Manage security roles

ONTAP 9.6 REST API reference

NetApp
August 29, 2024

Table of Contents

Manage security roles

Security roles endpoint overview

Overview

ONTAP supports Role Based Access Control (RBAC) wherein a user account must be associated with a role and the role defines the privileges and rights for that user account. A privilege defines the access level of the API as either "none", "readonly", or "all". This specifies whether the user account can perform only a GET operation or POST, PATCH, and DELETE operations as well. A role can comprise of multiple tuples and each tuple consists of the REST API and its access level. For example, "role1" might be a role that has a tuple {"access":"all","path":"/api/storage/volume"}, which means that a user account with "role1" can perform all GET, POST, PATCH, and DELETE operations on the *api/storage/volume* API or derived APIs which have *api/storage/volume* as the prefix.

In cases where a role has tuples with multiple APIs having the same prefix, the highest match wins out. For example, if "role1" has the following tuples: {"access":"readonly","path":"/api/cluster"} and {"access":"all","path":"/api/cluster/schedules"}, then only a GET operation is allowed on APIs with *api/cluster* as the prefix; while POST, PATCH and DELETE operations are possible on the *api/cluster/schedules* API.

Predefined (built-in) roles

Related REST APIs are used to form predefined cluster-scoped and SVM-scoped roles, such as: "admin", "backup", "readonly" for cluster and "vsadmin", "vsadmin-backup", "vsadmin-protocol" for SVMs. These can be retrieved by calling a GET request on */api/security/roles* API and can be assigned to user accounts. See the examples for *api/security/accounts*.

These predefined roles cannot be modified or deleted.

Mapped roles

Before REST APIs, the RBAC roles (legacy roles) were defined to contain the CLI commands and their access levels. Now, almost all REST APIs map to one or more CLI commands. When a role is created using a POST request on /api/security/roles, a mapped legacy role is created. This legacy role has the same access level (as that of the REST API) for the mapped CLI commands. However, if a legacy role with the same name already exists, the POST operation fails and you need to choose a unique name for the role. The legacy roles cannot be managed using the REST endpoint /api/security/roles or its derivatives. Legacy roles are managed using the CLI commands "security login role <create \| modify \| delete> -role <rolename>".</rolename>

Note that the mapped legacy role (for the REST API role created) cannot be manipulated using the CLI.

The reverse case is not true - the creation of a legacy role will not create a mapped role with equivalent REST APIs.

API restrictions

Numerous APIs are scoped for the cluster level only. This results in an access error if assigned to an SVM-scoped role. For example, *api/cluster/nodes* does not work when added as a tuple entry for an SVM-scoped role.

A number of APIs allowed for an SVM-scoped role might have restrictions on the access level. For example, */api/network/ethernet/ports* cannot have an access level of "all" for an SVM-scoped role; this results in an

access error when a POST or PATCH request is made.

Roles created with a REST API path prefix which is common to many APIs might have restrictions based on the scope of the role; cluster or SVM. For example, {"access":"all","path":"/api/security"} might be a tuple entry for an SVM role. Any GET, POST, PATCH, or DELETE operation fails on API */api/security/accounts* while the same on */api/security/login/messages* succeeds. However, a role with exactly the same tuple when created at the cluster-scope level allows the operations.

Numerous APIs have restrictions on the objects that can be operated on based on the context of the SVM or cluster. For example, a POST request on */api/security/authentication/password* API changes the password for a user account. If executed in the context of an SVM (POST request on an SVM interface), only the password of the user executing the POST can be modified, and attempts to modify the password of any other user results in an access error. However, if a POST request is performed by a cluster administrator account, the password for any user account (cluster or SVM) can be modified.

Examples

Creating a cluster-scoped custom role

Specify the role name and the tuples (of REST APIs and their access level) in the body of the POST request. The owner.uuid or owner.name are not required to be specified for a cluster-scoped role.

```
# The API:
POST "/api/security/roles"

# The call:
curl -k -u <cluster-admin>:<password> -X POST "https://<mgmt-
ip>/api/security/roles" -d '{"name":"cluster_role", "privileges" :
[{"access":"readonly","path":"/api/cluster/jobs"},{"access":"all","path":"
/api/application/applications"},{"access":"readonly","path":"/api/applicat
ion/templates"}]}'
```

Creating an SVM-scoped custom role

For an SVM scoped role, specify either owner.name or owner.uuid in the request body along with other parameters for the role. These correspond to the name or UUID of the SVM for which the role is being created and can be obtained from the response body of GET performed on the */api/svm/svms* API.

```
# The API:
POST "/api/security/roles"

# The call:
curl -k -u <cluster-admin>:<password> -X POST "https://<mgmt-
ip>/api/security/roles" -d '{"owner": {"uuid" : "9f93e553-4b02-11e9-a3f9-
005056bb7acd"},"name":"svm_role", "privileges" :
[{"access":"readonly","path":"/api/cluster/jobs"},{"access":"all","path":"
/api/application/applications"},{"access":"readonly","path":"/api/applicat
ion/templates"}]}'
```

Retrieving the configured roles

All of the roles or a filtered list of roles (for example by name, predefined, and so on) can be retrieved.

```
# The API:
GET "/api/security/roles"

# The call to retrieve all the roles configured in the cluster:
curl -k -u <cluster_admin>:<password> -X GET "https://<mgmt-
ip>/api/security/roles"

# The response:
{
"records": [
  {
    "owner": {
      "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "admin",
    "privileges": [
      {
        "path": "/api",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/admin/privileges/%2Fapi"
          }
        }
      }
    ],
    "builtin": true,
    "scope": "cluster",
    "_links": {
      "self": {
        "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/admin"
      }
    }
  },
```

```
  {
    "owner": {
      "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
      "name": "svm1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "vsadmin",
    "privileges": [
      {
        "path": "/api/application/applications",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fapplication%2Fapplications"
          }
        }
      },
      {
        "path": "/api/application/templates",
        "access": "readonly",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fapplication%2Ftemplates"
          }
        }
      },
      {
        "path": "/api/cluster",
        "access": "readonly",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fcluster"
          }
        }
      },
      {
        "path": "/api/svm/svms",
        "access": "readonly",
        "_links": {
```

```
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fsvm%2Fsvms"
          }
        }
      },
      {
        "path": "/api/svms",
        "access": "readonly",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fsvms"
          }
        }
      }
    ],
    "builtin": true,
    "scope": "svm",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin"
      }
    }
  }
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/security/roles"
  }
}
}
```

Using a scoped call to retrieve the configured roles

```
# Scoped call to retrieve all the roles for a particular SVM using
owner.uuid:
curl -k -u <cluster_admin>:<password> -X GET "https://<mgmt-
ip>/api/security/roles/?owner.uuid=aaef7c38-4bd3-11e9-b238-0050568e2e25"

# Scoped call to retrieve all the roles for a particular SVM using
owner.name:
curl -k -u <cluster_admin>:<password> -X GET "https://<mgmt-
ip>/api/security/roles/?owner.name=svm1"

# Scoped call to retrieve the roles having vsadmin as the prefix in the
role name:
curl -k -u <cluster_admin>:<password> -X GET "https://<mgmt-
ip>/api/security/roles/?name=vsadmin*"

# Scoped call to retrieve the predefined roles:
curl -k -u <cluster_admin>:<password> -X GET "https://<mgmt-
ip>/api/security/roles/?builtin=true"

# Scoped call to retrieve the custom roles:
curl -k -u <cluster_admin>:<password> -X GET "https://<mgmt-
ip>/api/security/roles/?builtin=false"
```

Retrieve a list of roles configured in the cluster

GET `/security/roles`

Retrieves a list of roles configured in the cluster.

Related ONTAP commands

- `security login rest-role show`

Learn more

- DOC /security/roles

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned.
return_timeout	integer	query	False	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.
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]	

Example response


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

_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 the REST endpoint and the access level assigned to that endpoint.

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

role

A named set of privileges that defines the rights an account has when it is assigned the role.

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.
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.

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.

Create a new cluster-scoped or SVM-scoped role

POST `/security/roles`

Creates a new cluster-scoped role or an SVM-scoped role. For an SVM-scoped role, specify either the SVM

name as the owner.name or SVM UUID as the owner.uuid in the request body along with other parameters for the role. The owner.uuid or owner.name are not required to be specified for a cluster-scoped role.

Required parameters

- `name` - Name of the role to be created.
- `privileges` - Array of privilege tuples. Each tuple consists of a REST API path and its desired access level.

Optional parameters

- `owner.name` or `owner.uuid` - Name or UUID of the SVM for an SVM-scoped role.

Related ONTAP commands

- `security login rest-role create`

Learn more

- DOC /security/roles

Request Body

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.
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 request


```
{
  "_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": "readonly",
      "path": "/api/storage/volumes"
    }
  ],
  "scope": "string"
}
```


Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
13434891	UUID lookup failed for Vserver roles.
13434890	Vserver-Id failed for Vserver roles.
13434892	Roles is a required field.
13434893	SVM does not exist.
5636169	Invalid character in URI.
5636170	URI does not exist.
5636129	Role with given name has not been defined.
5636144	Invalid value specified for access level.
5636171	Role already exists in legacy role table.
5636143	A Vserver admin cannot use the API with this access level.

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 the REST endpoint and the access level assigned to that endpoint.

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

role

A named set of privileges that defines the rights an account has when it is assigned the role.

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

Name	Type	Description
owner	owner	Owner name and UUID that uniquely identifies the role.
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.

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

Trademark information