



Role based access control

ONTAP tools for VMware vSphere 10.0

NetApp

October 23, 2024

Table of Contents

- Role based access control 1
 - Overview of role-based access control in ONTAP tools 1
 - Recommended ONTAP roles when using ONTAP tools for VMware vSphere 2

Role based access control

Overview of role-based access control in ONTAP tools

vCenter Server provides role-based access control (RBAC) that enables you to control access to vSphere objects. vCenter Server provides centralized authentication and authorization services at many different levels within its inventory, using user and group rights with roles and privileges. vCenter Server features five main components for managing RBAC:

Components	Description
Privileges	A privilege enables or denies access to perform actions in vSphere.
Roles	A role contains one or more system privileges where each privilege defines an administrative right to a certain object or type of object in the system. By assigning a user a role, the user inherits the capabilities of the privileges defined in that role.
Users and groups	Users and groups are used in permissions to assign roles from Active Directory (AD) or potentially local windows users/groups as well (not recommended)
Permissions	Permissions allow you to assign privileges to users or groups to perform certain actions and make changes to objects inside vCenter Server. vCenter Server permissions affect only those users who log into vCenter Server rather than users who log into an ESXi host directly.
Object	An entity upon which actions are performed. VMware vCenter objects are data centers, folders, resource pools, clusters, hosts, and VMs

To successfully complete a task, you must have the appropriate vCenter Server RBAC roles. During a task, ONTAP tools checks a user's vCenter Server roles before checking the user's ONTAP privileges.



The vCenter Server roles apply to ONTAP tools vCenter users, not to administrators. By default, administrators have full access to the product and do not require roles assigned to them.

The users and groups gain access to a role by being part of a vCenter Server role.

Key points about assigning and modifying roles for vCenter Server

You only need to set up vCenter Server roles 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 role determines the ONTAP tools tasks that a user can perform. You can modify one role at any time. If you change the privileges within a role, the user associated with that role should log out and then log back in to enable the updated role.

Standard roles packaged with ONTAP tools

To simplify working with vCenter Server privileges and RBAC, ONTAP tools provide standard ONTAP tools roles that enable you to perform key ONTAP tools tasks. There is also a read-only role that enables you to view the information, but not perform any tasks.

You can view the ONTAP tools standard roles by clicking **Roles** on the vSphere Client Home page. The roles that ONTAP tools provides enable you to perform the following tasks:

Role	Description
NetApp ONTAP tools Administrator	Provides all of the native vCenter Server privileges and ONTAP tools-specific privileges that are required to perform some of the ONTAP tools tasks.
NetApp ONTAP tools Read Only	Provides read-only access to ONTAP tools. These users cannot perform any ONTAP tools actions that are access-controlled.
NetApp ONTAP tools 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: <ul style="list-style-type: none">• Create new datastores• Manage datastores

The Manager UI admin role is not registered with vCenter. This role is specific to the manager UI.

If your company requires that you implement roles that are more restrictive than the standard ONTAP tools roles, you can use the ONTAP tools roles to create new roles.

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

Permissions for ONTAP storage backends and vSphere objects

If the vCenter Server permission is sufficient, ONTAP tools then checks the ONTAP RBAC privileges (your ONTAP role) that are associated with the storage backends credentials (the user name and password) to determine whether you have sufficient privileges to perform the storage operations that are required by that ONTAP tools task on that storage backend. If you have the correct ONTAP privileges, you can access the storage backends and perform the ONTAP tools task. The ONTAP roles determine the ONTAP tools tasks that you can perform on the storage backend.

Recommended ONTAP roles when using ONTAP tools for VMware vSphere

You can set up several recommended ONTAP roles for working with ONTAP tools 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 ONTAP tools tasks.

To create new user roles, you must log in as an administrator on storage systems running ONTAP. You can create ONTAP roles using ONTAP System Manager 9.8P1 or later. See [List of minimum privileges required for non-admin global scoped cluster user](#) for more information.

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 ONTAP tools-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 ONTAP tools 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 ONTAP tools. 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.

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.