Concepts

ONTAP tools for VMware vSphere

NetApp
December 02, 2021

Table of Contents

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

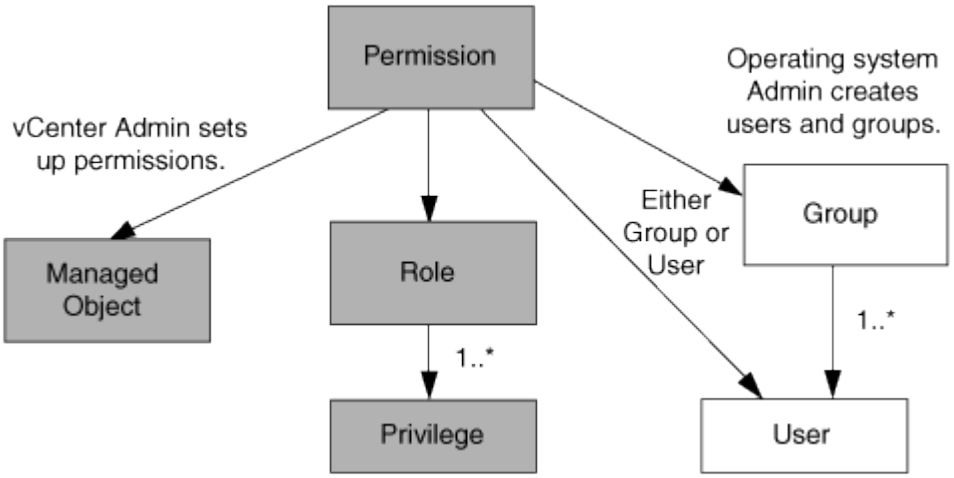
  The object is the target for the tasks.

- 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.

> 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.

How to configure RBAC for Virtual Storage Console

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 9.7 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

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

  - ONTAP System Manager 9.8

    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.