



Manage role privilege details

ONTAP 9.10.1 REST API Documentation

NetApp
April 02, 2024

Table of Contents

- Manage role privilege details 1
 - Security roles owner.uuid name privileges endpoint overview 1
 - Retrieve privilege details of the specified role 3
 - Add a privilege tuple to an existing role 8

Manage role privilege details

Security roles owner.uuid name privileges endpoint overview

Overview

This API is used to configure the role privileges (tuples of REST URI path and its access levels). It also retrieves all of the privilege tuples for a role and can add a tuple to an existing role. The REST URI path can be a resource-qualified endpoint. Currently, the only supported resource-qualified endpoints are `/api/storage/volumes/{volume.uuid}/snapshots` and `/api/storage/volumes//snapshots`. `"` is a wildcard character denoting "all" volumes.

The role can be SVM-scoped or cluster-scoped.

Specify the owner UUID and the role name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the role has been created and can be obtained from the response body of a GET request performed on one of the following APIs: `/api/security/roles` for all the roles
`/api/security/roles/?scope=svm` for SVM-scoped roles
`/api/security/roles/?owner.name=<svm-name><i></i>` for roles in a specific SVM This API response contains the complete URI for each role and can be used after suffixing it with `_"privileges"`.`</svm-name>_`



The pre-defined roles can be retrieved but cannot be updated.

Examples

Adding a privilege tuple for an existing custom role

```
# The API:
POST "/security/roles/{owner.uuid}/{name}/privileges"

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges" -d
'{"access":"readonly","path":"/api/protocols"}
```

Retrieving all the privilege tuples for a role

```
# The API:
GET "/api/security/roles/{owner.uuid}/{name}/privileges"

# The call:
curl -X GET "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges"
```

```

# The response:
{
  "records": [
    {
      "path": "/api/application",
      "access": "all",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fapplication"
        }
      }
    },
    {
      "path": "/api/protocols",
      "access": "readonly",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols"
        }
      }
    },
    {
      "path": "/api/storage/volumes/1385d680-74fc-4adb-a348-9a740e83702a/snapshots",
      "access": "all",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fstorage%2Fvolumes%2F1385d680-74fc-4adb-a348-9a740e83702a%2Fsnapshots"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges"
    }
  }
}

```

Retrieve privilege details of the specified role

GET /security/roles/{owner.uuid}/{name}/privileges

Introduced In: 9.6

Retrieves privilege details of the specified role.

Related ONTAP commands

- `security login rest-role show`

Learn more

- [DOC /security/roles/{owner.uuid}/{name}/privileges](#)
- [DOC /security/roles](#)

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Role owner UUID
name	string	path	True	Role name
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. <ul style="list-style-type: none">• Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[role_privilege]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "access": "readonly",
    "path": "/api/storage/volumes"
  }
}
```

Error

Status: Default, Error

Name	Type	Description
error	error	

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

role_privilege

A tuple containing the REST endpoint and the access level assigned to that endpoint. The REST endpoint can be a resource-qualified endpoint. At present, the only supported resource-qualified endpoints are `/api/storage/volumes/{volume.uuid}/snapshots` and `/api/storage/volumes//snapshots`. `"` is a wildcard character denoting "all" volumes.

Name	Type	Description
_links	_links	
access	string	Access level for the REST endpoint.
path	string	REST URI/endpoint

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Add a privilege tuple to an existing role

POST `/security/roles/{owner.uuid}/{name}/privileges`

Introduced In: 9.6

Adds a privilege tuple (of REST URI and its access level) to an existing role.

Required parameters

- `owner.uuid` - UUID of the SVM that houses this role.
- `name` - Name of the role to be updated.
- `path` - REST URI path (example: `/api/storage/volumes`). Can be a resource-qualified endpoint (example: `/api/storage/volumes/43256a71-be02-474d-a2a9-9642e12a6a2c/snapshots`). Currently, resource-qualified endpoints are limited to the "snapshots" endpoint: `/api/storage/volumes/{volume.uuid}/snapshots` and `/api/storage/volumes//snapshots`. `"` is a wildcard character denoting "all" volumes.
- `access` - Desired access level for the REST URI path (one of "all", "readonly" or "none").

Related ONTAP commands

- `security login rest-role create`

Learn more

- [DOC /security/roles/{owner.uuid}/{name}/privileges](#)
- [DOC /security/roles](#)

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Role owner UUID
name	string	path	True	Role name

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. <ul style="list-style-type: none"> • Default value:

Request Body

Name	Type	Description
_links	_links	
access	string	Access level for the REST endpoint.
path	string	REST URI/endpoint

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access": "readonly",
  "path": "/api/storage/volumes"
}
```

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
5636129	A role with given name has not been defined.
5636143	A Vserver admin cannot use the API with this access level.
5636144	The value specified for the access level is not valid.
5636169	A character in the URI is not valid.
5636170	The URI does not exist.
5636173	This feature requires an effective cluster version of 9.6 or later.
5636175	Vserver admin cannot have access to given API.
5636184	Expanded REST roles for granular resource control feature is currently disabled.
5636185	The specified UUID was not found.
5636186	Expanded REST roles for granular resource control requires an effective cluster version of 9.10.1 or later.
13434890	Vserver-ID failed for Vserver roles.
13434891	UUID LookUp failed for Vserver roles.
13434892	Roles is a required field.
13434893	The SVM does not exist.

Name	Type	Description
error	error	

Example error

```

{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

role_privilege

A tuple containing the REST endpoint and the access level assigned to that endpoint. The REST endpoint can be a resource-qualified endpoint. At present, the only supported resource-qualified endpoints are `/api/storage/volumes/{volume.uuid}/snapshots` and `/api/storage/volumes//snapshots`. `"` is a wildcard character denoting "all" volumes.

Name	Type	Description
_links	_links	
access	string	Access level for the REST endpoint.
path	string	REST URI/endpoint

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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.