



Manage security-related accounts

ONTAP 9.15.1 REST API reference

NetApp
September 11, 2024

Table of Contents

- Manage security-related accounts 1
 - Security accounts endpoint overview 1
 - Retrieve user accounts in the cluster 9
 - Create a new user account 18

Manage security-related accounts

Security accounts endpoint overview

Overview

A valid user account is required to login to and provision, monitor, and manage the cluster. The scope of the management operation can be at the cluster level or at an individual SVM level. There is a need to create user accounts with specific privileges apart from the default user accounts, "admin", for cluster and "vsadmin" for SVM. Custom user accounts can be configured to perform specific (scoped) operations. User accounts can either be created locally (on the Netapp system) or referenced from an external directory server (NIS, LDAP, or Active Directory). Apart from creation, modification, and deletion of a user account, locking and unlocking of a user account or resetting the password (for local accounts only) is possible.

A user account must be associated with the following before it can become operational:

1. A management application (SSH, HTTP, console, service_processor, and such like) for user login. HTTP enables REST API access.
2. Scope - either cluster or SVM.
3. Authentication source - password (local, NIS/LDAP, Active Directory), public/private key pair-based, certificate based.
4. RBAC role - determines what operations are permitted for the user account.

Restrictions

A number of internal/restricted account names, such as admin, diag, autosupport, and root cannot be used.

There must be at least one console cluster administrator account. Any attempt to delete the last remaining administrator account fails.

Multifactor authentication is only possible for SSH and Service Processor (SP) applications. For the SSH application, the only possible combinations are password (local or NIS/LDAP/Active Directory) and public key and password or public key (local) and TOTP. For the SP application, the only valid combination is password and public key.

If an account is created using the HTTP application type, the password authentication method, and its username contains one of the following special characters: @ or \, then you cannot use this account for basic authorization and its only purpose is for OAuth 2.0 validation.

All authentication sources are not supported by all applications. You must select a compatible authentication method based on the application. The following types of authentications methods are supported:

Application	Supported Authentication Methods
amqp	password
console	password
service_processor	password, publickey
HTTP	password, domain, nsswitch, certificate
ONTAPI	password, domain, nsswitch, certificate

Application	Supported Authentication Methods
SSH	password, publickey (key pair), domain, nsswitch, totp



In this table, "totp" means time-based one-time password and is only allowed to be configured as second authentication, "certificate" means security certificate, "domain" means that the user directory server is an external Active Directory, "nsswitch" means the directory server is an external NIS or LDAP server. At login time, the user is authenticated with these external directory servers which must be provisioned separately. For the SP (*service_processor* in above table) application, *publickey* can only be configured as the second factor of authentication.

Support for publickey authentication and MFA for Domain users has been added.

Support for TOTP as a secondary authentication method with password or public key as the primary authentication method has been added.

For SP (*service_processor* in above table) application, support for *publickey* as a secondary authentication method with password as the primary authentication method has been added.

Examples

Creating a cluster-scoped user account

Specify the user account name, role name, and the tuples (of application and authentication methods) in the body of the POST request. The owner.uid or owner.name are not required to be specified for a cluster-scoped user account.



Each entry in the applications array must be for a different application.

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

# The call to create a cluster user account with applications ssh, http
and password authentication scheme:
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"name":"cluster_user1","applications":[{"application":"ssh","authentication_methods":["password"],"second_authentication_method":"none"}, {"application":"http","authentication_methods":["password"]}],"role":"admin","password":"p@ssw@rd123"}
```

Note: The password is an optional parameter for creation and can be set later using a PATCH request. See the examples for modification of user account or password.

Creating an SVM-scoped user account

For an SVM-scoped account, specify either the SVM name as the owner.name or SVM uuid as the owner.uid along with other parameters for the user account. These indicate the SVM for which the user account 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/accounts"

# The call:
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"owner":{"uuid":"aaef7c38-4bd3-11e9-b238-0050568e2e25"},"name":"svm_user1","applications":[{"application":"ssh","authentication_methods":["password"],"second_authentication_method":"none"}],"role":"vsadmin","password":"p@ssw@rd123"}'
```

Retrieving the configured user accounts

Use the following API to retrieve all of the user accounts or a filtered list of user accounts (by name, for a specific SVM, and so on).

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

# The call to retrieve all the user accounts configured in the cluster:
curl -X GET "https://<mgmt-ip>/api/security/accounts"

# 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",
      "_links": {
        "self": {
          "href": "/api/security/accounts/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": "autosupport",
  "_links": {
    "self": {
      "href": "/api/security/accounts/2903de6f-4bd2-11e9-b238-0050568e2e25/autosupport"
    }
  }
},
{
  "owner": {
    "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
      }
    }
  },
  "name": "cluster_user1",
  "_links": {
    "self": {
      "href": "/api/security/accounts/2903de6f-4bd2-11e9-b238-0050568e2e25/cluster_user1"
    }
  }
},
{
  "owner": {
    "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
    "name": "svm1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
      }
    }
  },
  "name": "svm_user1",
  "_links": {
    "self": {

```

```

      "href": "/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1"
    }
  },
  {
    "owner": {
      "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
      "name": "svml",
      "_links": {
        "self": {
          "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "vsadmin",
    "_links": {
      "self": {
        "href": "/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/vsadmin"
      }
    }
  }
],
"num_records": 5,
"_links": {
  "self": {
    "href": "/api/security/accounts"
  }
}
}

```

```

# The scoped call to retrieve the configured cluster-scoped user accounts:
curl -X GET "https://<mgmt-ip>/api/security/accounts/?scope=cluster"

```

```

# The scoped call to retrieve the configured SVM-scoped user accounts:
curl -X GET "https://<mgmt-ip>/api/security/accounts/?scope=svm"

```

```

# The scoped call to retrieve the user accounts configured for the SVM
"svml":
curl -X GET "https://<mgmt-ip>/api/security/accounts/?owner.name=svml"

```

```

# The scoped call to retrieve the user accounts configured with the
"admin" role:
curl -X GET "https://<mgmt-ip>/api/security/accounts/?role=admin"

```

Creating an Active Directory users with publickey authentication

Specify the Active Directory user account name, role name, and the tuples (application and authentication methods) in the body of the POST request. The owner.uuid or owner.name are not required to be specified for a cluster-scoped user account.

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

# The call to create a cluster user account with application ssh and
publickey authentication scheme for domain users:
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"name":"domain_name\\cluster_user__u1","applications":[{"application":"s
sh","authentication_methods":["publickey"]}]}'
```

Creating an Active Directory user with MFA(domain+publickey)

Specify the Active Directory user account name, role name, and the tuples (application and authentication methods) in the body of the POST request. The owner.uuid or owner.name are not required to be specified for a cluster-scoped user account.

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

# The call to create a cluster user account with application ssh and and
MFA for domain users:
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"name":"domain_name\\cluster_user_u1","applications":[{"application":"ss
h","authentication_methods":["domain"],"second_authentication_method":"pub
lickey"]}]}'
```

Retrieving the configured Active directory user accounts

Use the following API to retrieve all of the Active directory user accounts.


```

# The API:
curl -X GET "https://<mgmt-ip>/api/security/accounts/?name=*\\*"

# The response:
{
"records": [
{
  "owner": {
    "uuid": "d6a740a0-4086-11ed-9f68-0050568edfd7",
    "name": "cluster-1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/d6a740a0-4086-11ed-9f68-0050568edfd7"
      }
    }
  },
  "name": "domain\\ad_user_u1",
  "_links": {
    "self": {
      "href": "/api/security/accounts/d6a740a0-4086-11ed-9f68-0050568edfd7/domain%5Cad_user_u1"
    }
  }
}
],
"num_records": 1,
"_links": {
"self": {
  "href": "/api/security/accounts/?name=*\\*"
}
}
}

```

Creating a user with MFA (password+TOTP)

Cluster-scoped user account: Follow the cluster-scoped user creation example and additionally specify the 'totp' as the second_authentication_method.

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

# The call to create a cluster user account with application ssh,
authentication password and totp:
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"name":"cluster_user_1","applications":[{"application":"ssh","authenticati
on_methods":["password"],"second_authentication_method":"totp"}]}'
```

SVM-scoped user account: Follow the SVM-scoped user creation example and additionally specify the 'totp' as the second_authentication_method.

```
#The API

# The call to create a SVM-scoped user account with application ssh,
authentication password and totp:
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"owner":{"uuid":"aaef7c38-4bd3-11e9-b238-
0050568e2e25"},"name":"svm_user1","applications":[{"application":"ssh","au
thentication_methods":["password"],"second_authentication_method":"totp"}]
,"role":"vsadmin","password":"p@ssw@rd123"}'
```

Creating an SP user with MFA (password + publickey)

Specify the SP user account name, role name, and the tuples (application and authentication methods) in the body of the POST request. The owner.uuid or owner.name are not required to be specified for a cluster-scoped user account.

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

# The call to create a cluster user account with application
service_processor, authentication method password and second
authentication publickey
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"name":"cluster_sp_user1","applications":[{"application":"service_proces
sor","authentication_methods":["password"],"second_authentication_method":
"publickey"}]}'
```

Retrieving the configured SP user accounts

Use the following API to retrieve all of the configured SP user accounts.

```

# The API:
curl -X GET "https://<mgmt-
ip>/api/security/accounts/?applications.application=service_processor"

# The response:
{
  "records": [
    {
      "owner": {
        "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
        "name": "cluster1",
        "_links": {
          "self": {
            "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
          }
        }
      },
      "name": "cluster_sp_user1",
      "applications": [
        {
          "application": "service_processor"
        }
      ],
      "_links": {
        "self": {
          "href": "/api/security/accounts/2903de6f-4bd2-11e9-b238-
0050568e2e25/"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href":
"/api/security/accounts/?applications.application=service_processor"
    }
  }
}

```

Retrieve user accounts in the cluster

GET /security/accounts

Introduced In: 9.6

Retrieves a list of user accounts in the cluster.

Related ONTAP commands

- `security login show`

Learn more

- [DOC /security/accounts](#)

Parameters

Name	Type	In	Required	Description
role.name	string	query	False	Filter by role.name <ul style="list-style-type: none">• Introduced in: 9.7
locked	boolean	query	False	Filter by locked <ul style="list-style-type: none">• Introduced in: 9.7
comment	string	query	False	Filter by comment <ul style="list-style-type: none">• Introduced in: 9.7
owner.uuid	string	query	False	Filter by owner.uuid <ul style="list-style-type: none">• Introduced in: 9.7
owner.name	string	query	False	Filter by owner.name <ul style="list-style-type: none">• Introduced in: 9.7
name	string	query	False	Filter by name <ul style="list-style-type: none">• Introduced in: 9.7• maxLength: 64• minLength: 3

Name	Type	In	Required	Description
password_hash_algorithm	string	query	False	Filter by password_hash_algorithm • Introduced in: 9.11
scope	string	query	False	Filter by scope • Introduced in: 9.7
applications.authentication_methods	string	query	False	Filter by applications.authentication_methods • Introduced in: 9.7
applications.is_ns_switch_group	boolean	query	False	Filter by applications.is_ns_switch_group • Introduced in: 9.15
applications.application	string	query	False	Filter by applications.application • Introduced in: 9.7
applications.second_authentication_method	string	query	False	Filter by applications.second_authentication_method • Introduced in: 9.7
applications.is_ldap_fastbind	boolean	query	False	Filter by applications.is_ldap_fastbind • Introduced in: 9.14

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.
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
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. <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[account]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "applications": [
        {
          "application": "string",
          "authentication_methods": [
            "string"
          ],
          "second_authentication_method": "string"
        }
      ],
      "authentication_methods": [
        "string"
      ],
      "comment": "string",
      "name": "joe.smith",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svml",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "password": "string",
      "password_hash_algorithm": "sha512",
      "public_key": "string",
      "role": {
```

```

    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "string",
  "ssl_ca_certificate": "string"
}
]
}

```

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	

account_application

Name	Type	Description
application	string	Applications
authentication_methods	array[string]	
is_ldap_fastbind	boolean	Optional property that specifies the mode of authentication as LDAP Fastbind.
is_ns_switch_group	boolean	Optional property that specifies whether the user is an LDAP or NIS group.

Name	Type	Description
second_authentication_method	string	An optional additional authentication method for multifactor authentication (MFA). This property is only supported for SSH (<i>ssh</i>) and Service Processor (<i>service_processor</i>) applications. It is ignored for all other applications. Time-based One-Time Passwords (TOTPs) are only supported with the authentication method password or public key. For the Service Processor (<i>service_processor</i>) application, <i>none</i> and <i>publickey</i> are the only supported enum values.

owner

Owner name and UUID that uniquely identifies the user account.

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

Name	Type	Description
_links	_links	
name	string	Role name

account

Name	Type	Description
_links	_links	
applications	array[account_application]	
authentication_methods	array[string]	

Name	Type	Description
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching. To modify "password_hash_algorithm", use REST API <code>"/api/security/authentication/password"</code> .
public_key	string	Public key for SSH.
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
ssl_ca_certificate	string	SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

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 user account

POST /security/accounts

Introduced In: 9.6

Creates a new user account.

Required parameters

- `name` - Account name to be created.
- `applications` - Array of one or more application tuples (of application and authentication methods).

Optional parameters

- `owner.name` or `owner.uuid` - Name or UUID of the SVM for an SVM-scoped user account. If not supplied, a cluster-scoped user account is created.
- `role` - RBAC role for the user account. Defaulted to `admin` for cluster user account and to `vsadmin` for SVM-scoped account.
- `password` - Password for the user account (if the authentication method is opted as password for one or more of applications).
- `second_authentication_method` - Needed for MFA and only supported for `ssh` and `service_processor` applications. Defaults to `none` if not supplied.
- `comment` - Comment for the user account (e.g purpose of this account).
- `locked` - Locks the account after creation. Defaults to `false` if not supplied.
- `is_ldap_fastbind` - Needed for LDAP Fastbind Authentication and only supported for applications SSH, ONTAPI, and HTTP with authentication method "nsswitch" only. Defaults to `false` if not supplied.
- `is_ns_switch_group` - Specifies whether the user is an LDAP or NIS group and is only supported for SSH, ONTAPI, and HTTP applications with the authentication method "nsswitch". Defaults to `false` if not supplied.

Related ONTAP commands

- `security login create`

Learn more

- [DOC /security/accounts](#)

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	
applications	array[account_application]	
authentication_methods	array[string]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.

Name	Type	Description
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching. To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
public_key	string	Public key for SSH.
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
ssl_ca_certificate	string	SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": [
    {
      "application": "string",
      "authentication_methods": [
        "string"
      ],
      "second_authentication_method": "string"
    }
  ],
  "authentication_methods": [
    "string"
  ],
  "comment": "string",
  "name": "joe.smith",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"password": "string",
"password_hash_algorithm": "sha512",
"public_key": "string",
"role": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  }
},
  "name": "admin"
},
"scope": "string",
"ssl_ca_certificate": "string"
}
```

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
1261215	The role was not found.
1261225	Invalid command directory name.
1263343	Cannot lock user with password not set or non-password authentication method.
2621475	This operation is not supported on a node SVM.
2621601	This operation is not supported on a system SVM.
2621706	The specified owner.uuid and owner.name refer to different SVMs.
5636099	User creation with a non-admin role is not supported for service-processor application.
5636121	The user account name is reserved for use by the system.
5636126	Cannot create a user with the username or role as AutoSupport because it is reserved by the system.
5636136	Specifying "is_ns_switch_group" as "true" is supported only for authentication method "nsswitch".
5636140	Creating a login with application console for a data SVM is not supported.
5636141	Creating a login with application service-processor for a data SVM is not supported.
5636154	The second authentication method parameter is supported for SSH and Service Processor (SP) applications only.

Error Code	Description
5636155	The second-authentication-method parameter can be specified only if the authentication-method password or public key nsswitch.
5636156	The same value cannot be specified for the second-authentication-method and the authentication-method.
5636164	If the value for either the authentication-method second-authentication-method is nsswitch or password, the other parameter must differ.
5636165	Second authentication method is not supported for NIS or LDAP group based accounts.
5636176	The application and authentication-method combination is invalid.
5636178	An invalid value is specified for field "application".
5636179	Creating an AMQP application login for a data SVM is not supported.
5636197	LDAP fastbind combination for application and authentication method is not supported.
5636198	LDAP fastbind authentication is supported only for nsswitch.
5636206	Non-domain user cannot have a backslash in the username.
5636207	If the value for either the authentication-method or second-authentication-method parameters is domain, the other parameter must be publickey or none.
5636212	TOTP is supported only when the primary authentication method is password or public key.
5636214	Configuring the user with TOTP as secondary authentication method requires an effective cluster version of 9.13.1 or later
5636223	Specifying "is_ns_switch_group" as "true" is supported only for SSH, ONTAPI and HTTP applications.
5636224	Configuring a Service Processor (SP) user with two-factor authentication requires an effective cluster version of 9.15.1 or later.
5636225	For a Service Processor (SP) user, the second factor of authentication must be one of publickey or none.
5636226	Internal error. Failed to check for ONTAP capability.
7077897	Invalid character in username.
7077898	The username must contain both letters and numbers.
7077899	The username does not meet length requirements.

Error Code	Description
7077906	A role with that name has not been defined for the Vserver.
7077918	The password cannot contain the username.
7077919	The minimum length for new password does not meet the policy.
7077920	A new password must have both letters and numbers.
7077921	The minimum number of special characters required do not meet the policy.
7077929	Cannot lock user with password not set or non-password authentication method.
7077940	The password exceeds the maximum supported length.
7077941	The defined password composition exceeds the maximum password length of 128 characters.
7078900	An admin password is not set. Set the password by including it in the request.

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	

account_application

Name	Type	Description
application	string	Applications
authentication_methods	array[string]	
is_ldap_fastbind	boolean	Optional property that specifies the mode of authentication as LDAP Fastbind.
is_ns_switch_group	boolean	Optional property that specifies whether the user is an LDAP or NIS group.
second_authentication_method	string	An optional additional authentication method for multifactor authentication (MFA). This property is only supported for SSH (<i>ssh</i>) and Service Processor (<i>service_processor</i>) applications. It is ignored for all other applications. Time-based One-Time Passwords (TOTPs) are only supported with the authentication method password or public key. For the Service Processor (<i>service_processor</i>) application, <i>none</i> and <i>publickey</i> are the only supported enum values.

owner

Owner name and UUID that uniquely identifies the user account.

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

Name	Type	Description
_links	_links	
name	string	Role name

account

Name	Type	Description
_links	_links	
applications	array[account_application]	
authentication_methods	array[string]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.

Name	Type	Description
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching. To modify "password_hash_algorithm", use REST API <code>"/api/security/authentication/password"</code> .
public_key	string	Public key for SSH.
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
ssl_ca_certificate	string	SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

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

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.