RBAC with ONTAP

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Table of Contents

RBAC with ONTAP . . . 1
- How ONTAP RBAC works with ONTAP tools . . . 1
  - Overview of the administrative options . . . 1
  - Working with ONTAP REST roles . . . 1
- ONTAP RBAC considerations for ONTAP tools . . . 2
  - Overview of the configuration process . . . 2
  - Configure the role using System Manager . . . 3

RBAC with ONTAP

How ONTAP RBAC works with ONTAP tools

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, aren't 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 that existed 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 offer some advantages. For example, additional query parameters can be included to let privileges more precisely define the objects to which they apply.

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.

ONTAP RBAC considerations for ONTAP tools

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 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 for 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 'Users and roles' page. Note that both HTTP and ONTAPI user login methods are supported.

Copyright information

Trademark information