RBAC with VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-tools-vmware-vsphere-10/concepts/rbac-vcenter-environment.html on February 11, 2026. Always check docs.netapp.com for the latest.

Table of Contents

RBAC with VMware vSphere . . . 1
- How vCenter Server RBAC works with ONTAP tools . . . 1
  - Illustration of a vCenter Server permission . . . 1
  - Components of a vCenter Server permission . . . 2
- vCenter Server RBAC considerations for ONTAP tools . . . 2
  - vCenter roles and the administrator account . . . 2
  - vSphere object hierarchy . . . 2
  - Roles included with ONTAP tools for VMware vSphere 10 . . . 3
  - vSphere objects and ONTAP storage backends . . . 6
  - Working with vCenter Server RBAC . . . 6

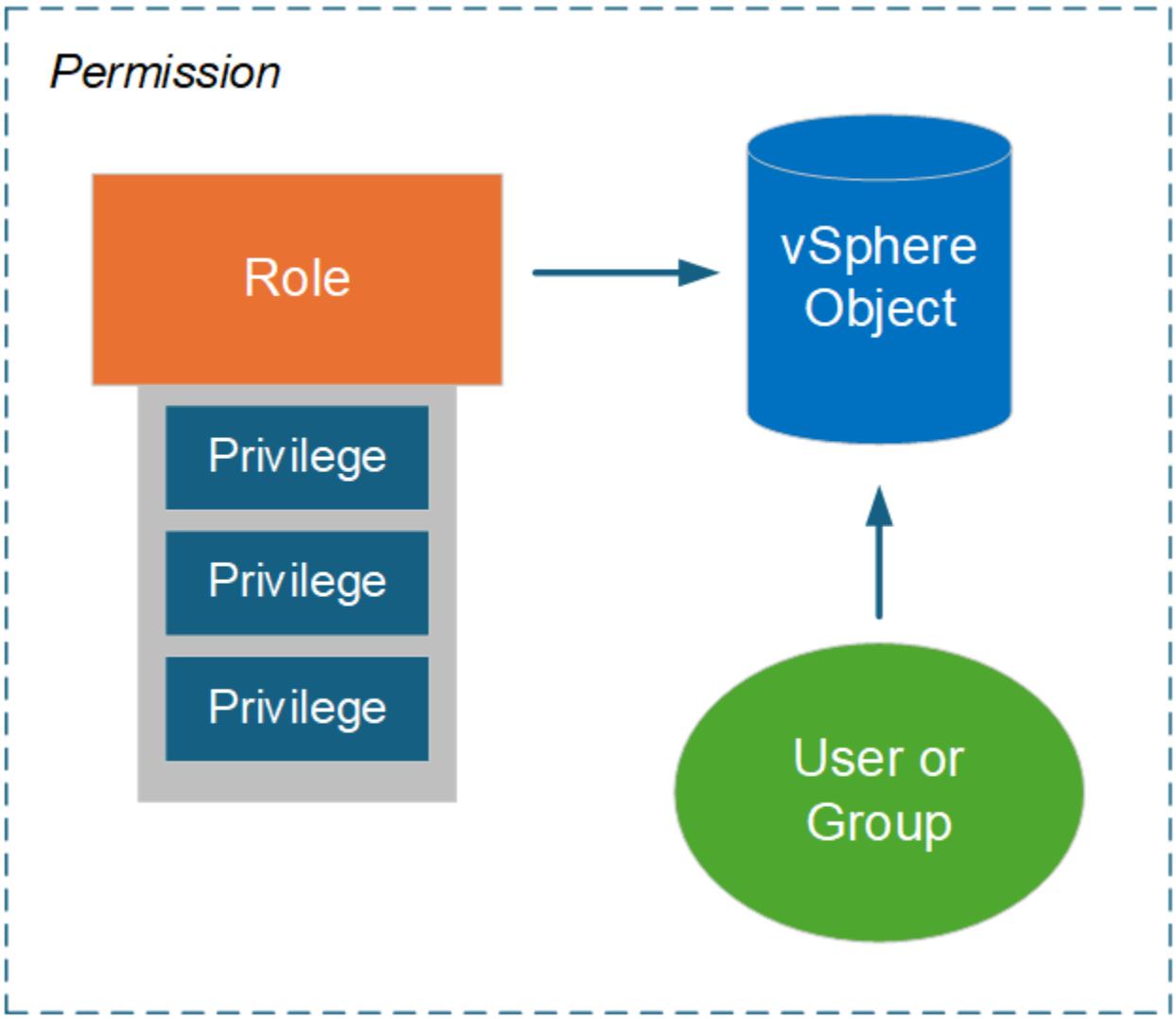
RBAC with VMware vSphere

How vCenter Server RBAC works with ONTAP tools

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.

vCenter Server RBAC considerations for ONTAP tools

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.
The following privileges must be included in the role assigned to the vCenter user responsible for deploying or onboarding vCenter. Ensure these privileges are configured as a prerequisite for the deployment or onboarding process.

- Alarms
  - Acknowledge alarm
- Content Library
  - Add library item
  - Check in a template
  - Check out a template
  - Download files
  - Import storage
  - Read storage
  - Sync library item
  - Sync subscribed library
  - View configuration settings
- Datastore
  - Allocate space
  - Browse datastore
  - Low level file operations
  - Remove file
  - Update virtual machine files
  - Update virtual machine metadata
- ESX Agent Manager
  - View
- Folder

    - Create folder
- Host
    - Configuration
        - Advanced settings
        - Change settings
        - Network configuration
        - System resources
        - Virtual machine autostart configuration
    - Local operations
        - Create virtual machine
        - Delete virtual machine
        - Reconfigure virtual machine
- Network
    - Assign network
    - Configure
- OvfManager
    - OvfConsumer Access
- Host profile
    - View
- Resource
    - Assign virtual machine to resource pool
- Scheduled task
    - Create tasks
    - Modify task
    - Run task
- Tasks
    - Create task
    - Update task
- vApp
    - Add virtual machine
    - Assign resource pool
    - Assign vApp
    - Create
    - Import
    - Move
    - Power off
    - Power on

    - Pull from URL
    - View OVF environment
- Virtual machine
    - Change Configuration
        - Add existing disk
        - Add new disk
        - Add or remove device
        - Advanced configuration
        - Change CPU count
        - Change Memory
        - Change Settings
        - Change resource
        - Extend virtual disk
        - Modify device settings
        - Remove disk
        - Reset guest information
        - Upgrade virtual machine compatibility
    - Edit Inventory
        - Create from existing
        - Create new
        - Move
        - Register
        - Remove
        - Unregister
    - Interaction
        - Backup operation on virtual machine
        - Configure CD media
        - Configure floppy media
        - Connect devices
        - Console interaction
        - Guest operating system management by VIX API
        - Power off
        - Power on
        - Reset
        - Suspend
    - Provisioning
        - Allow disk access

        - Clone template
        - Customize guest
        - Deploy template
        - Modify customization specification
        - Read customization specifications
    - Snapshot management
        - Create snapshot
        - Remove snapshot
        - Rename snapshot
        - Revert to snapshot

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.

Copyright information

Copyright © 2026 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.