Role based access control

ONTAP tools for VMware vSphere 10

NetApp
August 25, 2025

Table of Contents

Role based access control

Learn about ONTAP tools for VMware vSphere 10 RBAC

Role-based access control (RBAC) is a security framework for controlling access to resources within an organization. RBAC simplifies administration by defining roles with specific levels of authority to perform actions, instead of assigning authorization to individual users. The defined roles are assigned to users, which helps reduce risk of error and simplifies management of access control across your organization.

The RBAC standard model consists of several implementation technologies or phases of increasing complexity. The result is that actual RBAC deployments, based on the needs of the software vendors and their customers, can differ and range from relatively simple to very complex.

RBAC components

At a high level, there are several components which are generally included with every RBAC implementation. These components are bound together in different ways as part of defining the authorization processes.

Privileges

A *privilege* is an action or capability that can be allowed or denied. It might be something simple such as the ability to read a file or it could be a more abstract operation specific to a given software system. Privileges can also be defined to restrict access to REST API endpoints and CLI commands. Every RBAC implementation includes pre-defined privileges and might also allow administrators to create custom privileges.

Roles

A *role* is a container that includes one or more privileges. Roles are generally defined based on particular tasks or job functions. When a role is assigned to a user, the user is granted all the privileges contained in the role. And as with privileges, implementations include pre-defined roles and generally allow custom roles to be created.

Objects

An *object* represents a real or abstract resource identified within the RBAC environment. The actions defined through the privileges are performed on or with the associated objects. Depending on the implementation, privileges can be granted to an object type or a specific object instance.

Users and groups

Users are assigned or associated with a role applied after authentication. Some RBAC implementations allow only one role to be assigned to a user while others allow multiple roles per user, perhaps with only one role active at a time. Assigning roles to *groups* can further simplify security administration.

Permissions

A *permission* is a definition that binds a user or group along with a role to an object. Permissions can be useful with a hierarchical object model where they can optionally be inherited by the children in the hierarchy.

Two RBAC environments

There are two distinct RBAC environments you need to consider when working with ONTAP tools for VMware vSphere 10.

VMware vCenter Server

The RBAC implementation in VMware vCenter Server is used to restrict access to objects exposed through the vSphere Client user interface. As part of installing ONTAP tools for VMware vSphere 10, the RBAC environment is extended to include additional objects representing the capabilities of ONTAP tools. Access to these objects is provided through the remote plug-in. See vCenter Server RBAC environment for more information.

ONTAP cluster

ONTAP tools for VMware vSphere 10 connects to an ONTAP cluster through the ONTAP REST API to perform storage related operations. Access to the storage resources is controlled through an ONTAP role associated with the ONTAP user provided during authentication. See ONTAP RBAC environment for more information.

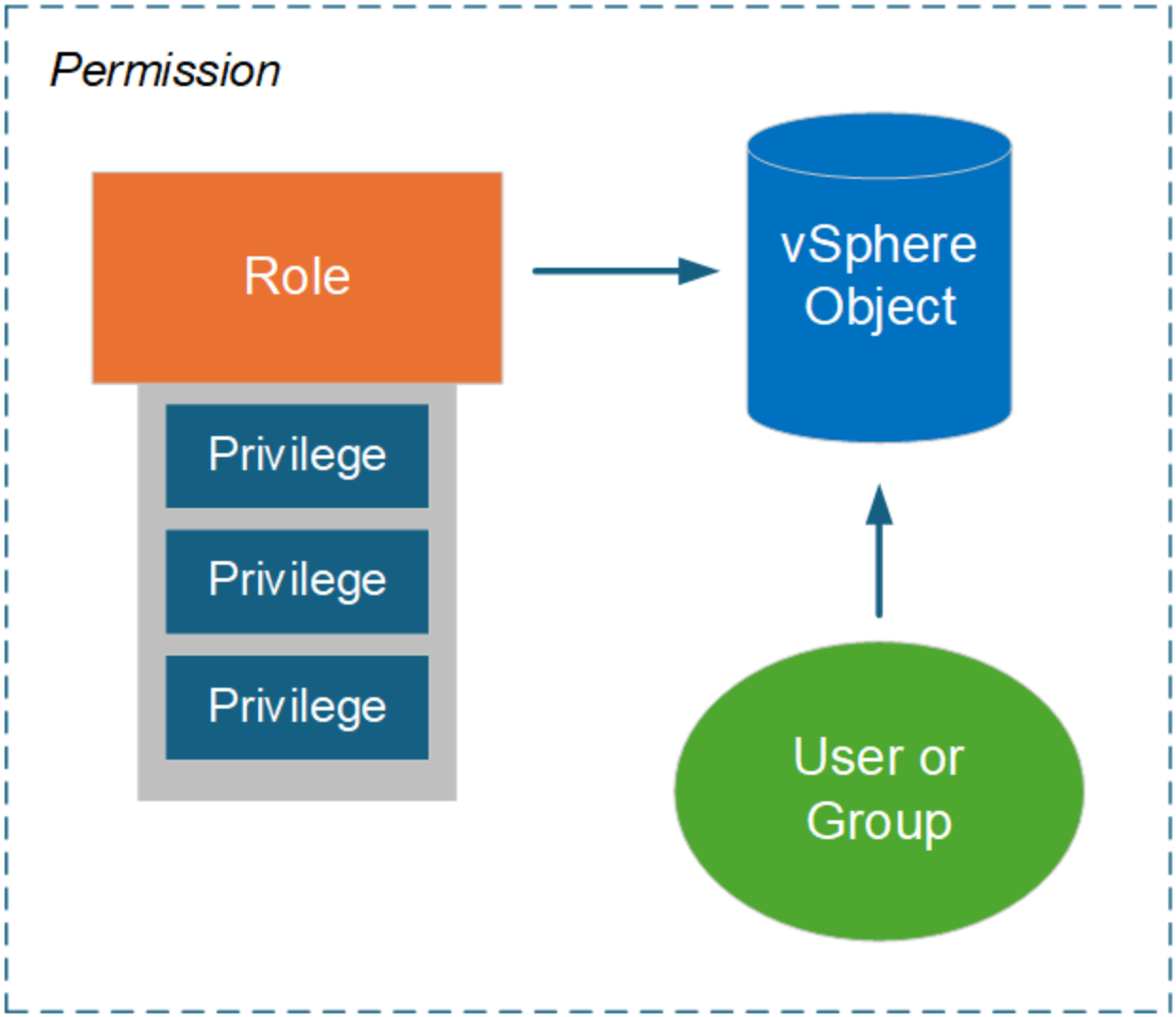
RBAC with VMware vSphere

vCenter Server RBAC environment with ONTAP tools for VMware vSphere 10

VMware vCenter Server provides an RBAC capability that enables you to control access to vSphere objects. It is an important part of the vCenter centralized authentication and authorization security services.

Illustration of a vCenter Server permission

A permission is the foundation for enforcing access control in the vCenter Server environment. It's applied to a vSphere object with a user or group included with the permission definition. A high-level illustration of a vCenter permission is provided in the figure below.



Components of a vCenter Server permission

A vCenter Server permission is a package of several components that are bound together when the permission is created.

vSphere objects

Permissions are associated with vSphere objects, such as the vCenter Server, ESXi hosts, virtual machines, datastores, data centers, and folders. Based on the object's assigned permissions, vCenter Server determines which actions or tasks can be performed on the object by each user or group. For the tasks specific to ONTAP tools for VMware vSphere, all permissions are assigned and validated at the root or root folder level of vCenter Server. See Use RBAC with vCenter server for more information.

Privileges and roles

There are two types of vSphere privileges used with ONTAP tools for VMware vSphere 10. To simplify working with RBAC in this environment, ONTAP tools provides roles containing the required native and custom privileges. The privileges include:

- Native vCenter Server privileges

  These are the privileges provided by vCenter Server.

- ONTAP tools-specific privileges

  These are custom privileges unique to ONTAP tools for VMware vSphere.

Users and groups

You can define users and groups using Active Directory or the local vCenter Server instance. Combined with a role, you can create a permission on an object in the vSphere object hierarchy. The permission grants access based on the privileges in the associated role. Note that roles aren't assigned directly to users in isolation. Instead, users and groups gain access to an object through role privileges as part of the larger vCenter Server permission.

Use vCenter Server RBAC with ONTAP tools for VMware vSphere 10

There are several aspects of the ONTAP tools for VMware vSphere 10 RBAC implementation with vCenter Server you should consider before using it in a production environment.

vCenter roles and the administrator account

You only need to define and use the custom vCenter Server roles if you want to limit access to the vSphere objects and associated administrative tasks. If limiting access is not required, you can use an administrator account instead. Each administrator account is defined with the Administrator role at the top level of the object hierarchy. This provides full access to the vSphere objects, including those added by ONTAP tools for VMware vSphere 10.

vSphere object hierarchy

The vSphere object inventory is organized in a hierarchy. For example, you can move down the hierarchy as follows:

`vCenter Server` --> `Datacenter` --> `Cluster` --> `ESXi host` --> `Virtual Machine`

All permissions are validated in the vSphere object hierarchy except the VAAI plug-in operations, which are validated against the target ESXi host.

Roles included with ONTAP tools for VMware vSphere 10

To simplify working with vCenter Server RBAC, ONTAP tools for VMware vSphere provides predefined roles tailored to various administration tasks.

> ⓘ You can create new custom roles if needed. In this case, you should clone one of the existing ONTAP tools roles and edit it as needed. After making the configuration changes, the affected vSphere client users need to log out and log back in to activate the changes.

To view the ONTAP tools for VMware vSphere roles, select **Menu** at the top of the vSphere Client and click **Administration** and then **Roles** on the left. There are three predefined roles as described below.

NetApp ONTAP tools for VMware vSphere Administrator

Provides all the native vCenter Server privileges and ONTAP tools-specific privileges required to perform core ONTAP tools for VMware vSphere administrator 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

vSphere objects and ONTAP storage backends

The two RBAC environments work together. When performing a task in the vSphere client interface, the ONTAP tools roles defined to vCenter Server are checked first. If the operation is permitted by vSphere, then the ONTAP role privileges are examined. This second step is performed based on the ONTAP role assigned to the user when the storage backend was created and configured.

Working with vCenter Server RBAC

There are a few things to consider when working with the vCenter Server privileges and permissions.

Required privileges

To access the ONTAP tools for VMware vSphere 10 user interface, you need to have the ONTAP tools-specific *View* privilege. If you sign in to vSphere without this privilege and click the NetApp icon, ONTAP tools for VMware vSphere displays an error message and prevents you from accessing the user interface.

The assignment level in the vSphere object hierarchy determines which portions of the user interface you can access. Assigning the View privilege to the root object enables you to access ONTAP tools for VMware vSphere by clicking the NetApp icon.

You can instead assign the View privilege to another lower vSphere object level. However, this will limit the ONTAP tools for VMware vSphere menus that you can access and use.

Assigning permissions

You need to use vCenter Server permissions if you want to limit access to the vSphere objects and tasks. Where you assign permission in the vSphere object hierarchy determines the ONTAP tools for VMware vSphere 10 tasks users can perform.

Unless you need to define more restrictive access, it’s generally a good practice to assign permissions at the root object or root folder level.

The permissions available with ONTAP tools for VMware vSphere 10 apply to custom non-vSphere objects, such as storage systems. If possible, you should assign these permissions to ONTAP tools for VMware vSphere root object because there is no vSphere object you can assign it to. For example, any permission that includes an ONTAP tools for VMware vSphere "Add/Modify/Remove storage systems" privilege should be assigned at the root object level.

When defining a permission at a higher level in the object hierarchy, you can configure the permission so it is passed down and inherited by the child objects. If needed you can assign additional permissions to the child objects that override the permissions inherited from the parent.

You can modify a permission at any time. If you change any of the privileges within a permission, users associated with the permission need to log out of vSphere and log back in to enable the change.

RBAC with ONTAP

ONTAP RBAC environment with ONTAP tools for VMware vSphere 10

ONTAP provides a robust and extensible RBAC environment. You can use the RBAC capability to control access to the storage and system operations as exposed through the REST API and CLI. It's helpful to be familiar with the environment before using it with an ONTAP tools for VMware vSphere 10 deployment.

Overview of the administrative options

There are several options available when using ONTAP RBAC depending on your environment and goals. An overview of the major administrative decisions is presented below. Also see ONTAP Automation: Overview of RBAC security for more information.

> ONTAP RBAC is tailored to a storage environment and is simpler than the RBAC implementation provided with vCenter Server. With ONTAP, you assign a role directly to the user. Configuring explicit permissions, such as those used with vCenter Server, are not needed with ONTAP RBAC.

Types of roles and privileges

An ONTAP role is required when defining an ONTAP user. There are two types of ONTAP roles:

- REST

  The REST roles were introduced with ONTAP 9.6 and are generally applied to users accessing ONTAP through the REST API. The privileges included in these roles are defined in terms of access to the ONTAP REST API endpoints and the associated actions.

- Traditional

  These are the legacy roles included prior to ONTAP 9.6. They continue to be a foundational aspect of RBAC. The privileges are defined in terms of access to the ONTAP CLI commands.

While the REST roles were introduced more recently, the traditional roles have some advantages. For example, additional query parameters can optionally be included so the privileges more precisely define the objects they are applied to.

Scope

ONTAP roles can be defined with one of two different scopes. They can be applied to a specific data SVM (SVM level) or to the entire ONTAP cluster (cluster level).

Role definitions

ONTAP provides a set of pre-defined roles at both the cluster and SVM level. You can also define custom

roles.

Working with ONTAP REST roles

There are several considerations when using the ONTAP REST roles included with ONTAP tools for VMware vSphere 10.

Role mapping

Whether using a traditional or REST role, all ONTAP access decisions are made based on the underlying CLI command. But because the privileges in a REST role are defined in terms of the REST API endpoints, ONTAP needs to create a *mapped* traditional role for each of the REST roles. Therefore each REST role maps to an underlying traditional role. This allows ONTAP to make access control decisions in a consistent way regardless of the role type. You cannot modify the parallel mapped roles.

Defining a REST role using CLI privileges

Because ONTAP always uses the CLI commands to determine access at a base level, it's possible to express a REST role using CLI command privileges instead of REST endpoints. One benefit of this approach is the additional granularity available with the traditional roles.

Administrative interface when defining ONTAP roles

You can create users and roles with the ONTAP CLI and REST API. However, it's more convenient to use the System Manager interface along with the JSON file available through the ONTAP tools Manager. See Use ONTAP RBAC with ONTAP tools for VMware vSphere 10 for more information.

Use ONTAP RBAC with ONTAP tools for VMware vSphere 10

There are several aspects of the ONTAP tools for VMware vSphere 10 RBAC implementation with ONTAP you should consider before using it in a production environment.

Overview of the configuration process

ONTAP tools for VMware vSphere 10 includes support for creating an ONTAP user with a custom role. The definitions are packaged in a JSON file that you can upload to the ONTAP cluster. You can create the user and tailor the role for your environment and security needs.

The major configuration steps are described at a high level below. Refer to Configure ONTAP user roles and privileges for more details.

1. Prepare

You need to have administrative credentials for both the ONTAP tools Manager and the ONTAP cluster.

2. Download the JSON definition file

After signing in to the ONTAP tools Manager user interface, you can download the JSON file containing the RBAC definitions.

3. Create an ONTAP user with a role

After signing in to System Manager, you can create the user and role:

a. Select **Cluster** on the left and then **Settings**.

b. Scroll down to **Users and roles** and click −→.

c. Select **Add** under **Users** and select **Virtualization products**.

d. Select the JSON file on your local workstation and upload it.

4. Configure the role

As part of defining the role, you need to make several administrative decisions. See Configure the role using System Manager for more details.

Configure the role using System Manager

After you begin creating a new user and role with System Manager and you have uploaded the JSON file, you can customize the role based on your environment and needs.

Core user and role configuration

The RBAC definitions are packaged as several product capabilities, including combinations of VSC, VASA Provider, and SRA. You should select the environment or environments where you need RBAC support. For example, if you want roles to support the remote plug-in capability, select VSC. You also need to choose the user name and associated password.

Privileges

The role privileges are arranged in four sets based on the level of access needed to the ONTAP storage. The privileges which the roles are based on include:

- Discovery

  This role enables you to add storage systems.

- Create storage

  This role enables you to create storage. It also includes all the privileges associated with the discovery role.

- Modify storage

  This role enables you to modify storage. It also includes all the privileges associated with the discovery and create storage roles.

- Destroy storage

  This role enables you to destroy storage. It also includes all the privileges associated with the discovery, create storage, and modify storage roles.

Generate the user with a role

After you've selected the configuration options for your environment, click **Add** and ONTAP creates the user and role. The name of the generated role is a concatenation of the following values:

- Constant prefix value defined in the JSON file (for example "OTV_10")
- Product capability you selected
- List of the privilege sets.

Example

```
OTV_10_VSC_Discovery_Create
```

The new user will be added to the list on the page "Users and roles". Note that both HTTP and ONTAPI user login methods are supported.

Copyright information

Trademark information