



# **vCenter Server role-based access control features in VSC for VMware vSphere**

VSC, VASA Provider, and SRA 9.7

NetApp  
August 30, 2024

# Table of Contents

- vCenter Server role-based access control features in VSC for VMware vSphere . . . . . 1
  - Components of vCenter Server permissions . . . . . 1
  - Key points about assigning and modifying permissions for vCenter Server . . . . . 3
  - Standard roles packaged with the virtual appliance for VSC, VASA Provider, and SRA . . . . . 4
  - Privileges required for VSC tasks . . . . . 5

# vCenter Server role-based access control features in VSC for VMware vSphere

vCenter Server provides role-based access control (RBAC) that enables you to control access to vSphere objects. In Virtual Storage Console for VMware vSphere, vCenter Server RBAC works with ONTAP RBAC to determine which VSC 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, VSC 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.

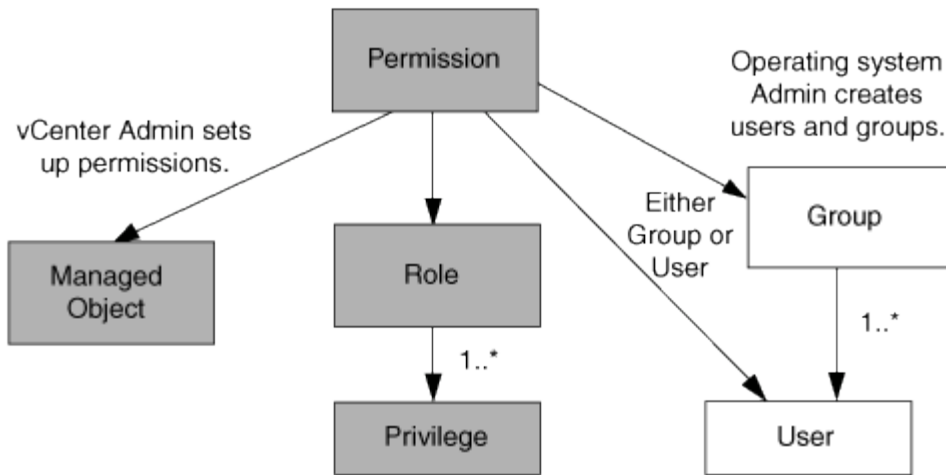
- A user or group

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 Virtual Storage Console for VMware vSphere:

- Native vCenter Server privileges

These privileges come with the vCenter Server.

- VSC-specific privileges

These privileges are defined for specific VSC tasks. They are unique to VSC.

VSC tasks require both VSC-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, VSC provides several standard roles that contain all the VSC-specific and native privileges that are required to perform VSC 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
<b>NetApp Virtual Storage Console</b> › <b>View</b>	<ul style="list-style-type: none"> <li>• VSC Administrator</li> <li>• VSC Provision</li> <li>• VSC Read-Only</li> </ul>	All the VSC and VASA Provider specific tasks require the View Privilege.
<b>NetApp Virtual Storage Console</b> › <b>Policy Based Management</b> › <b>Management</b> or <b>privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label</b> › <b>Management</b>	VSC Administrator	VSC 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 VSC 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 VSC tasks.



These vCenter Server permissions apply to VSC vCenter users, not to VSC administrators. By default, VSC 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 Virtual Storage Console 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 VSC 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 VSC 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 VSC 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 the virtual appliance for VSC, VASA Provider, and SRA

To simplify working with vCenter Server privileges and role-based access control (RBAC), (VSC) provides standard VSC roles that enable you to perform key VSC tasks. There is also a read-only role that enables you to view VSC information, but not perform any tasks.

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

You can view the VSC standard roles by clicking **Roles** on the vSphere Client **Home** page.

The roles that VSC provides enable you to perform the following tasks:

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

Role	Description
VSC Provision	<p>Provides all of the native vCenter Server privileges and VSC-specific privileges that are required to provision storage.</p> <p>You can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Create new datastores</li> <li>• Destroy datastores</li> <li>• View information about storage capability profiles</li> </ul>

## Guidelines for using VSC standard roles

When you work with standard Virtual Storage Console for VMware vSphere roles, there are certain guidelines you should follow.

You should not directly modify the standard roles. If you do, VSC will overwrite your changes each time you upgrade VSC. The installer updates the standard role definitions each time you upgrade VSC. Doing this ensures that the roles are current for your version of VSC 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 VSC 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 VSC Windows service.

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

- Use the standard VSC roles for all VSC tasks.

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

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

If the standard VSC 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-VSC 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 VSC roles, you can use the VSC roles to create new roles.

In this case, you would clone the necessary VSC roles and then edit the cloned role so that it has only the privileges your user requires.

## 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.	<p>The assignment level determines which portions of the UI you can see.</p> <p>Assigning the View privilege at the root object (folder) enables you to enter VSC by clicking the NetApp icon.</p> <p>You can assign the View privilege to another vSphere object level; however, doing that limits the VSC menus that you can see and use.</p> <p>The root object is the recommended place to assign any permission containing the View privilege.</p>

## 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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.