Concepts

ONTAP tools for VMware vSphere 10.0

NetApp
October 23, 2024

Table of Contents

Concepts

ONTAP tools Overview

The ONTAP tools for VMware vSphere manages provisioning of datastores and virtual-machines in VMware environments that use NetApp storage backends. It enables the administrators to manage the storage within the vCenter Server directly and hence simplifies the storage and data management for VMware environments.

ONTAP tools for VMware vSphere 10.0 release is a collection of horizontally scalable, event driven, microservices deployed as an Open Virtual Appliance (OVA). It is packaged in various deployment form factors like Open Virtual Appliance (OVA) and Software as a service (SaaS) for on-prem.

ONTAP tools for VMware vSphere consists of:

- Virtual machine functionality
- VASA Provider for VM granular
- Storage policy-based management

ONTAP tools VASA Provider

ONTAP tools VASA provider supports high scale requirements for Virtual volumes (vVols). It supports NFS protocol, iSCSI protocol, and OVA deployment. VASA Provider for VMware is a product that provides lifecycle management in a VMware deployment with ONTAP.

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.

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 or iSCSI) and the same storage virtual machines (SVMs).

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. Adding diverse volumes increases the datastore capabilities where there could be a mix of thin and thick volumes so that both kind of VMs can be created on the datastore.

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

- **Config**

VMware vSphere uses this vVols datastore to store configuration information.

In SAN (block) implementations, the storage is a 4 GB LUN. vCenter 8 takes the capacity to 256GB LUN in Thin provisioning.

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.

- **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.

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. vCenter Server provides centralized authentication and authorization services at many different levels within its inventory, using user and group rights with roles and privileges. vCenter Server features five main components for managing RBAC:

Components	Description
Privileges	A privilege enables or denies access to perform actions in vSphere.
Roles	A role contains one or more system privileges where each privilege defines an administrative right to a certain object or type of object in the system. By assigning a user a role, the user inherits the capabilities of the privileges defined in that role.

Users and groups	Users and groups are used in permissions to assign roles from Active Directory (AD) or potentially local windows users/groups as well (not recommended)
Permissions	Permissions allow you to assign privileges to users or groups to perform certain actions and make changes to objects inside vCenter Server. vCenter Server permissions affect only those users who log into vCenter Server rather than users who log into an ESXi host directly.
Object	An entity upon which actions are performed. VMware vCenter objects are data centers, folders, resource pools, clusters, hosts, and VMs

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

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

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

Key points about assigning and modifying roles for vCenter Server

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

Where you assign a role determines the ONTAP tools tasks that a user can perform. You can modify one role at any time. If you change the privileges within a role, the user associated with that role should log out and then log back in to enable the updated role.

Standard roles packaged with ONTAP tools

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

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

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

NetApp ONTAP tools Provision	Provides some of the native vCenter Server privileges and ONTAP tools-specific privileges that are required to provision storage. You can perform the following tasks: • Create new datastores • Manage datastores

The Manager UI admin role is not registered with vCenter. This role is specific to the manager UI.

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

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

Permissions for ONTAP storage backends and vSphere objects

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

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 ONTAP tools tasks.

To create new user roles, you must log in as an administrator on storage systems running ONTAP. You can create ONTAP roles using ONTAP System Manager 9.8P1 or later. See List of minimum privileges required for non-admin global scoped cluster user for more information.

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 ONTAP tools-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 ONTAP tools 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 ONTAP tools. 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.

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

  Only single node failure is supported.

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

No additional configuration is required for ONTAP tools 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.

vCenter HA is not supported by ONTAP tools.

AutoSupport

AutoSupport is a mechanism that proactively monitors the health of your system and

automatically sends messages to NetApp technical support, your internal support organization, and a support partner.

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

You can enable or disable AutoSupport only at the time of deployment. It is recommended to leave it enabled. Enabling AutoSupport can significantly help speed problem determination and resolution should a problem occur on your storage system. By default, the system collects AutoSupport information and stores it locally, even if you disable AutoSupport. You need to whitelist 216.240.21.18 // support.netapp.com URL in your network for successful transmission.

Copyright information

Trademark information