Manage security roles

ONTAP 9.14.1 REST API reference

NetApp
May 08, 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 that role defines the privileges and rights for that user account. A privilege defines the access level of the API or command/command directory path. If a privilege tuple refers to a command/command directory path, it can also be associated with an optional query. The access level specifies the subset of operations a user account can perform from the complete set of API methods {GET, POST, PATCH, and DELETE} or command operations {create, delete, modify, and show}. The optional query specifies the subset of objects that the role is allowed to access. The query can be specified, only if the privilege tuple refers to a command/command directory path. It is defined using one or more parameters of the command/command directory path.

A role can comprise of multiple privilege tuples and each privilege tuple consists of a REST API or command/command directory path, its access level, and an optional query. For a given role, only one type of privilege tuple can be defined. All privilege tuples for a role must contain REST API paths or all privilege tuples for the role must contain command/command directory paths. However, predefined/built-in roles (those defined later) are an exception to this rule.

For example, "role1" might be a role that has a tuple {"access":"all","path":"/api/network/ip"}, which means that a user account with "role1" can perform GET, POST, PATCH, and DELETE requests on the *api/network/ip* API or derived APIs that have *api/network/ip* as the prefix.

In other examples, "role2" might be a role that has a tuple {"access":"read_create_modify","path":"/api/storage/volumes"}, which means that a user account with "role2" can perform GET, POST and PATCH (but not DELETE) requests on the *api/storage/volumes* API or derived APIs that have *api/storage/volumes* as the prefix.

"role3" might be a role that has a tuple {"access":"read_create","path":"vserver nfs"}, which means that a user account with "role3" can perform "show" and "create" operations on *vserver nfs* command or derived commands that have *vserver nfs* as the prefix. There is no query associated with "role3".

"role4" might be a role that has a tuple {"access":"all","path":"snapmirror policy","query":"-policy !CustomPol*"}, which means that a user account with "role4" can perform "show", "create","modify" and "delete" operations on *snapmirror policy* command or derived commands that have *snapmirror policy* as the prefix. However, a user is not authorized to perform the above set of operations on SnapMirror policies starting with the name "CustomPol".

In cases where a role has tuples with multiple APIs having the same prefix or multiple commands/command directories having the same prefix, the highest match wins out. For example, if "role5" has the following tuples: {"access":"readonly","path":"/api/cluster"} and {"access":"all","path":"/api/cluster/schedules"}, then only a GET request is allowed on APIs with *api/cluster* as the prefix; while GET, POST, PATCH and DELETE requests are possible on the *api/cluster/schedules* API. Similarly, if "role6" has the following tuples: {"access":"readonly","path":"volume"} and {"access":"read_create_delete","path":"volume snapshot"}, then only a "show" operation is allowed on commands/command directories with *volume* but not *volume snapshot* as the prefix; while "show", "create" and "delete" operations are possible on the *volume snapshot* command directory or any other command/command directory under *volume snapshot*.

Predefined (built-in) roles

Related REST APIs and related commands/command directories 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*.

A GET request on */api/security/roles/{owner.uuid}/{name}* or */api/security/roles/{owner.uuid}/{name}/privileges*, where "name" refers to a predefined (built-in) role, returns privilege tuples containing REST API paths along with privilege tuples containing command/command directory paths.

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. Legacy roles are also managed using the REST endpoint /api/security/roles and its derivatives. In CLI, legacy roles are managed using the "security login role <create \| modify \| delete> -role <rolename>" commands.</rolename>

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

A role can be a REST role or a legacy role but not both. A role cannot be defined to have a mix of privilege tuples with REST API paths and privilege tuples with command/command directory paths. However, predefined (built-in) roles are an exception to this rule. 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.

Resource-qualified endpoints are now supported. 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

Ontap S3 APIs

– /api/protocols/s3/services/{svm.uuid}/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. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

Examples

Creating a cluster-scoped custom role of REST API tuples

Specify the role name and the tuples (of REST APIs and their access levels) 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 -X POST "https://<mgmt-ip>/api/security/roles" -d
'{"name":"cluster_role1", "privileges" :
[{"access":"readonly","path":"/api/cluster/jobs"},{"access":"all","path":"
/api/application/applications"},{"access":"readonly","path":"/api/applicat
ion/templates"}]}'
```

Creating a cluster-scoped custom role of command and/or command directory tuples

Specify the role name and the tuples (of commands/command directories, their access levels and associated optional queries) 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 -X POST "https://<mgmt-ip>/api/security/roles" -d
'{"name":"cluster_role2", "privileges" :
[{"access":"readonly","path":"volume
qtree","query":""},{"access":"all","path":"security
certificate"},{"access":"readonly","path":"snapmirror policy","query":"-
policy !CustomPol*"}]}'
```

Creating an SVM-scoped custom role of REST API tuples

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 the GET request performed on the */api/svm/svms* API.

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles" -d '{"owner": {"uuid"
: "9f93e553-4b02-11e9-a3f9-005056bb7acd"},"name":"svm_role1", "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 of command and/or command directory tuples

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 the GET request performed on the */api/svm/svms* API.

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles" -d '{"owner": {"uuid"
: "9f93e553-4b02-11e9-a3f9-005056bb7acd"},"name":"svm_role2", "privileges"
: [{"access":"readonly","path":"job schedule interval","query":"-days
>1"},{"access":"all","path":"application
snapshot"},{"access":"none","path":"volume move"}]}'
```

Creating a custom role with a resource-qualified endpoint

Specify the role name and the tuples (of REST APIs and their access levels) in the body of the POST request. One or more of the tuples can now contain a resource-qualified endpoint. At present, the only supported resource-qualified endpoints are the *Snapshots* and *File System Analytics* endpoints listed above in the *Overview* section.

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles" -d
'{"name":"cluster_role", "privileges" :
[{"access":"readonly","path":"/api/cluster/jobs"},{"access":"all","path":"
/api/storage/volumes/4ae77149-7752-11eb-8d4e-
0050568ed6bd/snapshots"},{"access":"all","path":"/api/storage/volumes/6519
986e-7752-11eb-8d4e-
0050568ed6bd/snapshots"},{"access":"readonly","path":"/api/storage/volumes
/8823c869-9ea1-11ec-8771-005056bb1a7c/top-
metrics/users"},{"access":"readonly","path":"/api/application/templates"}]
}'
```

Creating a custom role with a private CLI endpoint

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles" -d
'{"name":"cluster_role3", "privileges" :
[{"access":"readonly","path":"/api/private/cli/cluster"}]}'
```

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?fields=%2A"

# The call to retrieve all the roles configured in the cluster:
curl -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"
          }
        }
      },
      {
        "path": "DEFAULT",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/admin/privileges/DEFAULT"
          }
        }
      }
    ],
```

```
    "builtin": true,
    "scope": "cluster",
    "_links": {
      "self": {
        "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/admin"
      }
    }
  },
  {
    "owner": {
      "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "customRole_rest",
    "privileges": [
      {
        "path": "/api/storage/volumes/738e3c9f-9897-41f2-be92-
a00945fd9bdb/snapshots",
        "access": "readonly",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_rest/privileges/%2Fapi%2Fstorage%2Fvolumes%2F738e3
c9f-9897-41f2-be92-a00945fd9bdb%2Fsnapshots"
          }
        }
      },
      {
        "path": "/api/storage/volumes/e621583b-f445-4713-ba9e-
a052d53c8a83/snapshots",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_rest/privileges/%2Fapi%2Fstorage%2Fvolumes%2Fe6215
83b-f445-4713-ba9e-a052d53c8a83%2Fsnapshots"
          }
        }
      }
      {
```

```
        "path": "/api/svm/svms/881764b5-9ea1-11ec-8771-005056bb1a7c/top-
metrics/directories",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/881764b5-9ea1-11ec-8771-
005056bb1a7c/customRole_rest/privileges/%2Fapi%2Fstorage%2Fsvm%2F881764b5-
9ea1-11ec-8771-005056bb1a7c%2Ftop-metrics%2Fdirectories"
          }
        }
      }
    ],
    "builtin": false,
    "scope": "cluster",
    "_links": {
      "self": {
        "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_rest"
      }
    }
  },
  {
    "owner": {
      "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "customRole_legacy",
    "privileges": [
      {
        "path": "volume",
        "access": "readonly",
        "query":"-is_svm_root false",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_legacy/privileges/volume"
          }
        }
      },
      {
        "path": "volume snapshot",
```

```
        "access": "all",
        "query": "-volume vol1&#124;vol2",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_legacy/privileges/volume%20snapshot"
          }
        }
      }
    ],
    "builtin": false,
    "scope": "cluster",
    "_links": {
      "self": {
        "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_legacy"
      }
    }
  },
  {
    "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/cluster/jobs",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fcluster%2Fjobs"
          }
        }
      },
      {
        "path": "/api/cluster/schedules",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fcluster%2Fschedules"
          }
        }
      },
      {
        "path": "DEFAULT",
        "access": "none",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/DEFAULT"
          }
        }
      },
      {
```

```
        "path": "application create",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/application%20create"
          }
        }
      },
      {
        "path": "application delete",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/application%20delete"
          }
        }
      },
    ],
    "builtin": true,
    "scope": "svm",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin"
      }
    }
  }
],
"num_records": 4,
"_links": {
  "self": {
    "href": "/api/security/roles?fields=%2A"
  }
}
}
```

Using a scoped call to retrieve the configured roles

```
# Scoped call to retrieve all the roles for a particular SVM using
owner.uuid:
curl -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 -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 -X GET "https://<mgmt-ip>/api/security/roles/?name=vsadmin*"

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

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

Retrieve a list of roles configured in the cluster

GET `/security/roles`

Introduced In: 9.6

Retrieves a list of roles configured in the cluster.

Related ONTAP commands

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

Learn more

- DOC /security/roles

Parameters

Name	Type	In	Required	Description
scope	string	query	False	Filter by scope • Introduced in: 9.7

Name	Type	In	Required	Description
privileges.query	string	query	False	Filter by privileges.query • Introduced in: 9.11
privileges.access	string	query	False	Filter by privileges.access • Introduced in: 9.7
privileges.path	string	query	False	Filter by privileges.path • Introduced in: 9.7
name	string	query	False	Filter by name • Introduced in: 9.7
owner.uuid	string	query	False	Filter by owner.uuid • Introduced in: 9.7
owner.name	string	query	False	Filter by owner.name • Introduced in: 9.7
builtin	boolean	query	False	Filter by builtin • Introduced in: 9.7
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. • Default value: 1
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. • 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]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "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": "all",
      "path": "volume move start",
      "query": "-vserver vs1|vs2|vs3 -destination-aggregate
aggr1|aggr2"
    },
    "scope": "cluster"
  }
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_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. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

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*
- */api/protocols/s3/services/{svm.uuid}/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. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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.

Name	Type	Description
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.

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

returned_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`

Introduced In: 9.6

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 or command/command directory path and its desired access level. If the tuple refers to a command/command directory path, it could optionally contain a query.

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`
- `security login role create`

Learn more

- DOC /security/roles

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

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": "all",
    "path": "volume move start",
    "query": "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
  },
  "scope": "cluster"
}
```


Response

```
Status: 201, Created
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1263347	Cannot modify pre-defined roles
2621462	The supplied SVM does not exist.
5636129	Role with given name has not been defined.
5636143	Vserver admin cannot use the API with this access level.
5636144	Invalid value specified for access level.
5636168	This role is mapped to a rest-role and cannot be modified directly. Modifications must be done with rest-role.
5636169	Invalid character in URI.
5636170	URI does not exist.
5636171	Role already exists in legacy role table.
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.
5636191	The "path" parameter in a "privileges" tuple can contain only API endpoint entries or only command and command directory entries.
5636192	The query parameter cannot be specified for the privileges tuple with API endpoint entries.
5636200	The specified value of the access parameter is invalid, if a command or command directory is specified in the path parameter.
13434890	Vserver-ID failed for Vserver roles.
13434891	UUID lookup failed for Vserver roles.
13434892	Roles is a required field.

Also see the table of common errors in the Response body overview section of this documentation.

Name	Type	Description
error	returned_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. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

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*
- */api/protocols/s3/services/{svm.uuid}/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. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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.

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

returned_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