



RBAC security

ONTAP automation

NetApp
January 12, 2026

Table of Contents

- RBAC security 1
 - Overview of RBAC security with the ONTAP REST API 1
 - ONTAP roles 1
 - Role mapping and ONTAP processing 2
 - Summary of RBAC evolution 2
 - Work with roles and users in the ONTAP REST API 2
 - Administrative access 2
 - Role definitions 4
 - Privileges 4
 - Summary of the built-in roles 5
 - Comparing the role types 6

RBAC security

Overview of RBAC security with the ONTAP REST API

ONTAP includes a robust and extensible role-based access control (RBAC) capability. You can assign each account a different role to control the user's access to the resources exposed through the REST API and CLI. The roles define different levels of administrative access for the various ONTAP users.



The ONTAP RBAC capability has continued to expand and was significantly enhanced with ONTAP 9.11.1 (and subsequent releases). See [Summary of RBAC evolution](#) and [What's new with the ONTAP REST API](#) for more information.

ONTAP roles

A role is a set of privileges that collectively define what actions the user can take. Each privilege identifies a specific access path and the associated access level. Roles are assigned to user accounts and applied by ONTAP when making access control decisions.

Types of roles

There are two types of roles. They were introduced and tailored to different environments as ONTAP has evolved.



There are advantages and disadvantages when using each type of role. See [Comparing the role types](#) for more information.

Type	Description
REST	The REST roles were introduced with ONTAP 9.6 and are generally applied to users accessing ONTAP through the REST API. Creating a REST role automatically creates a traditional <i>mapping</i> role.
Traditional	These are the legacy roles included prior to ONTAP 9.6. They were introduced for the ONTAP CLI environment and continue to be fundamental to RBAC security.

Scope

Every role has a scope or context within which it is defined and applied. The scope determines where and how a specific role is used.



ONTAP user accounts also have a similar scope that determines how a user is defined and used.

Scope	Description
Cluster	Roles with a cluster scope are defined at the ONTAP cluster level. They are associated with cluster-level user accounts.
SVM	Roles with an SVM scope are defined for a specific data SVM. They are assigned to user accounts in the same SVM.

Source of the role definitions

There are two ways an ONTAP role can be defined.

Role source	Description
Custom	The ONTAP administrator can create custom roles. These roles can be tailored to a specific environment and security requirements.
Built-in	While custom roles provide more flexibility, there is also a set of built-in roles available at both the cluster and SVM level. These roles are pre-defined and can be used for many common administrative tasks.

Role mapping and ONTAP processing

Depending on the ONTAP release you are using, all or nearly all the REST API calls map to one or more CLI commands. When you create a REST role, a traditional or legacy role is also created. This **mapped** traditional role is based on the corresponding CLI commands and cannot be manipulated or changed.



Reverse role mapping is not supported. That is, creating a traditional role does not create a corresponding REST role.

Summary of RBAC evolution

The traditional roles are included with all ONTAP 9 releases. The REST roles were introduced later and have evolved as described below.

ONTAP 9.6

The REST API was introduced with ONTAP 9.6. The REST roles were included with this release as well. Also, when you create a REST role, a corresponding traditional role is also created.

ONTAP 9.7 through 9.10.1

Each ONTAP release from 9.7 through 9.10.1 includes enhancements to the REST API. For example, additional REST endpoints have been added with each release. However, the creation and management of the two roles types remained separate. Also, ONTAP 9.10.1 added REST RBAC support for the snapshots REST endpoint `/api/storage/volumes/{vol.uuid}/snapshots` which is a resource-qualified endpoint.

ONTAP 9.11.1

The ability to configure and manage traditional roles using the REST API was added with this release. Additional access levels for the REST roles were also added.

Work with roles and users in the ONTAP REST API

After understanding the basic RBAC capabilities, you can get started working with the ONTAP roles and users.



See [RBAC workflows](#) for examples of how to create and use roles with the ONTAP REST API.

Administrative access

You can create and manage the ONTAP roles through the REST API or command line interface. The access

details are described below.

REST API

There are several endpoints that can be used when working with RBAC roles and user accounts. The first four in the table are used to create and manage the roles. The last two are used to create and manage user accounts.



You can access the ONTAP online [API reference](#) documentation for more information including examples of how to use the API.

Endpoint	Description
<code>/security/roles</code>	This endpoint allows you to create a new REST role. And beginning with ONTAP 9.11.1 you can also create a traditional role. In this case, ONTAP determines the role type based on the input parameters. You can also retrieve a list of the defined roles.
<code>/security/roles/{owner.UUID}/{name}</code>	You can retrieve or delete a specific cluster or SVM scoped role. The UUID value identifies the SVM where the role is defined (cluster or data SVM). The name value is the name of the role.
<code>/security/roles/{owner.UUID}/{name}/privileges</code>	This endpoint allows you to configure the privileges for a specific role. The built-in roles can be retrieved but not updated. See the API reference documentation for your ONTAP release for more information.
<code>/security/roles/{owner.UUID}/{name}/privileges/[path]</code>	You can retrieve, modify, and delete the access level and optional query value for a specific privilege. See the API reference documentation for your ONTAP release for more information.
<code>/security/accounts</code>	This endpoint allows you to create a new cluster or SVM scoped user account. Several types of information must be included or subsequently added before the account is operational. You can also retrieve a list of the defined user accounts.
<code>/security/accounts/{owner.UUID}/{name}</code>	You can retrieve, modify, and delete a specific cluster or SVM scoped user account. The UUID value identifies the SVM where the user is defined (cluster or data SVM). The name value is the name of the account.

Command line interface

The relevant ONTAP CLI commands are described below. All commands are accessed at the cluster level through an administrator account.

Command	Description
<code>security login</code>	This is the directory containing the commands needed to create and manage a user login.
<code>security login rest-role</code>	This is the directory containing the commands needed to create and manage a REST role associated with a user login.
<code>security login role</code>	This is the directory containing the commands needed to create and manage a traditional role associated with a user login.

Role definitions

The REST and traditional roles are defined through a set of attributes.

Owner and scope

A role can be owned by the ONTAP cluster or a specific data SVM within the cluster. The owner also implicitly determines the scope of the role.

Unique name

Every role must have a unique name within its scope. The name of a cluster role must be unique at the ONTAP cluster level while SVM roles must be unique within the specific SVM.



The name of a new REST role must be unique among the REST roles as well as the traditional roles. This is because creating a REST role also results in a new traditional *mapping* role with the same name.

Set of privileges

Every role contains a set of one or more privileges. Each privilege identifies a specific resource or command and the associated access level.

Privileges

A role can contain one or more privileges. Each privilege definition is a tuple and establishes the level of access to a specific resource or operation.

Resource path

The resource path is identified as either a REST endpoint or CLI command/command directory path.

REST endpoint

An API endpoint identified the target resource for a REST role.

CLI command

A CLI command identifies the target for a traditional role. A command directory can also be specified, which will then include all the downstream commands in the ONTAP CLI hierarchy.

Access level

The access level defines the type of access the role has to the specific resource path or command. The access levels are identified through a set of pre-defined keywords. Three access levels were introduced with ONTAP 9.6. They can be used for both traditional and REST roles. In addition, three new access levels were added with ONTAP 9.11.1. These new access levels can only be used with REST roles.



The access levels follow the CRUD model. With REST, this is based on the primary HTTP methods (POST, GET, PATCH, DELETE). The corresponding CLI operations generally map to the REST operations (create, show, modify, delete).

Access level	REST primitives	Added	REST role only
none	n/a	9.6	No
readonly	GET	9.6	No

Access level	REST primitives	Added	REST role only
all	GET, POST, PATCH, DELETE	9.6	No
read_create	GET, POST	9.11.1	Yes
read_modify	GET, PATCH	9.11.1	Yes
read_create_modify	GET, POST, PATCH	9.11.1	Yes

Optional query

When creating a traditional role, you can optionally include a **query** value to identify the subset of applicable objects for the command or command directory.

Summary of the built-in roles

There are several pre-defined roles included with ONTAP that you can use at either the cluster or SVM level.

Cluster scoped roles

There are several built-in roles available at the cluster scope.

See [Predefined roles for cluster administrators](#) for more information.

Role	Description
admin	Administrators with this role have unrestricted rights and can do anything in the ONTAP system. They can configure all cluster-level and SVM-level resources.
autosupport	This is a special role tailored for the AutoSupport account.
backup	This Special role for backup software that needs to back up the system.
snaplock	This is a special role tailored for the SnapLock account.
readonly	Administrators with this role can view everything at the cluster level but can't make any changes.
none	No administrative capabilities are provided.

SVM scoped roles

There are several built-in roles available at the SVM scope. The **vsadmin** provides access to the most general and powerful capabilities. There are several additional roles tailored to specific administrative tasks, including:

- vsadmin-volume
- vsadmin-protocol
- vsadmin-backup
- vsadmin-snaplock
- vsadmin-readonly

See [Predefined roles for SVM administrators](#) for more information.

Comparing the role types

Before selecting a **REST** role or **traditional** role, you should be aware of the differences. Some of the ways the two role types can be compared are described below.



For more advanced or complex RBAC use cases, you should normally use a traditional role.

How the user accesses ONTAP

Before creating a role, it is important to know how the user will access the ONTAP system. Based on this a role type can be determined.

Access	Suggested type
REST API only	The REST role is designed to be used with the REST API.
REST API and CLI	You can define a REST role which also creates a corresponding traditional role.
CLI only	You can create a traditional role.

Precision of the access path

The access path defined for a REST role is based on a REST endpoint. The access path for a traditional role is based on a CLI command or command directory. In addition, you can include an optional query parameter with a traditional role to further restrict access based on the command parameter values.

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.