# Privileges required for VSC tasks

## VSC, VASA Provider, and SRA 9.7

NetApp
June 11, 2024

# Table of Contents

# Privileges required for VSC tasks

Different Virtual Storage Console for VMware vSphere tasks require different combinations of privileges specific to (VSC) and native vCenter Server privileges.

Information about the privileges required for VSC tasks is available in the NetApp Knowledgebase article 1032542.

How to configure RBAC for Virtual Storage Console

## Product-level privilege required by VSC for VMware vSphere

To access the Virtual Storage Console for VMware vSphere GUI, you must have the product-level, VSC-specific View privilege assigned at the correct vSphere object level. If you log in without this privilege, VSC displays an error message when you click the NetApp icon and prevents you from accessing VSC.

The following information describes the VSC product-level View privilege:

| Privilege | Description | Assignment level |
|---|---|---|
| View | You can access the VSC GUI. This privilege does not enable you to perform tasks within VSC. To perform any VSC tasks, you must have the correct VSC-specific and native vCenter Server privileges for those tasks. | The assignment level determines which portions of the UI you can see.<br><br>Assigning the View privilege at the root object (folder) enables you to enter VSC by clicking the NetApp icon.<br><br>You can assign the View privilege to another vSphere object level; however, doing that limits the VSC menus that you can see and use.<br><br>The root object is the recommended place to assign any permission containing the View privilege. |

## ONTAP role-based access control for the virtual appliance for VSC, VASA Provider, and SRA

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 Virtual Storage Console for VMware vSphere, ONTAP RBAC works with vCenter Server RBAC to determine which Virtual Storage Console (VSC) tasks a specific

user can perform on the objects on a specific storage system.

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

ONTAP RBAC applies only to accessing storage systems and performing VSC 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 VSC-specific privileges to control which VSC 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 VSC-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 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 VSC task, VSC 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, VSC 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, VSC 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 VSC task on that storage system. If you have the correct ONTAP privileges, you can access the storage system and perform the VSC task. The ONTAP roles determine the VSC 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, VSC provides 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 VSC for VMware vSphere

You can set up several recommended ONTAP roles for working with Virtual Storage Console 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 (VSC) tasks.

To create new user roles, you must log in as an administrator on storage systems running ONTAP. You can create ONTAP roles using one of the following:

- 9.7 or later

  Configure user roles and privileges

- RBAC User Creator for ONTAP tool (if using ONTAP 9.6 or earlier)

  RBAC User Creator tool for VSC, VASA Provider and Storage Replication Adapter 7.0 for VMware vSphere

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 VSC-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 VSC 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 VSC. 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 VSC 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 Virtual Storage Console for VMware vSphere (VSC). You can create one or more custom user accounts with limited access privileges with the ONTAP RBAC feature.

VSC and SRA can access storage systems at either the cluster level or the 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 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 VSC at the cluster level even if you are using VSC or SRA.

To create a new user and to connect a cluster or an to VSC, VASA Provider, and SRA, you should perform the following:

- Create a cluster administrator or an administrator role

  You can use one of the following to create these roles:

  - ONTAP System Manager 9.7 or later

  Configure user roles and privileges

  - RBAC User Creator for ONTAP tool (if using ONTAP 9.6 or earlier)

  RBAC User Creator tool for VSC, VASA Provider and Storage Replication Adapter 7.0 for VMware vSphere

- 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 VSC. You can configure storage systems for VSC by entering the credentials in VSC. Each time you log in to a storage system with these credentials, you will have permissions to the VSC functions that you had set up in ONTAP while creating the credentials.

- Add the storage system to VSC and provide the credentials of the user that you just created

## VSC roles

VSC classifies the ONTAP privileges into the following set of VSC 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 level. This enables users to run SRM operations.

> You must refer to the knowledge base articles if you want to manually configure roles and privileges using ONTAP commands.

- VSC, VASA, and SRA 7.0 ONTAP RBAC Configuration
- Roll up of all commands for VSC and SRA for SVM level

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

# Configure user roles and privileges

You can configure new user roles for managing storage systems using the JSON file provided with the virtual appliance for VSC, VASA Provider, and SRA and ONTAP System Manager.

**Before you begin**

- You should have downloaded the ONTAP Privileges file from the virtual appliance for VSC, VASA Provider, and SRA using `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`.
- You should have configured ONTAP 9.7 System Manager.
- You should have logged in with administrator privileges for the storage system.

**steps**

1. Unzip the downloaded `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip` file.

2. Access ONTAP System Manager.
3. Click **CLUSTER › Settings › Users and Roles**.
4. Click **Add User**.
5. In the **Add User** dialog box, select **Virtualization products**.
6. Click **Browse** to select and upload the ONTAP Privileges JSON file.

   The PRODUCT field is auto populated.

7. Select the required capability from the **PRODUCT CAPABILITY** drop-down menu.

   The **ROLE** field is auto populated based on the product capability selected.

8. Enter the required username and password.
9. Select the privileges (Discovery, Create Storage, Modify Storage, Destroy Storage) required for the user, and then click **Add**.

**Results**

The new role and user is added and you can see the detailed privileges under the role that you have configured.

## Copyright information



## Trademark information