RBAC

ONTAP automation

NetApp
January 18, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-automation/workflows/wf_rbac_prepare.html on January 18, 2026. Always check docs.netapp.com for the latest.

Table of Contents

RBAC . . . 1
- Prepare to use RBAC using the ONTAP REST API . . . 1
- Create roles . . . 1
  - Limit access to SVM volume operations using the ONTAP REST API . . . 1
  - Enable adminstration of data protection using the ONTAP REST API . . . 3
  - Allow generation of ONTAP reports using the ONTAP REST API . . . 4
- Create a user with a role using the ONTAP REST API . . . 5
  - Step 1: List the data SVMs in the cluster . . . 5
  - Step 2: List the users defined to the SVM . . . 6
  - Step 3: List the REST roles defined to the SVM . . . 6
  - Step 4: Create a custom REST role . . . 7
  - Step 5: Update the role by adding more privileges . . . 8
  - Step 6: Create a user . . . 8

RBAC

Prepare to use RBAC using the ONTAP REST API

You can use the ONTAP RBAC capability in several different ways depending on your environment. A few common scenarios are presented as workflows in this section. In each case the focus is on a specific security and administrative goal.

Before creating any roles and assigning a role to an ONTAP user account, you should prepare by reviewing the major security requirements and options presented below. Also make sure to review the general workflow concepts at Prepare to use the workflows.

What ONTAP release are you using?

The ONTAP release determines what REST endpoints and RBAC features are available.

Identify the protected resources and scope

You need to identify the resources or commands to be protected and the scope (cluster or SVM).

What access should the user have?

After identifying the resources and scope, you need to determine the access level to be granted.

How will the users access ONTAP?

The user can access ONTAP through the REST API or CLI or both.

Is one of the built-in roles sufficient or is a custom role needed?

It is more convenient to use an existing built-in role but you can create a new custom role if needed.

What type of role is needed?

Based on the security requirements and the ONTAP access, you need to choose whether to create a REST or traditional role.

Create roles

Limit access to SVM volume operations using the ONTAP REST API

You can define a role to restrict storage volume administration within an SVM.

About this workflow

A traditional role is first created to initially allow access to all the major volume administration functions except cloning. The role is defined with the following characteristics:

- Able to perform all CRUD volume operations including get, create, modify, and delete
- Cannot create a volume clone

You can then optionally update the role as needed. In this workflow, the role is changed in the second step to allow the user to create a volume clone.

Step 1: Create the role

You can issue an API call to create the RBAC role.

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
POST	/api/security/roles

Curl example

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON input example

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      { "path": "volume create", "access": "all" },
      { "path": "volume delete", "access": "all" }
    ]
}
```

Step 2: Update the role

You can issue an API call to update the existing role.

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
POST	/api/security/roles

Additional input parameters for curl examples

In addition to the parameters common with all REST API calls, the following parameters are also used in the curl example in this step.

Parameter	Type	Required	Description
$SVM_ID	Path	Yes	This is the UUID of the SVM that contains the role definition.
$ROLE_NAME	Path	Yes	This is the name of the role within the SVM to be updated.

Curl example

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON input example

```
{
  "path": "volume clone",
  "access": "all"
}
```

Enable adminstration of data protection using the ONTAP REST API

You can provide a user with limited data protection capabilities.

About this workflow

The traditional role created is defined with the following characteristics:

- Able to create and delete snapshots as well as update SnapMirror relationships
- Cannot create or modify higher level objects such as volumes or SVMs

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
POST	/api/security/roles

Curl example

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON input example

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "volume snapshot create", "access": "all"},
      {"path": "volume snapshot delete", "access": "all"},
      {"path": "volume show", "access": "readonly"},
      {"path": "vserver show", "access": "readonly"},
      {"path": "snapmirror show", "access": "readonly"},
      {"path": "snapmirror update", "access": "all"}
  ]
}
```

Allow generation of ONTAP reports using the ONTAP REST API

You can create a REST role to provide users with the ability to generate ONTAP reports.

About this workflow

The role created is defined with the following characteristics:

- Able to retrieve all storage object information related to capacity and performance (such as volume, qtree, LUN, aggregates, node, and SnapMirror relationships)
- Cannot create or modify higher level objects (such as volumes or SVMs)

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
POST	/api/security/roles

Curl example

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON input example

```
{
  "name": "rest_role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "/api/storage/volumes", "access": "readonly"},
      {"path": "/api/storage/qtrees", "access": "readonly"},
      {"path": "/api/storage/luns", "access": "readonly"},
      {"path": "/api/storage/aggregates", "access": "readonly"},
      {"path": "/api/cluster/nodes", "access": "readonly"},
      {"path": "/api/snapmirror/relationships", "access": "readonly"},
      {"path": "/api/svm/svms", "access": "readonly"}
  ]
}
```

Create a user with a role using the ONTAP REST API

You can use this workflow to create a user with an associated REST role.

About this workflow

This workflow includes the typical steps needed to create a custom REST role and associate it with a new user account. Both the user and role have an SVM scope and are associated with a specific data SVM. Some of the steps may be optional or need to change depending on your environment.

Step 1: List the data SVMs in the cluster

Perform the following REST API call to list the SVMs in the cluster. The UUID and name of each SVM are provided in the output.

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
GET	/api/svm/svms

Curl example

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

After you finish

Select the desired SVM from the list where you will create the new user and role.

Step 2: List the users defined to the SVM

Perform the following REST API call to list the users defined in the SVM you selected. You can identify the SVM through the owner parameter.

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
GET	/api/security/accounts

Curl example

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

After you finish

Based on the users already defined in the SVM, choose a unique name for the new user.

Step 3: List the REST roles defined to the SVM

Perform the following REST API call to list the roles defined in the SVM you selected. You can identify the SVM through the owner parameter.

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
GET	/api/security/roles

Curl example

```
curl --request GET \
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

After you finish

Based on the roles already defined in the SVM, choose a unique name for the new role.

Step 4: Create a custom REST role

Perform the following REST API call to a create a custom REST role in the SVM. The role initially has only one privilege which establishes a default access of **none** so that all access is denied.

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
POST	/api/security/roles

Curl example

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON input example

```
{
  "name": "dprole1",
  "owner": {
    "name": "dmp",
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "/api", "access": "none"},
  ]
}
```

After you finish

Optionally perform step 3 again to display the new role. You can also display the roles at the ONTAP CLI.

Step 5: Update the role by adding more privileges

Perform the following REST API call to modify the role by adding privileges as needed.

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
POST	/api/security/roles/{owner.uuid}/{name}/privileges

Additional input parameters for curl examples

In addition to the parameters common with all REST API calls, the following parameters are also used in the curl example in this step.

Parameter	Type	Required	Description
$SVM_ID	Path	Yes	The UUID of the SVM that contains the role definition.
$ROLE_NAME	Path	Yes	The name of the role within the SVM to be updated.

Curl example

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON input example

```
{
  "path": "/api/storage/volumes",
  "access": "readonly"
}
```

After you finish

Optionally perform step 3 again to display the new role. You can also display the roles at the ONTAP CLI.

Step 6: Create a user

Perform the following REST API call to a create a user account. The role **dprole1** created above is associated with the new user.

You can create the user without a role. In this case, the user is assigned a default role (either `admin` or `vsadmin`) depending on whether the user is defined with cluster or SVM scope. You'll need to modify the user to assign a different role.

HTTP method and endpoint

This REST API call uses the following method and endpoint.

HTTP method	Path
POST	/api/security/accounts

Curl example

```
curl --request POST \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON input example

```
{
  "owner": {"uuid":"daf84055-248f-11ed-a23d-005056ac4fe6"},
  "name": "david",
  "applications": [
      {"application":"ssh",
       "authentication_methods":["password"],
       "second_authentication_method":"none"}
  ],
  "role":"dprole1",
  "password":"<password>"
}
```

After you finish

You can sign in to the SVM management interface using the credentials for the new user.

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.