Create roles

ONTAP Automation

NetApp
February 11, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-automation/workflows/wf_rbac_role_limit_svm.html on February 11, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Create roles 1
Limit access to SVM volume operations 1
Enable adminstration of data protection 3
Allow generation of ONTAP reports 4

Create roles

Limit access to SVM volume operations

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/priveleges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON input example

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

Enable adminstration of data protection

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

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"}
  ]
}
```

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.