Role based access control

ONTAP tools for VMware vSphere 9.13

NetApp
June 19, 2024

Table of Contents

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 ONTAP tools 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, ONTAP tools 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

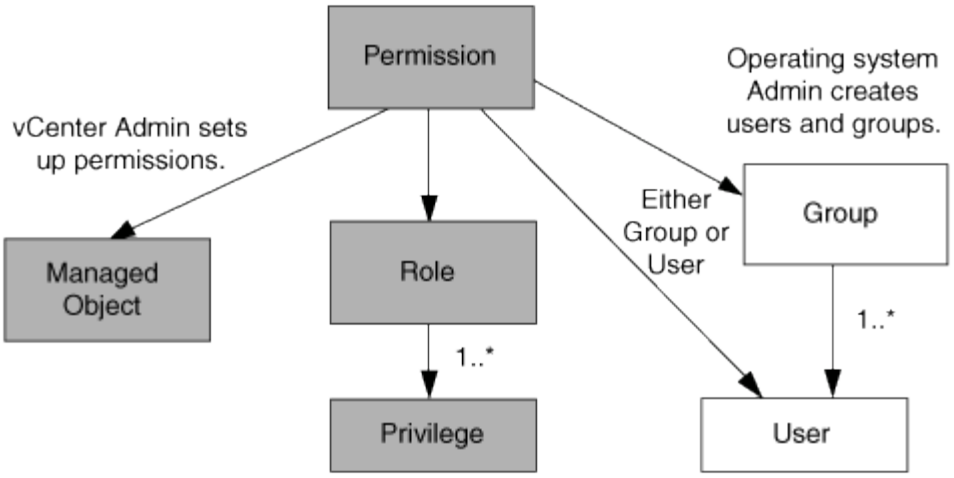
  The object is the target for the tasks.

- 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.

- ONTAP tools-specific privileges

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

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

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

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

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

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 ONTAP tools 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 ONTAP tools 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 ONTAP tools 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), 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.

The standard ONTAP tools roles have both the required ONTAP tools-specific privileges and the native vCenter Server privileges that are required for users to perform ONTAP tools 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 ONTAP tools to the latest version, the standard roles are automatically upgraded to work with the new version of the tool.

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

VSC Provision	Provides all 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 • Destroy datastores • View information about storage capability profiles

Guidelines for using ONTAP tools 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, ONTAP tools will overwrite your changes each time you upgrade. The installer updates the standard role definitions each time you upgrade ONTAP tools. Doing this ensures that the roles are current for your version of ONTAP tools for VMware vSphere 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 ONTAP tools 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 ONTAP tools Windows service.

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

- Use the standard ONTAP tools roles for all ONTAP tools tasks.

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

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

  If the standard ONTAP tools 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-ONTAP tools 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 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.

Privileges required for ONTAP tools tasks

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

Information about the privileges required for ONTAP tools 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, ONTAP tools-specific View privilege assigned at the correct vSphere object level. If you log in without this privilege, ONTAP tools displays an error message when you click the NetApp icon and prevents you from accessing ONTAP tools.

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

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

You can assign the View privilege to another vSphere object level; however, doing that limits the ONTAP tools 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 ONTAP tools tasks a specific user can perform on the objects on a specific storage system.

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

ONTAP RBAC applies only to accessing storage systems and performing ONTAP tools 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 ONTAP tools-specific privileges to control which ONTAP tools 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 ONTAP tools-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 ONTAP tools task, ONTAP tools 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, ONTAP tools 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, ONTAP tools 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 ONTAP tools task on that storage system. If you have the correct ONTAP privileges, you can access the storage system and perform the ONTAP tools task. The ONTAP roles determine the ONTAP tools 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, ONTAP tools provide 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 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 Configure user roles and privileges 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.

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.

ONTAP tools for VMware vSphere 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 ONTAP tools for VMware vSphere at the cluster level even if you are using ONTAP tools 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 using ONTAP System Manager 9.8P1 or later. See Configure user roles and privileges for more information.
- 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 ONTAP tools. You can configure storage systems for ONTAP tools by entering the credentials in ONTAP tools. Each time you log in to a storage system with these credentials, you will have permissions to the ONTAP tools functions that

you had set up in ONTAP while creating the credentials.

- Add the storage system to ONTAP tools for VMware vSphere and provide the credentials of the user that you just created

ONTAP tools roles

ONTAP tools classifies the ONTAP privileges into the following set of ONTAP tools 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.

ONTAP tools perform an initial privilege validation of ONTAP RBAC roles when you add the cluster to ONTAP tools. If you have added a SVM user storage IP, then ONTAP tools does not perform the initial validation. ONTAP tools checks and enforces the privileges later in the task workflow.

Copyright information

Trademark information