Role based access control

ONTAP tools for VMware vSphere 10.1

NetApp
June 21, 2024

Table of Contents

Role based access control

Overview of role-based access control in ONTAP tools for VMware vSphere

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). vCenter Server has its own local users and groups that you can use.
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 should have the appropriate vCenter Server RBAC roles. During a task, ONTAP tools for VMware vSphere checks a user's vCenter Server roles before checking the user's ONTAP privileges.

> The vCenter Server roles apply to ONTAP tools for VMware vSphere 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 ONTAP tools for VMware vSphere 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 for VMware vSphere

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

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

Role	Description
NetApp ONTAP tools for VMware vSphere Administrator	Provides all the native vCenter Server privileges and ONTAP tools-specific privileges that are required to perform some of ONTAP tools for VMware vSphere tasks.
NetApp ONTAP tools for VMware vSphere Read Only	Provides read-only access to ONTAP tools. These users cannot perform any ONTAP tools for VMware vSphere actions that are access-controlled.
NetApp ONTAP tools for VMware vSphere provision	Provides some of the native vCenter Server privileges and ONTAP tools-specific privileges that are required to provision storage. You can perform the following tasks: • Create new datastores • Manage datastores

The ONTAP tools Manager admin role is not registered with vCenter Server. This role is specific to the ONTAP tools Manager.

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

In this case, you would clone the necessary ONTAP tools for VMware vSphere 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 for VMware vSphere then checks the ONTAP RBAC privileges (your ONTAP role) that are associated with the storage backends credentials (the username and password) to determine whether you have sufficient privileges to perform the storage operations that are required by that ONTAP tools for VMware vSphere task on that storage backend. If you have the correct ONTAP privileges, you can access the storage backends and perform ONTAP tools for VMware vSphere tasks. The ONTAP roles determine ONTAP tools for VMware vSphere tasks that you can perform on the storage backend.

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.

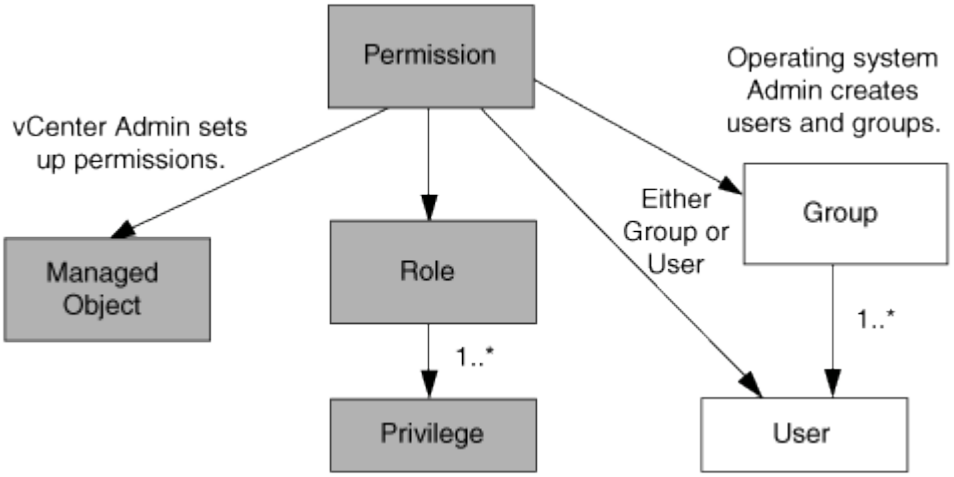
- A vSphere object

  The object is the target for the tasks.

- A user or group

  The user or group defines who can perform the task.

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 for VMware vSphere tasks. They are unique to ONTAP tools for VMware vSphere.

ONTAP tools for VMware vSphere 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 for VMware vSphere provides several standard roles that contain all ONTAP tools-specific and native privileges that are required to perform ONTAP tools for VMware vSphere 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.

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 for VMware vSphere specific tasks, permissions are assigned and validated only at the root-folder level (vCenter Server) and not on any other entity. Except for VAAI plug-in operation, where permissions are validated against the concerned ESXi host.

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 for VMware vSphere tasks.

> These vCenter Server permissions apply to ONTAP tools for VMware vSphere 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.

Assign and modify 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 permission determines ONTAP tools for VMware vSphere tasks that a user can perform.

Sometimes, to ensure the completion of a task, you should assign 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 you can give permissions to a child entity to restrict the scope of a permission 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 is 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 should assign the permission containing that privilege to ONTAP tools for VMware vSphere root object because there is no vSphere object to which you can assign it.

For example, any permission that includes a privilege such as ONTAP tools for VMware vSphere privilege "Add/Modify/Skip storage systems" should 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.

Privileges required for ONTAP tools for VMware vSphere 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.

To access ONTAP tools for VMware vSphere GUI, you should 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 for VMware vSphere displays an error message when you click the NetApp icon and prevents you from accessing ONTAP tools.

In **View** privilege, you can access ONTAP tools for VMware vSphere. This privilege does not enable you to perform tasks within ONTAP tools for VMware vSphere. To perform any ONTAP tools for VMware vSphere tasks, you should 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 to the root object (folder) enables you to enter ONTAP tools for VMware vSphere by clicking the NetApp icon.

You can assign the View privilege to another vSphere object level; however, doing that limits ONTAP tools for VMware vSphere menus that you can see and use.

The root object is the recommended place to assign any permission containing the View privilege.

Recommended ONTAP roles for 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 required to perform the storage operations executed by ONTAP tools for VMware vSphere tasks.

To create new user roles, you should log in as an administrator of the storage systems running ONTAP. You can create ONTAP roles using ONTAP System Manager 9.8P1 or later.

Each ONTAP role has an associated username 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, ONTAP tools for VMware vSphere specific ONTAP roles are ordered hierarchically. This means the first role is the most restrictive and has only the privileges associated with the most basic set of ONTAP tools for VMware vSphere storage operations. The next role includes its own privileges and all the privileges associated with the previous role. Each additional role is less restrictive regarding the supported storage operations.

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

Role	**privileges**
Discovery	This role enables you to add storage systems.
Create Storage	This role enables you to create storage. This role also includes all the privileges that are associated with the Discovery role.
Modify Storage	This role enables you to modify storage. This role also includes all the privileges that are associated with the Discovery role and the Create Storage role.
Destroy Storage	This role enables you to destroy storage. This role also includes all the privileges that are associated with the Discovery role, the Create Storage role, and the Modify Storage role.

If you are using ONTAP tools for VMware vSphere, 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.

Copyright information

Trademark information