# View or delete a role

## REST API reference

NetApp
September 12, 2025

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9131/security_roles_owner.uuid_name_endpoint_overview.html on September 12, 2025. Always check docs.netapp.com for the latest.

# Table of Contents


View or delete a role . . . 1
- Security roles owner.uuid name endpoint overview . . . 1
  - Overview . . . 1
  - Examples . . . 1
- Delete a role . . . 4
  - Required parameters . . . 4
  - Related ONTAP commands . . . 4
  - Learn more . . . 4
  - Parameters . . . 5
  - Response . . . 5
  - Error . . . 5
  - Definitions . . . 6
- Retrieve the details of a role . . . 7
  - Related ONTAP commands . . . 7
  - Learn more . . . 7
  - Parameters . . . 7
  - Response . . . 7
  - Error . . . 9
  - Definitions . . . 9

# View or delete a role

## Security roles owner.uuid name endpoint overview

### Overview

This API is used to retrieve or delete a role. 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 call performed on one of the following APIs: */api/security/roles* for all roles */api/security/roles/?scope=svm* for SVM-scoped roles */api/security/roles/?owner.name={svm-name}* for roles in a specific SVM This API response contains the complete URI for each role that can be used for retrieving or deleting a role.

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

### Examples

#### Retrieving the role configuration for a REST role

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

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

# The response:
{
"owner": {
  "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
  "name": "svm1",
  "_links": {
    "self": {
      "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
    }
  }
},
"name": "secure_role",
"privileges": [
  {
    "path": "/api/security",
    "access": "all",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
```

```
0050568e2e25/secure_role/privileges/%2Fapi%2Fsecurity"
      }
    }
  },
  {
    "path": "/api/storage/volumes/651f7fdf-7752-11eb-8d4e-
0050568ed6bd/snapshots",
    "access": "readonly",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/secure_role/privileges/%2Fapi%2Fstorage%2Fvolumes%2F651f7fdf-
7752-11eb-8d4e-0050568ed6bd%2Fsnapshots"
      }
    }
  },
  {
    "path": "/api/storage/volumes/6dfeb406-9a16-11ec-819e-
005056bb1a7c/top-metrics/clients",
    "access": "readonly",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/secure_role/privileges/%2Fapi%2Fstorage%2Fvolumes%2F6dfeb406-
9a16-11ec-819e-005056bb1a7c%2Ftop-metrics%2Fclients"
      }
    }
  }
],
"builtin": false,
"scope": "svm",
"_links": {
  "self": {
    "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/secure_role"
  }
}
}
```

**Retrieving the role configuration for a custom legacy role**

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

# The call:
```

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

# The response:
{
"owner": {
  "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
  "name": "svm1",
  "_links": {
    "self": {
      "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
    }
  }
},
"name": "finVolNoDel",
"privileges": [
  {
    "path": "DEFAULT",
    "access": "none",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/finVolNoDel/privileges/DEFAULT"
      }
    }
  },
  {
    "path": "volume",
    "access": "all",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/finVolNoDel/privileges/volume"
      }
    }
  },
  {
    "path": "volume delete",
    "access": "none",
    "query": "-volume vol_fin*",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/finVolNoDel/privileges/volume%20delete"
      }
    }
```

```
  }
],
"builtin": false,
"scope": "svm",
"_links": {
  "self": {
    "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/finVolNoDel"
  }
}
}
```

**Deleting a custom role**

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

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

# Delete a role

DELETE `/security/roles/{owner.uuid}/{name}`

**Introduced In:** 9.6

Deletes the specified role.

## Required parameters

- `name` - Name of the role to be deleted.
- `owner.uuid` - UUID of the SVM housing the role.

## Related ONTAP commands

- `security login rest-role delete`
- `security login role delete`

## Learn more

- DOC /security/roles/{owner.uuid}/{name}
- DOC /security/roles

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| owner.uuid | string | path | True | Role owner UUID |
| name | string | path | True | Role name to be deleted. |

## Response

```
Status: 200, Ok
```

## Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|---|---|
| 1263347 | Cannot modify pre-defined roles. |
| 5636169 | Specified URI path is invalid or not supported. Resource-qualified endpoints are not supported. |
| 5636170 | URI does not exist. |
| 5636172 | User accounts detected with this role assigned. Update or delete those accounts before deleting this role. |
| 5636173 | Features require an effective cluster version of 9.6 or later. |
| 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. |
| 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

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. |

# Retrieve the details of a role

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

**Introduced In:** 9.6

Retrieves the details of the specified role.

## Related ONTAP commands

- `security login rest-role show`
- `security login role show`

## Learn more

- DOC /security/roles/{owner.uuid}/{name}
- 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. |

## Response

```
Status: 200, Ok
```

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| builtin | boolean | Indicates if this is a built-in (pre-defined) role which cannot be modified or deleted. |
| name | string | Role name |
| owner | owner | Owner name and UUID that uniquely identifies the role. |

| Name | Type | Description |
|---|---|---|
| privileges | array[role_privilege] | The list of privileges that this role has been granted. |
| scope | string | Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects. |

**Example response**


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "admin",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "privileges": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access": "all",
      "path": "volume move start",
      "query": "-vserver vs1|vs2|vs3 -destination-aggregate
aggr1|aggr2"
    }
  ],
  "scope": "string"
}
```

## 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 |
|---|---|---|
| self | href | |

owner

Owner name and UUID that uniquely identifies the role.

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | The name of the SVM. |
| uuid | string | The unique identifier of the SVM. |

role_privilege

A tuple containing a REST endpoint or a command/command directory path and the access level assigned to that endpoint or command/command directory. If the "path" attribute refers to a command/command directory path, the tuple could additionally contain an optional query. The REST endpoint can be a resource-qualified endpoint. At present, the only supported resource-qualified endpoints are the following

Snapshots APIs

- */api/storage/volumes/{volume.uuid}/snapshots*

File System Analytics APIs

- */api/storage/volumes/{volume.uuid}/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/clients*
- */api/storage/volumes/{volume.uuid}/top-metrics/directories*
- */api/storage/volumes/{volume.uuid}/top-metrics/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/users*
- */api/svm/svms/{svm.uuid}/top-metrics/clients*
- */api/svm/svms/{svm.uuid}/top-metrics/directories*
- */api/svm/svms/{svm.uuid}/top-metrics/files*
- */api/svm/svms/{svm.uuid}/top-metrics/users*

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs.

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| access | string | Access level for the REST endpoint or command/command directory path. If it denotes the access level for a command/command directory path, the only supported enum values are 'none','readonly' and 'all'. |
| path | string | Either of REST URI/endpoint OR command/command directory path. |
| query | string | Optional attribute that can be specified only if the "path" attribute refers to a command/command directory path. The privilege tuple implicitly defines a set of objects the role can or cannot access at the specified access level. The query further reduces this set of objects to a subset of objects that the role is allowed to access. The query attribute must be applicable to the command/command directory specified by the "path" attribute. It is defined using one or more parameters of the command/command directory path specified by the "path" attribute. |

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 © 2025 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.