage system to VSC by using the ONTAP tools home page:

    ◦ Click **Storage Systems** > **Add**.

    ◦ Click **Overview** > **Getting Started**, and then click **ADD** button under Add Storage System.

2. In the **Add Storage System** dialog box, enter the management IP address and credentials for that storage system.

    You can also add storage systems using the IPv6 address of the cluster or SVM. You can also change the defaults for TLS and the port number in this dialog box.

    When you add storage from the VSC Storage System page, you must also specify the vCenter Server instance where the storage will be located. The Add Storage System dialog box provides a drop-down list of the available vCenter Server instances. VSC does not display this option if you are adding storage to a datacenter that is already associated with a vCenter Server instance.

3. Click **OK** after you have added all of the required information.

Discover storage systems and hosts

When you first run Virtual Storage Console (VSC) in a vSphere Client, VSC discovers the ESXi hosts, their LUNs and NFS exports, and the NetApp storage systems that own those LUNs and exports.

What you will need

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

About this task

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

While discovering the storage systems, VSC collects information from the ESXi hosts that are managed by the vCenter Server instance.

Steps

1. From the vSphere Client Home page, select **Hosts and Clusters**.

2. Right-click the required datacenter, and then select **NetApp VSC** > **Update Host and Storage Data** .

VSC displays a Confirm dialog box that informs you that this operation might take a long time.

3. Click **OK**.

4. Select the discovered storage controllers that have the status "Authentication Failure", and then click **ACTIONS** > **Modify**.

5. Fill in the required information in the Modify Storage System dialog box.

6. Repeat steps 4 and 5 for all storage controllers with "Authentication Failure" status.

After the discovery process is complete, perform the following:

- Use VSC 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.

Refresh the storage system display

You can use the update feature that is provided by ONTAP® tools for VMware vSphere to refresh the information about storage systems and to force Virtual Storage Console (VSC) to discover storage systems.

About this task

The "refresh" option is useful if you changed the default credentials for the storage systems after receiving an authentication error. You should always perform an update operation if you changed the storage system credentials after the storage system reported an "Authentication Failure Status". During the update operation, VSC tries to connect to the storage system by using the new credentials.

Depending on your system setup, this task can take a long time to complete.

Steps

1. On the VMware vSphere Client Home page, click **Storage Systems**.
2. Start the update:

If this location is…	Click…
Virtual Storage Console	The **REDISCOVER ALL** icon.
Datacenter	Right-click the datacenter, and then click **NetApp VSC** > **Update Host and Storage Data**.

3. In the Update Host and Storage Data dialog box, click **OK**.

   The discovery might take few minutes depending on the number of hosts and storage systems in your datacenter. This discovery operation works in the background.

4. Click **OK** in the Success dialog box.

Configure alarm thresholds

You can use VSC to set alarms to notify you when volume thresholds and aggregate thresholds reach the set limits.

Steps

1. From the ONTAP tools Home page, click **Settings**.
2. Click **Unified Appliance Settings**.
3. Specify the percent values for the **Nearly full threshold (%)** field and the **Full threshold (%)** field for both the volume alarm thresholds and the aggregate alarm thresholds.

   While setting the values, you must keep the following information in mind:

   - Clicking **Reset** resets the thresholds to the previous values.

     Clicking **Reset** does not reset the thresholds to the default values of 80 percent for "Nearly full" and 90 percent for "Full".

   - There are two ways to set the values:
     - You can use the up and down arrows next to the values to adjust the threshold values.
     - You can slide the arrows on the track bar below the values to adjust the threshold values.

   - The lowest value that you can set for the **Full threshold (%)** field for volumes and aggregates is 6 percent.

4. After specifying the required values, click **Apply**.

   You must click **Apply** for both volume alarm and aggregate alarm.

Configure user roles and privileges

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

What you'll need

- You should have downloaded the ONTAP Privileges file from ONTAP tools using https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip.
- You should have configured ONTAP 9.8P1 or later storage.
- You should have logged in with administrator privileges for the storage system.

Steps

1. Unzip the downloaded `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip` file.
2. Access ONTAP System Manager.
3. Click **CLUSTER** > **Settings** > **Users and Roles**.
4. Click **Add User**.

5. In the Add User dialog box, select **Virtualization products**.

6. Click **Browse** to select and upload the ONTAP Privileges JSON file.

   The PRODUCT field is auto populated.

7. Select the required capability from the PRODUCT CAPABILITY drop-down menu.

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

8. Enter the required username and password.

9. Select the privileges (Discovery, Create Storage, Modify Storage, Destroy Storage) required for the user, and then click **Add**.

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

> ⓘ The uninstall operation does not remove VSC roles but removes the localized names for the VSC-specific privileges and appends the prefix to "XXX missing privilege" them. This behavior happens because the vCenter Server does not provide an option to remove privileges. When you reinstall VSC or upgrade to a newer version of VSC, all of the standard VSC roles and VSC-specific privileges are restored.

Configure storage capability profiles

Overview of storage capability profiles

VASA Provider for ONTAP allows you to create storage capability profiles and map them to your storage. This helps you maintain consistency across the storage. You can also use VASA Provider to check for compliance between the storage and the storage capability profiles.

A storage capability is a set of storage system attributes that identifies a specific level of storage performance, storage efficiency, and other capabilities such as encryption for the storage object that is associated with the storage capability.

For traditional datastores, you can use a storage capability profile to create datastores consistently with common attributes, and assign QoS policy to them. During provisioning VSC displays clusters, SVMs, and aggregates that match the storage capability profile. You can generate a storage capability profile from existing traditional datastores by using the **GLOBAL AUTO-GENERATE PROFILES** option from the Storage Mapping menu. After the profile is created, you can use VSC to monitor the compliance of datastores with the profile.

When used with vVols datastores, the provisioning wizard can use multiple storage capability profiles to create different FlexVol volumes in the datastore. You can use the VM storage policy to automatically create vVols for a virtual machine in appropriate FlexVol volumes as defined. For example, you can create profiles for common storage classes (such as for performance limits and other capabilities like encryption or FabricPool). You can later create VM storage policies in vCenter Server representing business classes of virtual machines and link these to the appropriate storage capability profile by name (for example Production, Test, HR).

When used with vVols, the storage capability profile is also used to set the storage performance for the individual virtual machine and place it on the FlexVol volume in the vVols datastore that best satisfies the performance requirement. You can specify QoS policy with minimum and/or maximum IOPS for performance. You can use the default policies when you initially provision a virtual machine, or change your VM storage

policy later if your business requirements change. The default storage capability profiles for this release of ONTAP tools:

- AFF_Thick

- FAS_MAX20

- FAS_Default

- AFF_Default

- AFF_Tiering

- AFF_Encrypted

- AFF_Encrypted_Tiering

- AFF_Encrypted_Min50

- Platinum

- Bronze

The vCenter Server then associates the storage capability of a LUN or volume with the datastore that is provisioned on that LUN or volume. This enables you to provision a virtual machine in a datastore that matches the storage profile of the virtual machine and to ensure that all of the datastores in a datastore cluster have the same storage service levels.

With ONTAP tools, you can configure every virtual volume (vVols) datastore with a new storage capability profile that supports the provisioning of virtual machines with varying IOPS requirements on the same vVols datastore. While executing the VM provisioning workflow with IOPS requirement, all of the vVols datastores are listed in the compatible datastore list.

> ⓘ When you try to provision or modify virtual machines for vCenter Server earlier than 6.5, only the vVols datastores that contain storage capability profiles with performance set to "MAX_IOPS" are listed in the compatible datastore list. The remaining vVols datastores are listed in the incompatible datastore list. You can ignore this classification and select any vVols datastore from the incompatible datastore list to provision or modify the virtual machine.

Considerations for creating and editing storage capability profiles

You should be aware of the considerations for creating and editing storage capability profiles.

- You can configure Min IOPS only on AFF systems.

- You can configure QoS metrics at a virtual volume (vVols) datastore level.

  This capability provides greater flexibility in assigning varied QoS metrics for different VMDKs of the same virtual machine that is provisioned on a virtual datastore.

- You can configure storage capability profiles for both FAS and AFFdatastores.

  For FAS and AFF systems, you can configure space reserve to be either thick or thin.

- You can use storage capability profiles to provide encryption for your datastores.

- You cannot modify existing storage capability profiles (created prior to 7.2 version) after upgrading from an earlier version of the ONTAP tools for VMware vSphere to the latest version of the ONTAP tools.

  The legacy storage capability profiles are retained for backward compatibility. If the default templates are not in use, then during the upgrade to the latest version of the ONTAP tools, the existing templates are

overridden to reflect the new QoS metrics and tiering policies related to the performance of the storage capability profiles.

- You cannot modify or use the legacy storage capability profiles to provision new virtual datastores or VM storage policies.
- You must use new storage capability profiles for all new datastores.

Create storage capability profiles

You can use VSC to manually create storage capability profiles, automatically generate a profile based on the capabilities of a datastore, or modify a profile to meet your requirements.

What you'll need

You must have registered your VASA Provider instance with ONTAP tools for VMware vSphere.

After setting up a profile, you can edit the profile as required.

Steps

1. On the ONTAP tools Home page, click **Storage Capability Profiles**.
2. Create a profile or edit an existing profile, as required:

If you want to…	Do this…
Create a profile	Click **CREATE** .
Edit an existing profile	Click the profile that you want to modify from the profiles listed on the **Storage Capability Profiles** page.

> ⓘ To view the values that are associated with an existing profile, you can click the profile name in the Storage Capabilities Profile page. VASA Provider then displays the Summary page for that profile.

1. Complete the pages in the Create Storage Capability Profile wizard to set up a profile or to edit values to modify an existing profile.

   Most of the fields in this wizard are self-explanatory. The following table describes some of the fields for which you might require guidance.

Field	Explanation

Identifying multiple profiles	You can use the **Description** field on the Name and Description tab to describe the purpose of the storage capability profile. Providing a good description is useful because it is a good practice to set up different profiles based on the applications that are being used. For example, a business-critical application requires a profile with capabilities that support higher performance, such as an AFF platform. A datastore that is used for testing or training might use a profile with a lower performance FAS platform, and enable all of the storage efficiency capabilities and tiering to control costs. If you have enabled "linked" mode for your vCenter Servers, then you must select the vCenter Server for which you are creating the storage capability profile.
Platform	You can select your storage system to have either the AFF or FAS platform type. The options on the subsequent screens are updated based on your selection of the type of storage system.
Protocol	You can select from the available protocols listed based on the platform selected for the storage system. While configuring virtual machines you can configure VM storage policies with storage capability profile and the protocol field filters datastores based on specific protocol. The field 'Any' allows you to work with all protocols.

Performance	You can set traditional QoS policies for your storage system by using the Performance tab.
	• When you select **None**, a QoS policy with no limit (infinite) is applied to a data VVol.
	• When you select **QoS Policy Group**, then a traditional QoS policy is applied to a VVol.
	You can set the value for **Max IOPS** and **Min IOPS** which enables you to use the QoS functionality. If you select Infinite IOPS, the Max IOPS field is disabled. When applied for a traditional datastore, a QoS policy with "Max IOPS" value is created and assigned to a FlexVol volume. When used with a vVols datastore, a QoS policy with Max IOPS and Min IOPS values is created for each data vVols datastore.
	NOTE:
	◦ Max IOPS and Min IOPS can also be applied to the FlexVol volume for a traditional datastore.
	◦ You must ensure that the performance metrics are not also set separately at an storage virtual machine (SVM) level, an aggregate level, or a FlexVol volume level.

Storage Attributes	The storage attributes that you can enable in this tab depend on the storage type that you select in the Personality tab.
	• If you select FAS storage, you can configure space reserve (thick or thin), enable deduplication, compression, and encryption. The tiering attribute is disabled because this attribute is not applicable to FAS storage. • If you select AFF storage, you can enable encryption and tiering. Deduplication and compression are enabled by default for AFF storage and cannot be disabled. The tiering attribute enables the use of volumes that are part of a FabricPool-enabled aggregate (supported by VASA Provider for AFF systems with ONTAP 9.4 and later). You can configure one of the following policies for the tiering attribute: • None: Prevents volume data from being moved to the capacity tier • Snapshot: Moves user data blocks of volume Snapshot copies that are not associated with the active file system to the capacity tier

2. Review your selections on the Summary page, and then click **OK**.

   After you create a profile, you can return to the Storage Mapping page to view which profiles match which datastores.

Generate storage capability profiles automatically

VASA Provider for ONTAP enables you to automatically generate storage capability profiles for existing traditional datastores. When you select the auto-generate option for a datastore, VASA Provider creates a profile that contains the storage capabilities that are used by that datastore.

What you will need

• You must have registered your VASA Provider instance with Virtual Storage Console (VSC).

• VSC must have discovered your storage.

About this task

After you create a storage capability profile, you can modify the profile to include more capabilities. The Create storage capability profile wizard provides information about the capabilities that you can include in a profile.

Steps

1. From the ONTAP tools home page, click **Storage Mapping**.

2. Select the datastore from the available list.

3. From the Actions menu, select **Auto-generate**.

4. When the auto-generate process finishes, refresh the screen to view information about the new profile.

   The new profile is listed in the Associated profile column. The name of the new profile is based on the resources in the profile. You can rename the profile, if required.

Configure datastores

Provision traditional datastores

Provisioning a datastore creates a logical container for your virtual machines and their virtual machine disks (VMDKs). You can provision a datastore, and then attach the datastore to a single host, to all of the hosts in a cluster, or to all of the hosts in a datacenter.

What you will need

- To provision a datastore on an SVM that is directly connected to Virtual Storage Console (VSC), you must have added the SVM to VSC by using a user account that has the appropriate privileges, not the default vsadmin user account or vsadmin role.

  You can also provision a datastore by adding a cluster.

- You must ensure that the subnet details of all the networks to which the ESXi host is connected is entered in the kaminoprefs.xml.

  See "Enabling datastore mounting across different subnets".

- If you use NFS or iSCSI, and the subnet is different between your ESXi hosts and your storage system, then the NFS or iSCSI settings in the kaminoprefs preferences file must include ESXi host subnet masks.

  This preference file is also applicable to vVols datastore creation. See *Enable datastore mounting across different subnets* and *Configure the VSC preferences files* for more information.

- If you have enabled VASA Provider and you want to specify storage capability profiles for your NFS datastores or VMFS datastores, then you must have created one or more storage capability profiles.

- To create an NFSv4.1 datastore, you must have enabled NFSv4.1 at the SVM level.

The **Provision Datastore** option enables you to specify a storage capability profile for the datastore. Storage capability profiles help in specifying consistent service level objectives (SLOs) and simplify the provisioning process. You can specify a storage capability profile only if you have enabled VASA Provider. The ONTAP tools for VMware vSphere supports the following protocols:

- NFSv3 and NFSv4.1

- VMFS5 and VMFS6

VSC can create a datastore on either an NFS volume or a LUN:

- For an NFS datastore, VSC creates an NFS volume on the storage system, and then updates the export policies.

- For a VMFS datastore, VSC creates a new volume (or uses an existing volume, if you selected that option), and then creates a LUN and an igroup.

> ⓘ
> - ONTAP tools supports provisioning of VMFS5 and VMFS6 datastores up to the maximum VMFS LUN and volume size of 64TB when used with ASA and approved AFF systems running ONTAP 9.8 and later.
>
>   On other platforms the maximum LUN size supported is 16TB.
>
> - VMware does not support NFSv4.1 with datastore clusters.

- For Kerberos authentication, you will need the following:
  - Windows machine with Active Directory (AD)
  - Domain Name Server (DNS)
  - Key Distribution Center (KDC)
  - ONTAP Storage System (Cluster) with Kerberos configured
  - ESXi host with Kerberos configured

If a storage capability profile is not specified during provisioning, you can later use the Storage Mapping page to map a datastore to a storage capability profile. You can apply storage QoS settings, throughput ceiling (Max IOPS) and throughput floor (Min IOPS) on data VMDK files of virtual machines provisioned on FlexGroup backed datastore. QoS settings can be applied either at datastore level or at individual virtual machine level by right clicking the datastore. The right click option is available only on those datastores or virtual machines that are backed by FlexGroup datastore. After the QoS is applied to a datastore, any pre-existing datastore or virtual machine QoS settings are overridden. QoS settings cannot be applied at a datastore level or at a virtual machine level for datastores that are provisioned on direct SVM's, because ONTAP does not support QoS at SVM management level.

Steps

1. You can access the datastore provisioning wizard using one of the following:

If you select from …	Perform the following…
vSphere Client home page	a. Click **Hosts and Clusters**. b. In the navigation pane, select the datacenter on which you want to provision the datastore. c. To specify the hosts to mount the datastore, see the next step.
ONTAP tools home page	a. Click **Overview**. b. Click **Getting Started** tab. c. Click **Provision** button. d. Click **Browse** to select the destination to provision the datastore as per the next step.

2. Specify the hosts on which you want to mount the datastore.

To make the datastore available to…	Do this…
All of the hosts in a datacenter	Right-click a datacenter, and then select **NetApp ONTAP tools** > **Provision Datastore**.
All of the hosts in a cluster	Right-click a host cluster, and then select **NetApp ONTAP tools** > **Provision Datastore**.
A single host	Right-click a host, and select **NetApp ONTAP tools** > **Provision Datastore**.

3. Complete the fields in the New Datastore dialog box to create the datastore.

   Most of the fields in the dialog box are self-explanatory. The following table describes some of the fields for which you might require guidance.

Section	Description
General	The General section of the New Datastore provisioning dialog box provides options to enter the destination, name, size, type, and protocol for the new datastore. You can select either **NFS** or **VMFS** type of protocol to configure a traditional datastore. For NFS, you can either select NFS3 or NFS 4.1. This release allows you to configure a VMFS datastore of maximum size 64TB. You can select the option "Distribute datastore data across the ONTAP cluster" to provision a FlexGroup volume on the storage system. Selecting this option automatically deselects the checkbox "Use Storage Capability Profile for provisioning". For FlexGroup datastore provisioning, ONTAP cluster that are 9.8 and above only are listed for selection. The vVols datastore type is used to configure a vVols datastore. If VASA Provider is enabled, then you can also decide whether to use storage capability profiles. The **Datastore cluster** option is available only for traditional datastores. You should use the **Advanced** option to specify **VMFS5** or **VMFS6** file system.
Kerberos authentication	If you have selected NFS 4.1 in the **General** page, select the security level. Kerberos authentication is supported only for Flexvols.

Storage system	You can select one of the listed storage capability profiles if you have selected the option in the General section. • If you are provisioning a FlexGroup datastore, then the storage capability profile for this datastore is not supported. The system-recommended values for the storage system and storage virtual machine are populated for ease. But you can modify the values if required. • For Kerberos authentication, the storage systems enabled for Kerberos are listed.
Storage attributes	By default, VSC populates the recommended values for **Aggregates** and **Volumes** options. You can customize the values based on your requirements. Aggregate selection is not supported for FlexGroup datastores as ONTAP manages the aggregate selection. The **Space reserve** option available under **Advanced** menu is also populated to give optimum results. (Optional) You can specify the initiator group name in the **Change initiator group name** field. • A new initiator group will be created with this name if one does not already exist. • The protocol name will be appended to the specified initiator group name. • If an existing igroup is found with the selected initiators, the igroup will be renamed with the provided name and will be reused. • If you do not specify an igroup name, igroup will be created with the default name.
Summary	You can review the summary of the parameters you specified for the new datastore. The field "Volume Style" enables you to differentiate the type of datastore created. The "Volume Style" can be either "FlexVol" or "FlexGroup".

ⓘ A FlexGroup that is part of a traditional datastore cannot shrink below the existing size but can grow by 120% maximum. Default snapshots are enabled on these FlexGroup volumes.
. In the Summary section, click **Finish**.

Related information

Map datastores to storage capability profiles

You can map the datastores that are associated with VASA Provider for ONTAP to storage capability profiles. You can assign a profile to a datastore that is not associated with a storage capability profile.

What you will need

- You must have registered your VASA Provider instance with ONTAP® tools for VMware vSphere.
- Virtual Storage Console (VSC) must have already discovered your storage.

You can map traditional datastore with a storage capability profile or change the storage capability profile that is associated with a datastore. VASA Provider does *not* display any virtual volume (VVol) datastores on the Storage Mappings page. All the datastores that are referred to in this task are traditional datastores.

Steps

1. From the ONTAP tools Home page, click **Storage Mapping**.

   From the Storage Mapping page, you can determine the following information:

   ◦ The vCenter Server that is associated with the datastore
   ◦ How many profiles match the datastore

     The Storage Mapping page displays only traditional datastores. This page does not display any VVol datastores or qtree datastores.

   ◦ Whether the datastore is currently associated with a profile

     A datastore can match multiple profiles, but a datastore can be associated with only one profile.

   ◦ Whether the datastore is compliant with the profile that is associated with it

2. To map a storage capability profile to a datastore or to change the existing profile of a datastore, select the datastore.

   To locate specific datastores or other information on the Storage Mapping page, you can enter a name or a partial string in the search box. VSC displays the search results in a dialog box. To return to the full display, you should remove the text from the search box, and then click **Enter**.

3. From the Actions menu, select **Assign matching profile**.

4. Select the profile that you want to map to the datastore from the list of matching profiles that is provided in

the **Assign profile to datastore** dialog box, and then click **OK** to map the selected profile to the datastore.

5. Refresh the screen to verify the new assignment.

Assign QoS policies

The provisioning of FlexGroup datastores does not support assigning storage capability profiles to the datastores. But you can assign QoS policies to virtual machines that are created on FlexGroup backed datastores.

About this task

The QoS policies can be applied either at a virtual machine level or a datastore level. The QoS policies are required for a datastore to configure throughput (Max and Min IOPS) thresholds. When you set QoS on a datastore it is applied to the virtual machines residing on the datastore and not on the FlexGroup volume. But if you set QoS on all the virtual machines in a datastore, then any individual QoS settings for the virtual machines are overridden. This is applicable only to the virtual machines available in the datastore and not to any migrated or added virtual machines. If you want to apply QoS to newly added or migrated virtual machines of a particular datastore, then you have to manually set the QoS values.

ⓘ You cannot apply QoS settings at a datastore or virtual machine level for datastores that are provisioned on direct storage VM's because ONTAP does not support QoS at storage VM management level.

Steps

1. On the ONTAP tools homepage, click **Menu** > **Host and Clusters**.

2. Right-click the required datastore or virtual machine and click **NetApp ONTAP tools** > **Assign QoS**.

3. In the Assign QoS dialog box, enter values the required IOPS values, and click **Apply**.

Verify datastore compliance with the mapped storage capability profile

You can quickly verify whether your datastores are compliant with the storage capability profiles that are mapped to the datastores.

What you will need

- You must have registered your VASA Provider instance with ONTAP® tools for VMware vSphere (VSC).
- VSC must have discovered your storage.

Steps

1. From the ONTAP tools Home page, click **Storage Mapping**.

2. Review the information in the Compliance Status column to identify non-compliant datastores and review the alerts for non-compliance reason.

ⓘ When you click the **COMPLIANCE CHECK** button, VSC performs a rediscovery operation for all of the storage, which might take few minutes.

If a datastore is no longer compliant with its profile, then the Compliance Status column displays an alert stating the reason for non-compliance. For example, a profile might require compression. If that setting has

been changed on the storage, compression is no longer used, and the datastore is non-compliant.

When you discover a datastore that is not compliant with its profile, you can modify the settings on the volume backing the datastore to make the datastore compliant, or you can assign a new profile to the datastore.

You can modify the settings from the Storage Capability Profile page.

Provision vVols datastores

You can provision a vVols datastore using the Provision Datastore wizard only if VASA Provider is enabled in your ONTAP tools.

What you will need

- You should ensure that the subnet details of all the networks to which the ESXi hosted is connected is entered in the Kaminoprefs.xml.

  See **Enabling datastore mounting across different subnets** section.

- You should configure similar replication policy and schedule on the datastores at both the source and target sites for reverse replication to be successful.

The Provision datastore menu enables you to specify a storage capability profile for the datastore, which helps in specifying consistent service level objectives (SLOs) and simplifies the provisioning process. You can specify a storage capability profile only if you have enabled VASA Provider.

FlexVol volumes that are used as backing storage are displayed on the vVols dashboard only if they are running ONTAP 9.5 or later. You should not use the vCenter Server New Datastore wizard to provision vVols datastores.

- You must use cluster credentials to create vVols datastores.

  You cannot use SVM credentials to create vVols datastores.

- VASA Provider does not support the cloning of a virtual machine that is hosted on the vVols datastore of one protocol to another datastore with a different protocol.

- You should have completed cluster pairing and SVM pairing both on the source and destination sites.

About this task

> (i) The 9.10 release of ONTAP tools supports creating vVols datastores with vmdk size greater than 16TB for All SAN Array (ASA) type ONTAP 9.9.1 or later storage platforms.

Steps

1. From the vSphere Client home page, click **Hosts and Clusters**.

2. In the navigation pane, select the datacenter on which you want to provision the datastore.

3. Specify the hosts on which you want to mount the datastore.

To make the datastore available to…	Do this…

All of the hosts in a datacenter	Right-click a datacenter, and then select **NetApp VSC** > **Provision Datastore**.
All of the hosts in a cluster	Right-click a cluster, and then select **NetApp VSC** > **Provision Datastore**.
A single host	Right-click a host, and then select **NetApp VSC** > **Provision Datastore**.

4. Complete the fields in the New Datastore dialog box to create the datastore.

   Most of the fields in the dialog box are self-explanatory. The following table describes some of the fields for which you might require guidance.

Section	Description
General	The General section of the New Datastore dialog box provides options to enter the location, name, description, type, and protocol for the new datastore. The vVols datastore type is used to configure a vVols datastore. ⓘ If you are provisioning iSCSI vVols datastore for vVols replication, then before creating vVols datastore at the target site, you need to perform SnapMirror update and cluster rediscovery.
Storage system	This section enables you to select whether you want the vVols datastore to have either replication enabled or disabled. Only asynchronous type replication profile is allowed for this release. You can then select one or more storage capability profiles listed. The system recommended values of paired **Storage system** and **Storage VM** are populated automatically. The recommended values are populated only if they are paired in ONTAP. You can modify these values if required. **Note:** While creating FlexVol volumes in ONTAP, you should ensure to create them with the attributes you wish to select in the storage capability profile. Both read write and data protection FlexVol volumes should have similar attributes. After FlexVol volumes are created and SnapMirror is initialized in ONTAP, you should run a storage rediscovery in VSC to be able to see the new volumes.

Storage attributes	You should select the schedule for SnapMirror and the required FlexVol volume from the existing list. This schedule should be similar to the one selected in the VM Storage Policies page. The user should have created FlexVol volumes on ONTAP with SnapMirror that are listed. You can select the default storage capability profile to be used for creating vVols using the **Default storage capability profile** option. By default all the volumes are set to maximum Autogrow size to 120 % and default Snapshots are enabled on these volumes.
	Note:
	• A FlexVol volume that is part of a vVols datastore cannot shrink below the existing size but can grow by 120% maximum. Default snapshots are enabled on this FlexVol volume.
	• The minimum size of FlexVol volume that you should create is 5GB.

5. In the Summary section, click **Finish**.

Result

A Replication group is created in the backend when a vVols datastore is configured.

Related information

[Analyze performance data using the vVols dashboard](#)

Rebalance vVols datastores

ONTAP tools supports a command to rebalance FlexVol volumes in your datacenter. The main goal is to enable even space utilization among FlexVol volumes. ONTAP tools redistributes vVols among existing volumes based on space usage, thin provisioning, LUN count, and storage capability profiles.

The rebalancing of vVols datastore is performed by LUN move or file move. The criteria considered during vVols rebalancing are as follows:

- NFS vVol datastores are not supported
- Existing FlexVol volumes will not be resized and neither will new FlexVol volumes be added
- Only FlexVol volumes that have same storage capability or volume attributes are rebalanced
- FlexVol volumes with highest space utilization are considered for rebalancing
- All vVols associated with a virtual machine are moved to the same FlexVol volumes
- LUN and File count limit is retained
- Rebalance is not performed if the delta between the FlexVol volumes space utilization is 10%

The rebalance command removes empty FlexVol volumes to provide space for other datastores. Thus, the command enables you to remove unwanted FlexVol volumes so that they can be removed from the datastore. The command intends to move all the vVols associated with a virtual machine to same FlexVol volume. There is a precheck performed by the command before rebalance is started to minimize failures. But even with successful precheck, the rebalance operation might fail for one or more vVols. When this happens, then there is no rollback of the rebalance operation. So, vVols associated with a virtual machine might be placed on different FlexVol volumes and will result in warning logs.

- Parallel datastore and virtual machine operations are not supported.
- You must perform cluster rediscovery operation after every vVols rebalance operation completes.
- During vVols rebalance operation, if large number of vVols datastores are identified, then the transfer operation times out after the set default value.
  - If this occurs, then you should modify the `vvol.properties` file to set the value to `offtap.operation.timeout.period.seconds=29700` and restart VASA Provider service.
- If a FlexVol volume has Snapshots, then during the vVols rebalance operation, the vVols are not correctly rebalanced due to insufficient details on the space utilization.
- You can set the VASA Provider property *enable.update.vvol.through.discovery* to true to get consistent data between ONTAP tools and ONTAP, when timeout occurs during container rebalance operation.

Protect datastores and virtual machines

Enable SRA to protect datastores

The ONTAP tools for VMware vSphere provides the option to enable the SRA capability to be used with VSC to configure disaster recovery.

What you will need

- You must have set up your vCenter Server instance and configured ESXi.
- You must have deployed ONTAP tools.
- You must have downloaded the `.msi` file for the SRA plug-in, or the `.tar.gz` file for SRM appliance only if you want to configure the Site Recovery Manager (SRM) disaster recovery solution.

  Site Recovery Manager Installation and Configuration Site Recovery Manager 8.2 has more information.

About this task

The flexibility to enable VASA Provider and SRA capabilities enables you to execute only the workflows that you require for your enterprise.

Steps

1. Log in to the web user interface of VMware vSphere.
2. From the vSphere Client, click **Menu** > **ONTAP tools Console**.
3. Click **Settings**.
4. Click **Manage Capabilities** in the **Administrative Settings** tab.
5. In the **Manage Capabilities** dialog box, select the SRA extension want to enable.
6. Enter the IP address of ONTAP tools and the administrator password, and then click **Apply**.
7. You can use one of the following methods to deploy SRA:

For Windows SRM	For SRM appliance
a. Double-click the downloaded `.msi` installer for the SRA plug-in. b. Follow the on-screen instructions. c. Enter the IP address and password of your deployed ONTAP tools.	a. Access the SRM appliance page, and then go to Storage Replication Adapters page of SRM appliance. b. Click **New Adapter**. c. Upload the *.tar.gz* installer for the SRA plug-in to SRM. d. Rescan the adapters to verify that the details are updated in the SRM Storage Replication Adapters page.

You must log out of the vSphere Client, and then log in again to verify that your selected extension is available for configuration.

Related information

Configure storage system for disaster recovery

Configure Storage Replication Adapter for SAN environment

You must set up the storage systems before running Storage Replication Adapter (SRA) for Site Recovery Manager (SRM).

What you will need

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

- SRM

  Documentation about installing SRM is on the VMware site.

  VMware Site Recovery Manager Documentation

- SRA

  The adapter is installed either on SRM.

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 FC or iSCSI connectivity to the storage virtual machine (SVM). The secondary site ESXi hosts should have access to the secondary site storage, similarly 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 by using the `fcp show initiators` command or the `iscsi show initiators` command on the SVMs. Check the LUN access for the mapped LUNs in the ESXi to verify FC and iSCSI connectivity.

Configure Storage Replication Adapter for NAS environment

What you will need

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

- SRM

  Documentation about installing SRM can be found on the VMware site.

  VMware Site Recovery Manager Documentation

- SRA

The adapter is installed on SRM and the SRA server.

Steps

1. Verify that the datastores at the protected site contain virtual machines that are registered with vCenter Server.

2. Verify that the ESXi hosts at the protected site have mounted the NFS exports volumes from the storage virtual machine (SVM).

3. Verify that valid addresses such as the IP address, host name, or FQDN on which the NFS exports are present are specified in the **NFS Addresses** field when using the Array Manager wizard to add arrays to SRM.

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.

NetApp Support

Configure Storage Replication Adapter for highly scaled environment

You must 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 SRM 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.

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

VMware vSphere Documentation: Change Storage Provider Settings

Storage settings

You must set the value of the `storage.commandTimeout` and `storage.maxConcurrentCommandCnt` timeout interval for highly scaled environments to 99,999 seconds.

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

You should also set the maximum time for SRA to perform a single operation in the vvol.properties file: offtap.operation.timeout.period.seconds=86400.

NetApp Knowledgebase Answer 1001111: NetApp Storage Replication Adapter 4.0/7.X for ONTAP Sizing Guide

VMware documentation on modifying SAN Provider settings has more information.

VMware Site Recovery Manager Documentation: Change Storage Settings

Configure SRA on the SRM Appliance

After you have deployed the SRM Appliance, you should configure SRA on the SRM Appliance. The successful configuration of SRA enables SRM Appliance to communicate with SRA for disaster recovery management. You should store the ONTAP tools credentials (IP address and administrator password) in the SRM Appliance to enable communication between SRM Appliance and SRA.

What you will need

You should have downloaded the *tar.gz* file from NetApp Support Site.

About this task

The configuration of SRA on SRM Appliance stores the SRA credentials in the SRM Appliance.

Steps

1. On the SRM Appliance screen, click **Storage Replication Adapter** > **New Adapter**.
2. Upload the *.tar.gz* file to SRM.
3. Rescan the adapters to verify that the details are updated in the SRM Storage Replication Adapters page.
4. Log in using administrator account to the SRM Appliance using putty.
5. Switch to the root user using the command: `su root`
6. Run command `cd /var/log/vmware/srm` to navigate to the log directory.
7. At the log location enter the command to get the docker ID used by SRA: `docker ps -l`
8. To login to the container ID, enter command: `docker exec -it -u srm <container id> sh`
9. Configure SRM with the ONTAP tools IP address and password using the command: `perl command.pl -I <otv-IP> administrator <otv-password>`

   A success message confirming that the storage credentials are stored is displayed. SRA can communicate with SRA server using the provided IP address, port and credentials.

Update SRA credentials

For SRM to communicate with SRA, you should update SRA credentials on the SRM server if you have modified the credentials.

What you will need

You should have executed the steps mentioned in the topic "Configuring SRA on SRM appliance".

Configuring SRA on the SRM Appliance

Steps

1. Delete the contents of the `/srm/sra/conf` directory using:

   a. `cd /srm/sra/conf`

   b. `rm -rf *`

2. Execute the perl command to configure SRA with the new credentials:

   a. `cd /srm/sra/`

   b. `perl command.pl -I <otv-IP> administrator <otv-password>`

Migration of Windows SRM to SRM Appliance

If you are using Windows based Site Recovery Manager(SRM) for disaster recovery and you want to use the SRM Appliance for the same setup, then you should migrate your Windows disaster recovery setup to the appliance based SRM.

The steps involved in the migration of the disaster recovery are:

1. Upgrading your existing ONTAP tools to the 9.7.1 release.

   Upgrade to the latest release of ONTAP tools

2. Migrating Windows based Storage Replication Adapter to Appliance based SRA.

3. Migrating Windows SRM data to SRM Appliance.

See Migrate from Site Recovery Manager for Windows to Site Recovery Manager Virtual Appliance for detailed steps

Configure replication for vVols datastore to protect virtual machines

You can configure replication for your vVols datastore using ONTAP tools. The main aim of vVols replication is to protect critical virtual machines during disaster recovery using VMware Site Recovery Manager (SRM).

However, to configure vVols replication for ONTAP tools, VASA Provider capability and vVols replication must be enabled. VASA Provider is enabled by default in ONTAP tools. The Array Based Replication is performed at the FlexVol level. Each vVols datastore is mapped to a storage container that consists of one or more FlexVol volumes. The FlexVol volumes should be pre-configured with SnapMirror from ONTAP.
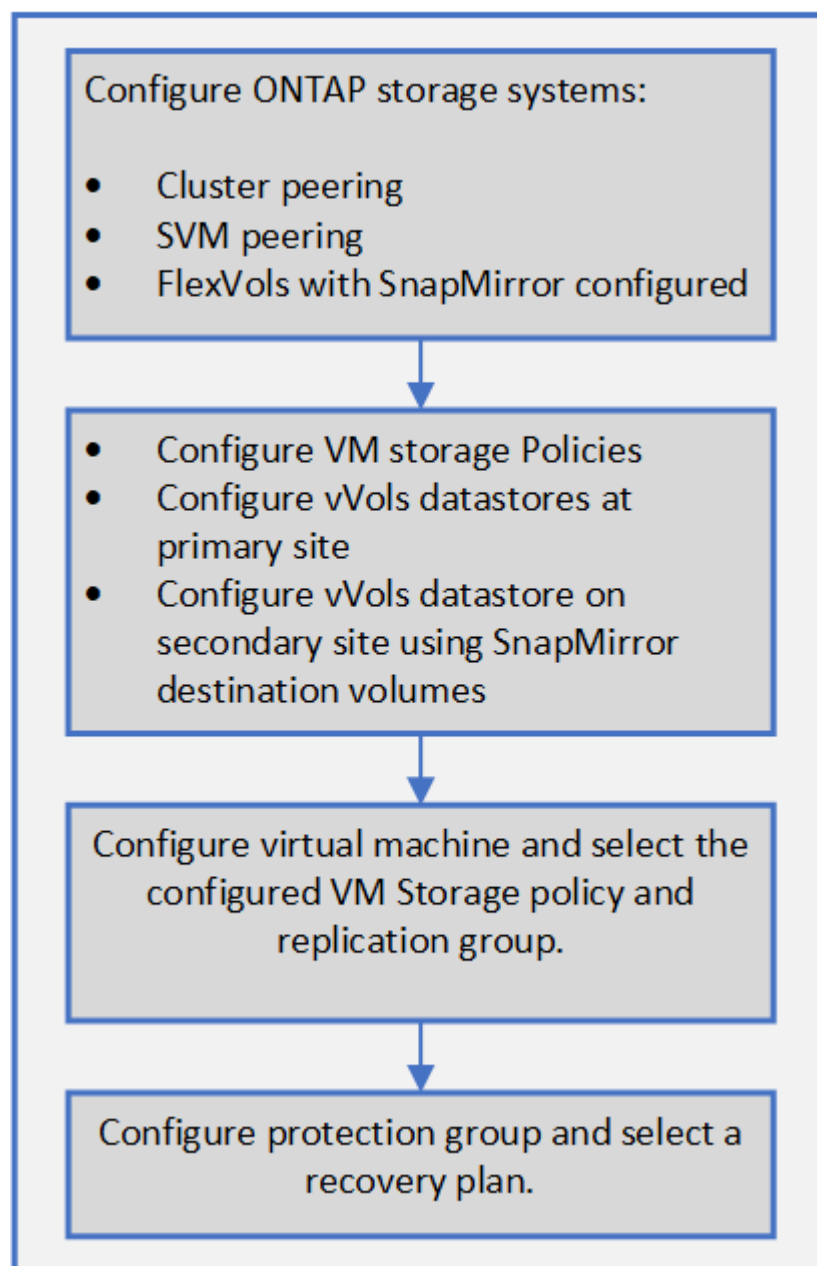
> ⚠️ You should not configure a mix of protected and unprotected virtual machines in a single vVols datastore. A reprotect operation after failover will cause unprotected virtual machines to be deleted. Ensure that all virtual machines in a vVols datastore are protected when using replication.

Replication groups are created during vVols datastore create workflow for each FlexVol volume. To use vVols replication, you will need to create VM Storage Policies that include replication status and schedule along with storage capability profile. A Replication group includes virtual machines that are replicated as part of disaster recovery to the target site. You can configure replication groups with protection groups and recovery plans using SRM console, for DR workflows.

> ℹ️ If you are using disaster recovery for vVols datastore, then you do not need to configure Storage Replication Adapter (SRA) separately as VASA Provider capability is enhanced to have vVols replication.

Configure ONTAP storage systems:

- Cluster peering
- SVM peering
- FlexVols with SnapMirror configured

↓

- Configure VM storage Policies
- Configure vVols datastores at primary site
- Configure vVols datastore on secondary site using SnapMirror destination volumes

↓

Configure virtual machine and select the configured VM Storage policy and replication group.

↓

Configure protection group and select a recovery plan.

Configure vVols replication for existing datastores

Configure vVols replication for existing datastores

The vVols replication feature is enhanced to provide vVols replication for existing virtual machines that were created before SRM setup. This enables you to recover existing virtual machines and protect them on the recovery site.

What you will need

- Cluster and SVM are peered.
- Datastores and FlexVol volumes are created on source and target sites.
- Source and target sites have same storage capability profiles.
- FlexVol volumes are having same SnapMirror schedule.
- vVols replication is enabled.

An existing datastore does not have replication groups created.

Steps

1. Access Swagger interface.

2. Execute the REST API to configure replication group for existing datastore.

   API: /3.0/admin/{datastore}/replication-groups

3. Create VM Storage policy for existing vVols datastore with the storage capability profile that was used to create the datastore.

   Add the replication policy, replication schedule, and compatible datastore from the available list.

> ⓘ If you are using System Manager to protect the Flexvol volumes and storage capability profile has QoS policy as 'None', then ensure that the **Enforce Performance Limit** option is unchecked for disaster recovery to succeed.

   a. Access the unprotected virtual machine and edit the VM storage policy.

   b. Select the VM Storage policy and datastore.

   c. Add the replication group to the unprotected virtual machine.

New datastore | Select a datastore for vVols replication. | Existing datastore

Configure ONTAP storage systems:
- Cluster peering
- SVM peering
- FlexVols with SnapMirror configure

Configure ONTAP storage systems:
- Cluster peering
- SVM peering
- FlexVols with SnapMirror configure

- Configure VM storage policies
- Configure vVols datastores at primary site
- Configure vVols datastores at secondary site using SnapMirror destination volumes

Configure replication group using REST API calls.

Configure virtual machine and select the configured VM storage policy and replication group.

- Configure VM storage policies with replication group and replication schedule
- Configure the same replication for target site

Configure protection group and select a recovery plan.

Apply the configured VM storage policy to selected existing datastore.

Configure protection group and select a recovery plan.

NOTE:

- When configuring a virtual machine to enable replication for an existing datastores, ensure to verify the FlexVol volume that has a Config vVols.

- When vVols of an existing virtual machine are spread across multiple datastores, then you should move all the vVols of that virtual machine using vMotion to a single datastore before enabling replication.

Protect unprotected virtual machines

You can configure protection for your existing unprotected virtual machines that were created using VM storage Policy with replication disabled. To provide protection, you should change the VM storage policy and assign a replication group.

About this task

If SVM is having both IPv4 and IPv6 LIFs, then you should disable IPv6 LIFs and later perform disaster recovery workflows.

Steps

1. Click the required virtual machine and verify that it is configured with default VM storage policy.

2. Right-click the selected virtual machine, and click **VM Policies** > **Edit VM Storage Policies**.

3. Select a VM Storage policy that has replication enabled from the **VM storage policy** drop-down.

4. Select a replication group from the **Replication group** drop-down, and then click **OK**.

5. Verify the Summary of the virtual machine to confirm that the virtual machine is protected.

◦ This release of ONTAP tools does not support hot clone of protected virtual machines. You should power off the virtual machine and then perform the clone operation.

◦ If a datastore does not appear in ONTAP tools after a Reprotect operation, then you should run a storage system discovery or wait for the next scheduled discovery operation.

Configure protected and recovery sites

Configure VM Storage Policies

You should configure VM storage policies to manage virtual machines that are configured on vVols datastore and to enable services like replication for the virtual disks. For the traditional datastores, it is optional to use these VM storage policies.

About this task

The vSphere web client provides default storage policies. But you can create policies and assign them to the virtual machines.

Steps

1. On the vSphere Client page, click **Menu** > **Policies and Profiles**.

2. Click **VM Storage Policies** > **Create VM Storage Policy**.

3. In the Create VM Storage Policy page, provide the following details:

   a. Enter a name and description for the VM Storage Policy.

   b. Select **Enable rules for "NetApp clustered Data ONTAP.VP.vvol" storage**.

   c. Select the required storage capability profile in the Placement tab.

   d. Select the **Custom** option to enable Replication.

   e. Click **ADD RULE** to select **Asynchronous** replication and required SnapMirror Schedule, and then click **NEXT**.

   f. Verify the compatible datastores listed, and then click **NEXT** in the Storage compatibility tab.

   For vVols datastores having data protection FlexVol volumes, compatible datastores check is not performed.

4. Review your VM Storage Policy selection in the **Review and finish** tab, and then click **Finish**.

Configure protection groups

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

What you will need

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

- Same version of SRM installed

- vVols datastore configured with replication enabled and datastore mounted
- Similar storage capability profiles
- Similar VM Storage Policies with replication capability that must be mapped in SRM
- Virtual machines
- Paired protected and recovery sites
- Source and destination datastores should be mounted on respective sites

Steps

1. Log in to your vCenter Server, and then click **Site Recovery** > **Protection Groups**.
2. In the **Protection Groups** pane, click **New**.
3. Specify a name and description for the protection group, direction, and then click **NEXT**.
4. In the **Type** field, select one of the following:

For…	Type field option…
Traditional datastore	Datastore groups (array-based replication)
vVols datastore	Virtual Volumes (vVol replication)

   The fault domain is nothing but SVMs with replication enabled. The SVMs that have only peering implemented and with no issues are displayed.

5. In the Replication groups tab, select either the enabled array pair or the replication groups that have the virtual machine you configured, and then click **NEXT**.

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

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

Pair protected and recovery sites

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

What you will need

- You must have installed Site Recovery Manager (SRM) on the protected and recovery sites.
- You must have installed SRA on the protected and recovery sites.

About this task

SnapMirror fan-out configurations are those where a source volume is replicated to two different destinations. These create a problem during recovery when SRM needs to recover the virtual machine from destination.

ⓘ   Storage Replication Adapter (SRA) does not support fan-out SnapMirror configurations.

Steps

1. Double-click **Site Recovery** on the vSphere Client home page, and then click **Sites**.

2. Click **Objects** > **Actions** > **Pair Sites**.

3. In the Pair Site Recovery Manager Servers dialog box, enter the address of the protected site's Platform Services Controller, and then click **Next**.

4. In the Select vCenter Server section, do the following:

    a. Verify that the protected site's vCenter Server appears as a matching candidate to pair.

    b. Enter the SSO administrative credentials, and then click **Finish**.

5. If prompted, click **Yes** to accept the security certificates.

Result

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

Configure protected and recovery site resources

Configure network mappings

You must 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 must complete the following resource configurations:

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

What you will need

You must have connected the protected and recovery sites.

Steps

1. Log in to your vCenter Server and click on **Site Recovery** > **Sites**.

2. Select your protected site, and then click **Manage**.

3. In the Manage tab, select **Network Mappings**.

4. Click the icon to create a new network mapping.

    The Create Network Mapping wizard appears.

5. In the Create Network Mapping wizard, perform the following:

    a. Select **Automatically Prepare Mappings for Networks with Matching Names**, and click **Next**.

    b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.

    c. Click **Next** after mappings are created successfully.

    d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Result

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

Configure folder mappings

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

What you will need

You must have connected the protected and recovery sites.

Steps

1. Log in to your vCenter Server, and click on **Site Recovery** > **Sites**.

2. Select your protected site, and then click **Manage**.

3. In the Manage tab, select **Folder Mappings**.

4. Click the ![icon] icon to create a new folder mapping.

   The Create Folder Mapping wizard appears.

5. In the Create Folder Mapping wizard, perform the following:

    a. Select **Automatically Prepare Mappings for Folders with Matching Names**, and click **Next**.

    b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.

    c. Click **Next** after mappings are created successfully.

    d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Result

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

Configure resource mappings

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

What you will need

You must have connected the protected and recovery sites.

> ⓘ   In Site Recovery Manager (SRM), resources can be resource pools, ESXi hosts, or vSphere clusters.

Steps

1. Log in to your vCenter Server, and click on **Site Recovery** > **Sites**.

2. Select your protected site, and then click **Manage**.

3. In the Manage tab, select **Resource Mappings**.

4. Click the ![icon] icon to create a new resource mapping.

   The Create Resource Mapping wizard appears.

5. In the Create Resource Mapping wizard, perform the following:

   a. Select **Automatically Prepare Mappings for Resource with Matching Names**, and click **Next**.

   b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.

   c. Click **Next** after mappings are created successfully.

   d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Result

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

Map storage policies

You should map the storage policies on the protected site to the storage policies on the recovery site for your recovery plan to place the recovered virtual machines on the appropriate datastores based on your mappings. After the virtual machine is recovered on recovery site, mapped VM Storage Policy will be assigned to virtual machine.

Steps

1. On the vSphere Client, click **Site Recovery** > **Open Site Recovery**.

2. In the Site Pair tab, click **Configure** > **Storage Policy Mappings**.

3. Select the required site, and then click **New** to create a new mapping.

4. Select the option **Automatically prepare mappings for storage policies with matching names**, and then click **NEXT**.

   SRM will select storage policies on the protected site for which a storage policy with the same name exists on the recovery site. You can also select the manual mapping option to select multiple storage policies.

5. Click **Add mappings**, and the click **NEXT**.

6. In the **Reverse mapping** section, select the required check boxes for mapping, and then click **NEXT**.

7. In the **Ready to complete** section, review your selections and click **FINISH**.

Configure placeholder datastores

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

What you will need

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

Steps

1. Log in to your vCenter Server, and click on **Site Recovery** > **Sites**.

2. Select your protected site, and then click **Manage**.

3. In the Manage tab, select **Placeholder Datastores**.

4. Click the ⚑ icon to create a new placeholder datastore.

5. Select the appropriate datastore, and then click **OK**.

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

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

Configure SRA using array manager

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

What you will need

- You must have paired the protected sites and recovery sites in SRM.
- You must have configured your storage before configuring the array manager.
- You must have configured and replicated the SnapMirror relationships between the protected sites and recovery sites.
- You must 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 of the SVMs in the cluster. If you add storage at an SVM level, then you can manage only that specific SVM.

> ⓘ   VMware does not support NFS4.1 protocol for SRM.

Steps

1. In SRM, click **Array Managers**, and then click **Add Array Manager**.

2. Enter the following information to describe the array in SRM:

    a. Enter a name to identify the array manager in the **Display Name** field.

    b. In the **SRA Type** field, select **NetApp Storage Replication Adapter for ONTAP**.

    c. Enter the information to connect to the cluster or the SVM:

    - If you are connecting to a cluster, you should enter the cluster management LIF.

    - If you are connecting directly to an SVM, you should enter the IP address of the SVM management

LIF.

> (i) When configuring the array manager, you must use the same connection and credentials for the storage system that was used to add the storage system in Virtual Storage Console's Storage Systems menu. For example, if the array manager configuration is SVM scoped, then the storage under VSC must be added at SVM level.

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

       You can also leave this field blank.

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

       You can enter the source volume at the protected site and the replicated destination volume at the recovery site. You can enter either the full volume name or the partial volume name.

       For example, if you want to discover volume src_vol1 that is in a SnapMirror relationship with volume dst_vol1, you must 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. You can enter either the full volume name or the partial volume name.

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

    g. **(Optional)** Enter the user name of the cluster-level account or SVM-level account in the **Username** field.

    h. Enter the password of the user account in the **Password** field.

3. Click **Next**.

4. Verify that the array is discovered and displayed at the bottom of the Add Array Manager window.

5. Click **Finish**.

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

Verify replicated storage systems

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

What you will need

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

Steps

1. Log in to your vCenter Server.

2. Navigate to **Site Recovery** > **Array Based Replication**.

3. Select the required SVM, and then verify the corresponding details in the Array Pairs.

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

Manage ONTAP tools

Manage datastores

Mount datastore on additional hosts

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.

What you will need

You must ensure that the subnet details of all the networks to which the ESXi hosted is connected is entered in the `Kaminoprefs.xml`.

See Enabling datastore mounting across different subnets section.

Steps

1. From the vSphere Client Home page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the host.
3. Repeat Step 2 for any additional hosts.
4. Right-click the host, and then select **NetApp ONTAP tools** > **Mount Datastores**.
5. Select the datastores that you want to mount, and then click **OK**.

Resize datastores

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

About this task

If you want VSC to resize the containing volume when it resizes the VMFS datastore, you should not use the **Use existing volume** option under Storage attributes section when initially provisioning VMFS datastore, but instead let it automatically create a new volume for each datastore.

You can increase or decrease the size of an NFS datastore but for a VMFS datastore, you can only increase the size. Resizing of datastore is also supported for FlexGroup datastores with auto grow and shrink option. A FlexGroup that is part of a traditional datastore and FlexVol volume that is part of a vVols datastore cannot shrink below the existing size but can grow by 120% maximum. Default snapshots are enabled on these FlexGroup and FlexVol volumes.

(i) If you are using All SAN Array (ASA) type storage platforms with ONTAP 9.9.1 or later, only then you can create vVols datastores with vmdk size greater than 16TB.

Steps

1. From the vSphere Client Home page, click **Hosts and Clusters**.
2. In the navigation pane, select the datacenter that contains the datastore.

3. Right-click the datastore and select **NetApp ONTAP tools** > **Resize non-vVols datastore**.

4. In the Resize dialog box, specify a new size for the datastore, and then click **OK**.

   You can run the **REDISCOVER ALL** option in the Storage Systems menu to manually update the storage listing under Storage Systems and dashboard, or wait for the next scheduled refresh.

Edit a vVols datastore

You can edit an existing VMware Virtual Volumes (vVols) datastore to change the default storage capability profile. The default storage capability profile is primarily used for Swap vVols.

Steps

1. From the vSphere Client page, click **Hosts and Clusters**.

2. Right-click the datastore, and then select **NetApp ONTAP tools** > **Edit Properties of vVols Datastore**.

   The Edit Properties of vVols Datastore dialog box is displayed.

3. Make the required changes.

   You can change the default storage capability profile for the vVols datastore by selecting a new profile from the drop-down list in the Edit vVols Datastore dialog box. You can also change the vVols datastore name and description.

   > ⓘ You cannot change the vCenter Server where the vVols datastore is located.

4. When you have made your changes, click **OK**.

   A message box asks whether you want to update the vVols datastore.

5. Click **OK** to apply your changes.

   A success message appears to inform that the vVols datastore has been updated.

Add storage to a vVols datastore

You can increase the available storage by using the Add Storage wizard to add FlexVol volumes to an existing VMWare Virtual Volumes (vVols) datastore.

About this task

When you add a FlexVol volume, you also have the option of changing the storage capability profile associated with that volume. You can either use the VASA Provider auto-generate feature to create a new profile for the volume, or you can assign one of the existing profiles to the volume.

- While expanding a vVols datastore with replication capabilities, you cannot create new FlexVol volumes but can only select pre-configured FlexVol volumes from the existing list.

- When cloning a protected virtual machine deployed on datastore with vVols replication fails due to insufficient space, then you should increase the FlexVol volume size.

- When a vVols datastore is created on a AFF cluster, then you cannot expand the datastore with another FlexVol volume that has auto generate storage capability profile.

  ◦ You can expand the vVols datastore with FlexVol volumes that have pre-created storage capability profiles.

Steps

1. On the vSphere Client Home page, click **Hosts and Clusters**.
2. Right-click the vVols datastore, and then select **NetApp ONTAP tools** > **Expand Storage of vVol Datastore**.
3. On the Expand Storage of vVols Datastore page, you can either add an existing FlexVol volume to the vVols datastore, or create a new FlexVol volume to add to the database.

If you select…	Perform the following…
Select volumes	a. Select the FlexVol volumes that you want to add to the vVols datastore. b. In the Storage Capability Profiles column, use the drop-down list to either create a new profile based on the FlexVol volumes, or select one of the existing profiles. The auto-generate feature creates a profile based the storage capabilities that are associated with that FlexVol volume. For example: disk type, high availability, disaster recovery, performance features, and deduplication.
Create new volumes	a. Enter the name, size, and storage capability profile for the FlexVol. The aggregates are selected by the system based on the storage capability profile selected. b. Select the **Auto Grow** option and provide the maximum size. c. Click **ADD** to add the FlexVol to the list of volumes.

Reminder: All FlexVol volumes in a vVols datastore must be from the same storage virtual machine (SVM, formerly known as Vserver).

After you create a FlexVol volume, you can edit it by clicking the **Modify** button. You can also delete it.

4. Select a default storage capability profile to be used during virtual machine creation, and then click **Next** to review the summary of the storage added to vVols datastore.

5. Click **Finish**.

Result

The wizard adds the storage that you specified to the vVols datastore. It displays a success message when it finishes.

> ⓘ The Expand Storage of vVols Datastore wizard automatically handles any ESXi storage rescans or any other significant operations that are required. Because a vVols datastore is a logical entity controlled by VASA Provider, adding the FlexVol volume is the only thing you need to do to enlarge the capacity of your storage container.

Remove storage from a vVols datastore

If a VMware Virtual Volumes (vVols) datastore has multiple FlexVol volumes, you can remove one or more of the FlexVol volumes from the vVols datastore without deleting the datastore.

About this task

A vVols datastore exists as long as at least one FlexVol volume is available on the datastore. If you want to delete a vVols datastore in a HA cluster, then you should first unmount the datastore from all hosts within the HA cluster, and then delete the residing .vsphere-HA folder manually using vCenter Server user interface. You can then delete the vVols datastore.

Steps

1. From the vSphere Client Home page, click **Hosts and Clusters**.

2. Right-click the vVols datastore that you want to modify, and then select **NetApp ONTAP tools** > **Remove Storage from vVols Datastore**.

   The Remove Storage from vVols Datastore dialog box is displayed.

3. Select the FlexVol volumes that you want to remove from the vVols datastore, and click **Remove**.

4. Click **OK** in the confirmation dialog box.

> ⓘ If you select all of the FlexVol volumes, an error message is displayed, indicating that the operation will fail.

Mount a vVols datastore

You can mount a VMware Virtual Volumes (vVols) datastore to one or more additional hosts by using the Mount vVols Datastore dialog box. Mounting the datastore provides storage access to additional hosts.

Steps

1. From the vSphere Client Home page, click **Hosts and Clusters**.

2. Right-click the datastore that you want to mount, and then select **NetApp ONTAP tools** > **Mount vVols Datastore**.

   The Mount vVols Datastore dialog box is displayed, which provides a list of the hosts that are available in the datacenter where you can mount the datastore. The list does not include the hosts on which the datastore has already been mounted, hosts that are running ESX 5.x or earlier, or hosts that do not support the datastore protocol. For example, if a host does not support the FC protocol, you cannot mount an FC datastore to the host.

   > ⓘ   Even though the vSphere Client provides a mount dialog box for the vCenter Server, you must always use the VASA Provider dialog box for this operation. VASA Provider sets up access to storage systems that are running ONTAP software.

3. Select the host on which you want to mount the datastore, and then click **OK**.

Manage virtual machines

Considerations for migrating or cloning virtual machines

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

Migrate protected virtual machines

You can migrate the protected virtual machines to:

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

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

Clone protected virtual machines

You can clone protected virtual machines to the following:

- Same container of same FlexVol volume using replication group

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

- Same container of a different FlexVol volume using replication group

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

- Different container or vVols datastore

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

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

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

Virtual Machine Snapshots

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

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

Migrate traditional virtual machines to vVols datastores

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

What you will need

You must have ensured 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 traditional 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 then click **Migrate**.

2. Select **Change storage only**, and then click **Next**.

3. Select a virtual disk format, a VM Storage Policy, and a VVol datastore that matches the features of the datastore that you are migrating, and then click **Next**.

4. Review the settings, and then click **Finish**.

Migrate virtual machines with older storage capability profiles

If you are using the latest version of ONTAP tools for VMware vSphere, then you should migrate your virtual machines that are provisioned with the "MaxThroughput MBPS" or "MaxThroughput IOPS" QoS metrics to new VVol datastores that are provisioned with the "Max IOPS" QoS metrics of the latest version of ONTAP tools.

About this task

With the latest version of ONTAP tools, you can configure QoS metrics for each virtual machine or virtual machine disk (VMDK). The QoS metrics were earlier applied at the ONTAP FlexVol volume level and were shared by all of the virtual machines or VMDKs that were provisioned on that FlexVol volume.

Starting with the 7.2 version of ONTAP tools, the QoS metrics of one virtual machine is not shared with other

virtual machines.

> ⓘ You must not modify the existing VM Storage Policy as the virtual machines might become non-compliant.

Steps

1. Create vVols datastores by using a new storage capability profile with the required "Max IOPS" value.
2. Create a VM Storage Policy, and then map the new VM Storage Policy with the new storage capability profile.
3. Migrate the existing virtual machines to the newly created VVol datastores by using the new VM Storage Policy.

Modify ESXi host settings using ONTAP tools

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

What you will need

You must have configured an ESXi host system for your vCenter Server instance.

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

Steps

1. From the vSphere Client Home page, click **ONTAP tools**.
2. Edit the ESXi host settings.

If you want to edit the ESXi host settings from…	Do this…
Issues displayed	a. Click the issue in the ESXi Host Systems portlet. b. Click the ESXi host names for which you want to modify the settings. c. Right-click the ESXi host name, and click **NetApp ONTAP tools** > **Set Recommended Values**. d. Modify the required settings, and then click **OK**.
vSphere Client home page	a. Click **Menu** > **Hosts and Clusters**. b. Right-click the required ESXi host, and select **NetApp ONTAP tools** > **Set Recommended Value**. c. Click **OK**.

ESXi Host Systems portlet	a. Click the **Traditional dashboard** tab in the Overview section of VSC.
	b. Click **Edit ESXi Host Settings**.
	c. Select the ESXi host name in the Host settings and status tab for which you want to modify the settings, and click **NEXT**.
	d. Select the required settings in the Recommended host settings tab, and then click **Next**.
	e. Review your selection in the Summary tab, and then click **FINISH**.

Access ONTAP tools maintenance console

Overview of ONTAP tools maintenance console

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

You must have installed VMware tools after deploying ONTAP tools to access the maintenance console. You should use "maint" as the user name and the password you configured during deployment to log in to the maintenance console of the ONTAP tools.

> ⓘ   You must set a password for the "diag" user while enabling remote diagnostics.

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

Console Menu	Options

Application Configuration	1. Display server status summary
	2. Start Virtual Storage Console service
	3. Stop Virtual Storage Console service
	4. Start VASA Provider and SRA service
	5. Stop VASA Provider and SRA service
	6. Change 'administrator' user password
	7. Re-generate certificates
	8. Hard reset key Store and certificates
	9. Hard reset database
	10. Change LOG level for Virtual Storage Console service
	11. Change LOG level for VASA Provider and SRA service
	12. Display TLS configuration
System Configuration	1. Reboot virtual machine
	2. Shutdown virtual machine
	3. Change 'maint' user password
	4. Change time zone
	5. Add new NTP server
	You can provide an IPv6 address for your NTP server.
	6. Enable SSH Access
	7. Increase jail disk size (/jail)
	8. Upgrade
	9. Install VMware Tools

Network Configuration	1. Display IP address settings
	2. Change IP address settings
	You can use this option to change the IP address post deployment to IPv6.
	3. Display domain name search settings
	4. Change domain name search settings
	5. Display static routes
	6. Change static routes
	You can use this option to add an IPv6 route.
	7. Commit changes
	8. Ping a host
	You can use this option to ping to an IPv6 host.
	9. Restore default settings
Support and Diagnostics	1. Generate support bundle
	2. Access diagnostic shell
	3. Enable remote diagnostic access

Virtual Storage Console and VASA Provider log files

You can check the log files in the `/opt/netapp/vscserver/log` directory and the `/opt/netapp/vpserver/log` directory when you encounter errors.

The following three log files can be helpful in identifying problems:

- `cxf.log`, containing information about API traffic into and out of VASA Provider
  `*kaminoPrefs.xml`, containing information about VSC settings

- `vvolvp.log`, containing all log information about VASA Provider

The maintenance menu of ONTAP tools for VMware vSphere enables you to set different log levels for your requirement. The following log levels are available:

- Info
- Debug
- Error
- Trace

When you set the log levels, the following files are updated:

- VSC server: `kamino.log` and `vvolvp.log`

- VASA Provider server: `vvolvp.log`, `error.log`, and `netapp.log`

In addition, the VASA Provider web command-line interface (CLI) page contains the API calls that were made, the errors that were returned, and several performance-related counters. The web CLI page is located at `https://<IP_address_or_hostname>:9083/stats`.

Change the administrator password

You can change the administrator password of ONTAP tools post deployment using the maintenance console.

Steps

1. From the vCenter Server, open a console to the ONTAP tools.
2. Log in as the maintenance user.
3. Enter `1` in the maintenance console to select Application Configuration.
4. Enter `6`to select **Change 'administrator' user password**.
5. Enter a password with minimum eight characters and maximum 63 characters.
6. Enter `y`in the confirmation dialog box.

Configure VASA Provider to work with SSH

You can set up VASA Provider to use SSH for secure access by configuring the ONTAP tools .

About this task

When you configure SSH, you must log in as the maintenance user. This is because root access to VASA Provider has been disabled. If you use other login credentials, you cannot use SSH to access VASA Provider.

Steps

1. From the vCenter Server, open a console to the ONTAP tools.
2. Log in as the maintenance user.
3. Enter `3` to select **System Configuration**.
4. Enter `6` to select **Enable SSH Access**.
5. Enter `y` in the confirmation dialog box.

Configure remote diagnostic access

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

What you will need

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

About this task

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

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

    The login session remains valid only until 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 3 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.

Collect the log files

You can collect log files for ONTAP tools for VMware vSphere from the option available in the VSC graphical user interface (GUI). Technical support might ask you to collect the log files to help troubleshoot a problem.

About this task

If you need VASA Provider log files, you can generate a support bundle from the Vendor Provider Control Panel screen. This page is part of the VASA Provider maintenance menus, which are accessible from the virtual appliance's console.

```
https://vm_ip:9083
```

You can collect the VSC log files by using the "Export VSC Logs" feature in the VSC GUI. When you collect a VSC log bundle with VASA Provider enabled, the VSC log bundle will also have the VP logs. The following steps tell you how to collect the VSC log files:

Steps

1. From the ONTAP tools home page, click **Configuration** > **Export VSC Logs**.

   This operation can take several minutes.

2. When prompted, save the file to your local computer.

   You can then send the *.zip* file to technical support.

Monitor performance of datastores and vVols reports

Overview of ONTAP tools datastore and vVols reports

You can use the ONTAP tools console **Reports** menu to view pre-defined reports for all the datastores managed by a selected VSC instance in a particular vCenter Server. You can perform operations such as sorting and exporting reports.

Reports display detailed information about datastores and virtual machines, that enables you to review and identify potential issues with datastores and virtual machines in your vCenter Server

You can view, sort, and export reports.

Virtual Storage Console (VSC) provides the following pre-defined reports:

- Datastore Report
- Virtual Machine Report
- vVols Datastore Report
- vVols Virtual Machine Report

Datastore Reports

The datastore reports provide detailed information about traditional datastores and the virtual machines that are created on these datastores.

The traditional dashboard enables you to review and identify potential issues with the datastores and virtual machines in your vCenter Server. You can view, sort, and export reports. The data for the traditional datastores and virtual machines report is provided by the vCenter Server. But due to the introduction of FlexGroup backed datastore support, some metrics such as latency, throughput, and IOPS are obtained from ONTAP.

> ⓘ File monitoring is not supported for FlexGroup datastores configured on direct storage virtual machines (SVMs).

The datastore provides the following pre-defined reports:

- Datastore Report
- Virtual Machine Report

Datastore Report

The Datastore Report menu provides information on the following parameters for datastores:

- Name of the datastore
- Type of datastore: NFS or VMFS
- Volume style

  The volume style can either be a FlexVol volume or a FlexGroup volume.

- Free space
- Used space

- Total space

- Percentage of space utilized

- Percentage of space available

- IOPS

  The report displays the IOPS for the datastore.

- Latency

  The report displays the latency information for the datastore.

  You can also verify the time at which the report was generated. The Datastore Report menu enables you to organize the report as per your requirement, and then export the organized report using the **Export to CSV** button. The datastore names in the report are links that navigate to the Monitor tab of the selected datastore, where you can view the datastore performance metrics.

Virtual Machine Report

The Virtual Machine Report menu provides the performance metrics for all the virtual machines that use datastores provisioned by VSC for a selected vCenter Server. The virtual machine metrics displayed in the Virtual Machine Reports is historical data that is collected every 30 minutes for virtual machines on traditional datastores. The "Last refresh time" and "Next refresh time" are added to the table to provide details on when the data was collected and when will be the next data collection.

- Name of the virtual machine

- Datastore name

- Volume style

  The volume style can be either a FlexVol volume or a FlexGroup volume.

- Source

  The source to gather details for the virtual machine can be either ONTAP or vCenter Server.

- Latency

  The report displays the latency for virtual machines across all datastores associated with the virtual machines.

- IOPS

- Throughput

- Committed capacity

  The report displays the value for the committed capacity for a virtual machine.

- Host

  The report displays the host systems on which the virtual machine is available.

- Uptime

  The report displays the time for which the virtual machine is powered on and is available on an ESXi host.

* Power state

  The report displays whether the virtual machine is powered on or powered off.

Each virtual machine name in the report is a link to the Monitor tab of the selected virtual machine. You can sort the virtual machine report as per your requirement and export the report in a .CSV file, and save the report on your local system. The timestamp of the report is also appended to the saved report.

For virtual machines that are backed by FlexGroup volumes, when new virtual machine is powered on, files are registered for monitoring on ONTAP. The historical metrics for Latency, Throughput and IOPS are obtained when VM reports are accessed from ONTAP.

vVols reports

vVols reports display detailed information about VMware Virtual Volumes (vVols) datastores and the virtual machines that are created on these datastores. The vVols dashboard enables you to review and identify potential issues with the vVols datastores and virtual machines in your vCenter Server.

You can view, organize, and export reports. The data for the vVols datastores and virtual machines report is provided by the ONTAP along with OnCommand API Services.

vVols provides the following pre-canned reports:

* vVols Datastore Report
* vVols VM Report

vVols Datastore Report

The vVols Datastore Report menu provides information about the following parameters for datastores:

* vVols datastore name
* Free space
* Used space
* Total space
* Percentage of space utilized
* Percentage of space available
* IOPS
* Latency
  Performance metrics are available for NFS based vVols datastores on ONTAP 9.8 and later. You can also verify the time at which the report was generated. The vVols Datastore Report menu enables you to organize the report as per your requirement, and then export the organized report by using the **Export to CSV** button. Each SAN vVols datastore name in the report is a link that navigates to the Monitor tab of the selected SAN vVols datastore, which you can use to view the performance metrics.

vVols Virtual Machine Report

The vVols Virtual Machine Summary Report menu provides the performance metrics for all of the virtual machines that use the SAN vVols datastores that are provisioned by VASA Provider for ONTAP for a selected vCenter Server. The virtual machine metrics displayed in VM reports is historical data that is collected every 10 minutes for virtual machines on vVols datastores. "Last refresh time" and "Next refresh time" are added to the table to provide information on when data was collected and when will be the next data collection.

- Name of the virtual machine

- Committed capacity

- Uptime

- IOPS

- Throughput

  The report displays whether the virtual machine is powered on or powered off.

- Logical space

- Host

- Power state

- Latency

  The report displays the latency for virtual machines across all of the vVols datastores that are associated with the virtual machines.

Each virtual machine name in the report is a link to the Monitor tab of the selected virtual machine. You can organize the virtual machine report according to your requirement, export the report in `.csv` format, and then save the report on your local system. The timestamp of the report is appended to the saved report.

Analyze performance data using the traditional dashboard

You can monitor the traditional datastores and virtual machines using the traditional dashboard of the ONTAP tools. The dashboard data enables you to analyze the datastore usage and to take corrective action to prevent the virtual machines from running into space-related constraints.

What you will need

You should select either the **Enable Storage I/O Control and statistics collection** or **Disable Storage I/O Control but enable statistics collection** option in the Configure Storage I/O Control dialog box. You can enable Storage I/O Control only if you have the Enterprise Plus license from VMware.

VMware vSphere Documentation: Enable Storage I/O Control

The traditional dashboard displays IOPS, space utilized, latency, and committed capacity metrics that are obtained from your vCenter Server. ONTAP provides aggregate space saving metrics to the traditional dashboard. You can view space saving for a specific aggregate. These performance parameters enable you to identify performance bottlenecks in the virtual environment and to take corrective action to resolve the issues.

> (i) File monitoring is not supported for FlexGroup datastores configured on direct storage virtual machines (SVMs).

The traditional dashboard of the ONTAP tools enables you to view either NFS datastores or VMFS datastores. You can click a datastore to navigate to the datastore details view that is provided by the vCenter Server instance to view and fix any issues with the datastores in your vCenter Server.

Steps

1. From the vSphere Client home page, click **ONTAP tools for VMware vSphere**.

2. Select the required vCenter Server using the vCenter Server drop-down menu to view the datastores.

3. Click **Traditional Dashboard**.

   The Datastores portlet provides the following details:

   - The number of traditional datastores along with their performance metrics that are managed by VSC in your vCenter Server instance

   - The top five datastores based on resource usage and performance parameters that can be modified, if required
     You can change the listing of the datastores based on the space utilized, IOPS, or latency and in the order required.

   The Virtual Machines portlet provides the following details:

   - Number of virtual machines using NetApp datastores in your vCenter Server

   - Top five virtual machines based on committed capacity, latency, IOPS, throughput, and uptime

     The IOPS and throughput data in the Virtual Machines portlet is available only for datastores created on FlexGroup backed volumes.

Analyze performance data using the vVols dashboard

You can monitor the performance and view the top five SAN and NAS VMware Virtual Volumes (vVols) datastores in your vCenter Server based on the parameters that you select by using the vVols dashboard of the ONTAP tools.

What you will need

- You should have enabled OnCommand API Services 2.1 or later if you are using ONTAP 9.6 or earlier.

  You do not require to register OnCommand API Services with VASA Provider to get the details of SAN vVols datastore or SAN vVols VM datastore report for ONTAP 9.7 or later.

  https://mysupport.netapp.com/site/global/dashboard

- You should be using ONTAP 9.3 or later for your storage system.

The IOPS data that is provided by ONTAP is rounded off and displayed on the vVols dashboard. There might be a difference between the actual IOPS value that is provided by ONTAP and the IOPS value that is displayed on the vVols dashboard. ONTAP tools provides performance monitoring for NFS based vVols datastores.

> (i) If you are registering OnCommand API Services for the first time, then you can view all of the performance metrics data for SAN vVols datastores on the vVols dashboard only after 15 to 30 minutes.

- The vVols dashboard data is refreshed periodically, at an interval of 10 minutes.

- If you have added, modified, or deleted a storage system from your vCenter Server instance, then you might not notice any change in the data on the vVols dashboard for some time.

  This is because OnCommand API Services takes time to obtain updated metrics from ONTAP.

- The Total IOPS value that is displayed in the Overview portlet of the vVols dashboard is not a cumulative value of the Read IOPS value and Write IOPS value.

  Read IOPS, Write IOPS, and Total IOPS are separate metrics that are provided by OnCommand API Services. If there is a difference between the Total IOPS value and the cumulative IOPS value (Read IOPS value + Write IOPS value) provided by OnCommand API Services, then the same difference is observed in the IOPS values on the vVols dashboard.

- NFS based data vVols provisioned on ONTAP 9.8 and above are automatically registered for performance monitoring in the vVols dashboard.

Steps

1. From the vSphere Client home page, click **ONTAP tools**.
2. Select the required vCenter Server using the **vCenter server** drop-down menu to view the datastores.
3. Click **vVols Dashboard**.

   The Datastores portlet provides the following details:

   ◦ The number of vVols datastores that are managed by VASA Provider in your vCenter Server instance

   ◦ The top five vVols datastores based on resource usage and performance parameters
   You can change the listing of the datastores based on the space utilized, IOPS, or latency and in the order required.

4. View the details of the virtual machines using the Virtual Machines portlet.

   The Virtual Machines portlet provides the following details:

   ◦ Number of virtual machines using ONTAP datastores in your vCenter Server

   ◦ Top five virtual machines based on IOPS, latency, throughput, committed capacity, uptime, and logical space
   You can customize how the top five virtual machines are listed in the vVols dashboard.

vVols dashboard data requirements

You must verify some important requirements of the vVols dashboard to display dynamic details of the VMware Virtual Volumes (vVols) datastores and virtual machines.

The following table presents an overview of what you should verify if the vVols dashboard does not display the performance metrics for the provisioned SAN vVols datastores and virtual machines.

Considerations	Description

First-time deployment of OnCommand API Services	• If you are having ONTAP clusters 9.6 or earlier, then you are using OnCommand API Services 2.1 or later.
	You do not require OnCommand API Services to be registered with VASA Provider if you are using ONTAP 9.7 and later.
	• You must have followed the installation instructions that are provided in the *OnCommand API Services Installation and Setup guide* after downloading and installing OnCommand API Services from the NetApp Support Site.
	• Each VASA Provider instance must have a dedicated OnCommand API Services instance.
	OnCommand API Services must not be shared among multiple VASA Provider instances or vCenter Servers.
	• OnCommand API Services is running and accessible.
Storage system	• You are using ONTAP 9.3 or later.
	• You are using appropriate credentials for the storage system.
	• Your storage system is active and accessible.
	• The virtual machine that you selected must be using at least one vVols datastore, and I/O operations are executing on the disk of the virtual machine.

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/

Notice for ONTAP tools for VMware vSphere 9.11