



Security

ONTAP 9.11.1 REST API reference

NetApp
May 08, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9111/ontap/security_overview.html on May 08, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Security 1
 - Security overview 1
 - Manage security-related operations 1
 - Migrate SVM keys between security key managers 850
 - List key servers configured in an external key manager 856
 - Add primary key servers to an external key manager 862
 - Delete a primary key server 870
 - Retrieve key servers configured in an external key manager 872
 - Update a primary key server 877
 - View key stores 884

Security

Security overview

Overview

You can use ONTAP security APIs to manage security settings for the cluster and SVMs.

SAML

Configure the SAML 2.0 SP (Service Provider) protocol inside ONTAP. Doing so redirects the authentication task to a third-party Identity Provider (IDP) that can utilize any number of approaches for multi-factor authentication. After SAML authentication is enabled, all interactive web access (System Manager, SPI) is authenticated via SAML and a third-party IDP.

Manage security-related operations

Security endpoint overview

Overview

You can use this API for various cluster-wide security-related operations.

"onboard_key_manager_configurable_status" object

Use this API to retrieve details of whether or not the Onboard Key Manager can be configured on the cluster.

– GET /api/security

– GET /api/security?fields=onboard_key_manager_configurable_status

"software_data_encryption" object

Contains software data encryption related information.

The following APIs can be used to enable or disable and obtain default software data at rest encryption values:

– PATCH /api/security -d '{ "software_data_encryption.disabled_by_default" : true }'

– PATCH /api/security -d '{ "software_data_encryption.disabled_by_default" : false }'

– GET /api/security

– GET /api/security?fields=software_data_encryption

A PATCH request on this API using the parameter "software_data_encryption.conversion_enabled" triggers the conversion of all non-encrypted metadata volumes to encrypted metadata volumes and all non-NAE aggregates to NAE aggregates. For the conversion to start, the cluster must have either an Onboard or an external key manager set up and the aggregates should either be empty or have only metadata volumes. No data volumes should be present in any of the aggregates. For MetroCluster configurations, the PATCH request will fail if the cluster is in the switchover state.

The following API can be used to initiate software data encryption conversion.

– PATCH /api/security -d '{ "software_data_encryption.conversion_enabled" : true }'

"fips" object

Contains FIPS mode information.

A PATCH request on this API using the parameter "fips.enabled" switches the system from using the default cryptographic module software implementations to validated ones or vice versa, where applicable. If the value of the parameter is "true" and unapproved algorithms are configured as permitted in relevant subsystems, those algorithms will be disabled in the relevant subsystem configurations. If "false", there will be no implied change to the relevant subsystem configurations.

– GET /api/security

– GET /api/security?fields=fips

– PATCH /api/security -d '{ "fips.enabled" : true }'

– PATCH /api/security -d '{ "fips.enabled" : false }'

"tls" object

Contains TLS configuration information.

A PATCH request on this API using the parameter "tls.cipher_suites" and/or "tls.protocol_versions" configures the permissible cipher suites and/or protocol versions for all TLS-enabled applications in the system.

– GET /api/security

– GET /api/security?fields=tls

– PATCH /api/security -d '{ "tls" : { "protocol_versions" : ["TLSv1.3", "TLSv1.2", "TLSv1.1"],
"cipher_suites" : ["TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"]} }'

"management_protocols" object

Contains Security Protocols information.

This security protocols endpoint is used to retrieve and configure security protocols.

– GET /api/security

– GET /api/security?fields=management_protocols

– PATCH /api/security -d '{ "management_protocols" : { "rsh_enabled" : true } }'

– PATCH /api/security -d '{ "management_protocols" : { "rsh_enabled" : false } }'

– PATCH /api/security -d '{ "management_protocols" : { "telnet_enabled" : true } }'

– PATCH /api/security -d '{ "management_protocols" : { "telnet_enabled" : false } }'

– PATCH /api/security -d '{ "management_protocols" : { "rsh_enabled" : true, "telnet_enabled" : true } }'

GET Examples

Retrieving information about the security configured on the cluster

The following example shows how to retrieve the configuration of the cluster.

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

# The call:
curl -X GET 'https://<mgmt-ip>/api/security?fields=*' -H 'accept:
application/hal+json'

# The response:
{
  "onboard_key_manager_configurable_status": {
    "supported": false,
    "message": "Onboard Key Manager cannot be configured on the cluster.
There are no self-encrypting disks in the cluster, and the following nodes
do not support volume granular encryption: ntap-vsim2.",
    "code": 65537300
  },
  "fips": {
    "enabled": false
  },
  "tls": {
    "cipher_suites": [
      "TLS_RSA_WITH_AES_128_CCM",
      "TLS_RSA_WITH_AES_128_CCM_8",
      "TLS_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_RSA_WITH_AES_128_CBC_SHA",
      "TLS_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_RSA_WITH_AES_256_CCM",
      "TLS_RSA_WITH_AES_256_CCM_8",
      "TLS_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_RSA_WITH_AES_256_CBC_SHA",
      "TLS_RSA_WITH_AES_256_CBC_SHA256",
      "TLS_RSA_WITH_ARIA_128_GCM_SHA256",
      "TLS_RSA_WITH_ARIA_256_GCM_SHA384",
      "TLS_RSA_WITH_CAMELLIA_128_CBC_SHA",
      "TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256",
      "TLS_RSA_WITH_CAMELLIA_256_CBC_SHA",
      "TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256",
      "TLS_DHE_DSS_WITH_AES_128_GCM_SHA256",
      "TLS_DHE_DSS_WITH_AES_128_CBC_SHA",
      "TLS_DHE_DSS_WITH_AES_128_CBC_SHA256",
      "TLS_DHE_DSS_WITH_AES_256_GCM_SHA384",
```

```
"TLS_DHE_DSS_WITH_AES_256_CBC_SHA",
"TLS_DHE_DSS_WITH_AES_256_CBC_SHA256",
"TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256",
"TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384",
"TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA",
"TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA",
"TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256",
"TLS_DHE_PSK_WITH_AES_128_CBC_SHA",
"TLS_DHE_PSK_WITH_AES_128_CBC_SHA256",
"TLS_DHE_PSK_WITH_AES_128_CCM",
"TLS_PSK_DHE_WITH_AES_128_CCM_8",
"TLS_DHE_PSK_WITH_AES_128_GCM_SHA256",
"TLS_DHE_PSK_WITH_AES_256_CBC_SHA",
"TLS_DHE_PSK_WITH_AES_256_CBC_SHA384",
"TLS_DHE_PSK_WITH_AES_256_CCM",
"TLS_PSK_DHE_WITH_AES_256_CCM_8",
"TLS_DHE_PSK_WITH_AES_256_GCM_SHA384",
"TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256",
"TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384",
"TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256",
"TLS_DHE_RSA_WITH_AES_128_CCM",
"TLS_DHE_RSA_WITH_AES_128_CCM_8",
"TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_DHE_RSA_WITH_AES_256_CCM",
"TLS_DHE_RSA_WITH_AES_256_CCM_8",
"TLS_DHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA256",
"TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256",
"TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA",
"TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA",
"TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256",
"TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384",
"TLS_ECDHE_ECDSA_WITH_AES_128_CCM",
"TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8",
"TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA",
```

"TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_256_CCM",
"TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8",
"TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
"TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256",
"TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384",
"TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384",
"TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
"TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_PSK_WITH_AES_128_CBC_SHA",
"TLS_PSK_WITH_AES_128_CBC_SHA256",
"TLS_PSK_WITH_AES_128_CCM",
"TLS_PSK_WITH_AES_128_CCM_8",
"TLS_PSK_WITH_AES_128_GCM_SHA256",
"TLS_PSK_WITH_AES_256_CBC_SHA",
"TLS_PSK_WITH_AES_256_CBC_SHA384",
"TLS_PSK_WITH_AES_256_CCM",
"TLS_PSK_WITH_AES_256_CCM_8",
"TLS_PSK_WITH_AES_256_GCM_SHA384",
"TLS_PSK_WITH_ARIA_128_GCM_SHA256",
"TLS_PSK_WITH_ARIA_256_GCM_SHA384",
"TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_PSK_WITH_CHACHA20_POLY1305_SHA256",
"TLS_RSA_PSK_WITH_AES_128_CBC_SHA",
"TLS_RSA_PSK_WITH_AES_128_CBC_SHA256",
"TLS_RSA_PSK_WITH_AES_128_GCM_SHA256",
"TLS_RSA_PSK_WITH_AES_256_CBC_SHA",

```

    "TLS_RSA_PSK_WITH_AES_256_CBC_SHA384",
    "TLS_RSA_PSK_WITH_AES_256_GCM_SHA384",
    "TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256",
    "TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384",
    "TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256",
    "TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384",
    "TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256",
    "TLS_SRP_SHA_WITH_AES_128_CBC_SHA",
    "TLS_SRP_SHA_WITH_AES_256_CBC_SHA",
    "TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA",
    "TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA",
    "TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA",
    "TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA"
  ],
  "protocol_versions": [
    "TLSv1.3",
    "TLSv1.2",
    "TLSv1.1"
  ]
},
"management_protocols": {
  "rsh_enabled": false,
  "telnet_enabled": false
}
}

```

```
'''
```

== PATCH Examples

=== Enabling software encryption conversion in the cluster

The following example shows how to convert all the aggregates and metadata volumes in the cluster from non-encrypted to encrypted.

= The API:

PATCH /api/security

= The call

```

curl -X PATCH "https://+++<mgmt_ip>+++/api/security" -d '{
  "software_data_encryption.conversion_enabled" : true }'+++</mgmt_ip>+++

```


= The response:

```
{
  "job": {
    "uuid": "ebcbd82d-1cd4-11ea-8f75-005056ac4adc",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/ebcbd82d-1cd4-11ea-8f75-005056ac4adc"
      }
    }
  }
}
```

This returns a job UUID. A subsequent GET for this job UUID returns details of the job.

= The call

```
curl -X GET "https://+++<mgmt_ip>+++/api/cluster/jobs/ebcbd82d-1cd4-11ea-8f75-005056ac4adc"+++</mgmt_ip>+++
```

= The response:

```
{
  "uuid": "ebcbd82d-1cd4-11ea-8f75-005056ac4adc",
  "description": "PATCH /api/security",
  "state": "success",
  "message": "success",
  "code": 0,
  "start_time": "2019-12-12T06:45:40-05:00",
  "end_time": "2019-12-12T06:45:40-05:00",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/ebcbd82d-1cd4-11ea-8f75-005056ac4adc"
    }
  }
}
```

[discrete]

=== Enabling FIPS mode in the cluster

The following example shows how to enable FIPS mode in the cluster.

= The API:

```
PATCH /api/security
```

= The call

```
curl -X PATCH "https://+++<mgmt_ip>+++/api/security" -d '{ "fips.enabled"
: true }'+++</mgmt_ip>+++
```

= The response:

```
{
  "job": {
    "uuid": "8e7f59ee-a9c4-4faa-9513-bef689bbf2c2",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/8e7f59ee-a9c4-4faa-9513-
bef689bbf2c2"
      }
    }
  }
}
```

This returns a job UUID. A subsequent GET for this job UUID returns details of the job.

= The call

```
curl -X GET "https://+++<mgmt_ip>+++/api/cluster/jobs/8e7f59ee-a9c4-4faa-
9513-bef689bbf2c2"+++</mgmt_ip>+++
```

= The response:

```
{
  "uuid": "8e7f59ee-a9c4-4faa-9513-bef689bbf2c2",
  "description": "PATCH /api/security",
  "state": "success",
  "message": "success",
  "code": 0,
  "start_time": "2020-04-28T06:55:40-05:00",
  "end_time": "2020-04-28T06:55:41-05:00",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/8e7f59ee-a9c4-4faa-9513-bef689bbf2c2"
    }
  }
}
```

[discrete]

=== Configuring permissible TLS protocols and cipher suites in the cluster

The following example shows how to configure the cluster to only allow TLSv1.3 & TLSv1.2 with selected cipher suites.

= The API:

PATCH /api/security

= The call

```
curl -X PATCH "https://+++<mgmt_ip>+++/api/security" -d '{ "tls" : {  
  "protocol_versions" : ["TLSv1.3", "TLSv1.2"], "cipher_suites" :  
  ["TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",  
  "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"] } }'+++</mgmt_ip>+++
```

= The response:

```
{  
  "job": {  
    "uuid": "b45b6290-f4f2-442a-aa0e-4d3ffefe5e0d",  
    "_links": {  
      "self": {  
        "href": "/api/cluster/jobs/b45b6290-f4f2-442a-aa0e-  
4d3ffefe5e0d"  
      }  
    }  
  }  
}
```

This returns a job UUID. A subsequent GET for this job UUID returns details of the job.

= The call

```
curl -X GET "https://+++<mgmt_ip>+++/api/cluster/jobs/b45b6290-f4f2-442a-  
aa0e-4d3ffefe5e0d"+++</mgmt_ip>+++
```

= The response:

```
{  
  "uuid": "b45b6290-f4f2-442a-aa0e-4d3ffefe5e0d",  
  "description": "PATCH /api/security",  
  "state": "success",  
  "message": "success",  
  "code": 0,  
  "start_time": "2021-03-22T08:52:50-05:00",  
  "end_time": "2021-03-22T08:52:51-05:00",  
  "_links": {  
    "self": {
```

```

    "href": "/api/cluster/jobs/b45b6290-f4f2-442a-aa0e-4d3ffefe5e0d"
  }
}
}

```

[discrete]
 == Enabling security protocols in the cluster

The following example shows how to enable the security protocol rsh in the cluster.

= The API:

PATCH /api/security

= The call

```

curl -X PATCH "https://+++<mgmt_ip>+++/api/security" -d '{
"management_protocols" : { "rsh_enabled" : true } }'+++</mgmt_ip>+++

```

= The response

```

{
  "job": {
    "uuid": "2980ba28-adab-11eb-8fa3-005056bbfa84",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2980ba28-adab-11eb-8fa3-005056bbfa84"
      }
    }
  }
}

```

= The call:

```

curl -H "accept: application/hal+json" -X GET "https://+++<mgmt-
ip>+++/api/security/?fields=management_protocols"+++</mgmt-ip>+++

```

= The response:

```

{
  "management_protocols": {
    "rsh_enabled": false,
    "telnet_enabled": false
  },
  "_links": {
    "self": {

```

```

    "href": "/api/security"
  }
}
}

'''

[[IDe2c3bb4655b846ca448affebc2c8d4c8]]
= Retrieve information about security configured on the cluster

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security`#

*Introduced In:* 9.7

Retrieves information about the security configured on the cluster.

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|fips
|link:#fips[fips]
a|Cluster-wide Federal Information Processing Standards (FIPS) mode
information.

|management_protocols
|link:#management_protocols[management_protocols]
a|Cluster-wide security protocols related information.

|onboard_key_manager_configurable_status
|link:#onboard_key_manager_configurable_status[onboard_key_manager_configu
rable_status]
a|Indicates whether the Onboard Key Manager can be configured in the
cluster.

|software_data_encryption
|link:#software_data_encryption[software_data_encryption]
a|Cluster-wide software data encryption related information.

|tls
|link:#tls[tls]
a|Cluster-wide Transport Layer Security (TLS) configuration information

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {

```

```

    "href": "/api/resourcelink"
  }
},
"onboard_key_manager_configurable_status": {
  "code": 65537300,
  "message": "No platform support for volume encryption in following
nodes - node1, node2."
},
"tls": {
  "cipher_suites": {
  },
  "protocol_versions": {
  }
}
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",

```

```

    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```



```
[#fips]
[.api-collapsible-fifth-title]
fips
```

Cluster-wide Federal Information Processing Standards (FIPS) mode information.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|enabled
|boolean
```

a|Indicates whether or not the software FIPS mode is enabled on the cluster. Our FIPS compliance involves configuring the use of only approved algorithms in applicable contexts (for example TLS), as well as the use of formally validated cryptographic module software implementations, where applicable. The US government documents concerning FIPS 140-2 outline the relevant security policies in detail.

```
|===
```

```
[#management_protocols]
[.api-collapsible-fifth-title]
management_protocols
```

Cluster-wide security protocols related information.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|rsh_enabled
|boolean
```

a|Indicates whether or not security protocol rsh is enabled on the cluster.

```
|telnet_enabled
```

```
|boolean
a|Indicates whether or not security protocol telnet is enabled on the
cluster.
```

```
|===
```

```
[#onboard_key_manager_configurable_status]
[.api-collapsible-fifth-title]
onboard_key_manager_configurable_status
```

Indicates whether the Onboard Key Manager can be configured in the cluster.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|integer
a|Code corresponding to the status message. Returns a 0 if the Onboard Key
Manager can be configured in the cluster.
```

```
|message
|string
a|Reason that Onboard Key Manager cannot be configured in the cluster.
```

```
|supported
|boolean
a|Set to true if the Onboard Key Manager can be configured in the cluster.
```

```
|===
```

```
[#software_data_encryption]
[.api-collapsible-fifth-title]
software_data_encryption
```

Cluster-wide software data encryption related information.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|conversion_enabled
```

```
|boolean
```

a|Indicates whether or not software encryption conversion is enabled on the cluster. A PATCH request initiates the conversion of all non-encrypted metadata volumes in the cluster to encrypted metadata volumes and all non-NAE aggregates to NAE aggregates. For the PATCH request to start, the cluster must have either an Onboard or an external key manager set up and the aggregates should either be empty or have only metadata volumes. No data volumes should be present in any of the aggregates in the cluster. For MetroCluster configurations, a PATCH request enables conversion on all the aggregates and metadata volumes of both local and remote clusters and is not allowed when the MetroCluster is in switchover state.

```
|disabled_by_default
```

```
|boolean
```

a|Indicates whether or not default software data at rest encryption is disabled on the cluster.

```
|===
```

```
[#tls]
```

```
[.api-collapsible-fifth-title]
```

```
tls
```

Cluster-wide Transport Layer Security (TLS) configuration information

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|cipher_suites
```

```
|array[string]
```

a|Names a cipher suite that the system can select during TLS handshakes. A list of available options can be found on the Internet Assigned Number

Authority (IANA) website.

```
|protocol_versions
|array[string]
a|Names a TLS protocol version that the system can select during TLS
handshakes. The use of SSLv3 or TLSv1 is discouraged.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
[[ID7581f4e63859494e5387fb992c50b02a]]
```

```
= Update the software FIPS mode or enable conversion of non-encrypted  
metadata volumes non-NAE aggregates
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-  
block]#`/security`#
```

```
*Introduced In:* 9.8
```

```
Updates the software FIPS mode or enables conversion of non-encrypted  
metadata volumes to encrypted metadata volumes and non-NAE aggregates to  
NAE aggregates.
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```

|In
|Required
|Description

|return_timeout
|integer
|query
|False
a|The number of seconds to allow the call to execute before returning.
When doing a POST, PATCH, or DELETE operation on a single record, the
default is 0 seconds. This means that if an asynchronous operation is
started, the server immediately returns HTTP code 202 (Accepted) along
with a link to the job. If a non-zero value is specified for POST, PATCH,
or DELETE operations, ONTAP waits that length of time to see if the job
completes so it can return something other than 202.

* Default value: 1
* Max value: 120
* Min value: 0

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|fips
|link:#fips[fips]
a|Cluster-wide Federal Information Processing Standards (FIPS) mode
information.

|management_protocols
|link:#management_protocols[management_protocols]
a|Cluster-wide security protocols related information.

```

```
|onboard_key_manager_configurable_status
|link:#onboard_key_manager_configurable_status[onboard_key_manager_configurable_status]
a|Indicates whether the Onboard Key Manager can be configured in the cluster.
```

```
|software_data_encryption
|link:#software_data_encryption[software_data_encryption]
a|Cluster-wide software data encryption related information.
```

```
|tls
|link:#tls[tls]
a|Cluster-wide Transport Layer Security (TLS) configuration information
```

```
|===
```

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "onboard_key_manager_configurable_status": {
    "code": 65537300,
    "message": "No platform support for volume encryption in following nodes - node1, node2."
```

```
  },
  "tls": {
    "cipher_suites": {
    },
    "protocol_versions": {
    }
  }
}
```

```
====
```

```
== Response
```

Status: 202, Accepted

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|job
|link:#job_link[job_link]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
====

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 5636142
| This operation is not supported in a mixed-release cluster.

| 52428817
| SSLv3 is not supported when FIPS is enabled.
```



```

| 52428824
| TLSv1 is not supported when FIPS is enabled.

| 52428830
| Cannot enable FIPS-compliant mode because the configured minimum
security strength for certificates is not compatible.

| 52428832
| TLSv1.1 is not supported when FIPS is enabled.

| 52559974
| Cannot enable FIPS-compliant mode because a certificate that is not
FIPS-compliant is in use.

| 196608081
| Cannot start software encryption conversion while there are data volumes
in the cluster.

| 196608082
| The operation is not valid when the MetroCluster is in switchover mode.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    }
  }
}

```

```

    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```

```
[#fips]
[.api-collapsible-fifth-title]
fips
```

Cluster-wide Federal Information Processing Standards (FIPS) mode information.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|enabled
|boolean
```

a|Indicates whether or not the software FIPS mode is enabled on the cluster. Our FIPS compliance involves configuring the use of only approved algorithms in applicable contexts (for example TLS), as well as the use of formally validated cryptographic module software implementations, where applicable. The US government documents concerning FIPS 140-2 outline the relevant security policies in detail.

```
|===
```

```
[#management_protocols]
[.api-collapsible-fifth-title]
management_protocols
```

Cluster-wide security protocols related information.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|rsh_enabled
|boolean
```

a|Indicates whether or not security protocol rsh is enabled on the cluster.

```
|telnet_enabled
|boolean
a|Indicates whether or not security protocol telnet is enabled on the
cluster.
```

```
|===
```

```
[#onboard_key_manager_configurable_status]
[.api-collapsible-fifth-title]
onboard_key_manager_configurable_status
```

Indicates whether the Onboard Key Manager can be configured in the cluster.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|integer
```

a|Code corresponding to the status message. Returns a 0 if the Onboard Key Manager can be configured in the cluster.

```
|message
```

```
|string
```

a|Reason that Onboard Key Manager cannot be configured in the cluster.

```
|supported
```

```
|boolean
```

a|Set to true if the Onboard Key Manager can be configured in the cluster.

```
|===
```

```
[#software_data_encryption]
[.api-collapsible-fifth-title]
software_data_encryption
```

Cluster-wide software data encryption related information.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|conversion_enabled
```

```
|boolean
```

a|Indicates whether or not software encryption conversion is enabled on the cluster. A PATCH request initiates the conversion of all non-encrypted metadata volumes in the cluster to encrypted metadata volumes and all non-NAE aggregates to NAE aggregates. For the PATCH request to start, the cluster must have either an Onboard or an external key manager set up and the aggregates should either be empty or have only metadata volumes. No data volumes should be present in any of the aggregates in the cluster. For MetroCluster configurations, a PATCH request enables conversion on all the aggregates and metadata volumes of both local and remote clusters and is not allowed when the MetroCluster is in switchover state.

```
|disabled_by_default
```

```
|boolean
```

a|Indicates whether or not default software data at rest encryption is disabled on the cluster.

```
|===
```

```
[#tls]
```

```
[.api-collapsible-fifth-title]
```

tls

Cluster-wide Transport Layer Security (TLS) configuration information

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|cipher_suites
```

```
|array[string]
```

```

a|Names a cipher suite that the system can select during TLS handshakes. A
list of available options can be found on the Internet Assigned Number
Authority (IANA) website.

|protocol_versions
|array[string]
a|Names a TLS protocol version that the system can select during TLS
handshakes. The use of SSLv3 or TLSv1 is discouraged.

|===

[#security_config]
[.api-collapsible-fifth-title]
security_config

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|fips
|link:#fips[fips]
a|Cluster-wide Federal Information Processing Standards (FIPS) mode
information.

|management_protocols
|link:#management_protocols[management_protocols]
a|Cluster-wide security protocols related information.

|onboard_key_manager_configurable_status
|link:#onboard_key_manager_configurable_status[onboard_key_manager_configu
rable_status]
a|Indicates whether the Onboard Key Manager can be configured in the
cluster.

|software_data_encryption

```

```
|link:#software_data_encryption[software_data_encryption]
a|Cluster-wide software data encryption related information.
```

```
|tls
|link:#tls[tls]
a|Cluster-wide Transport Layer Security (TLS) configuration information
```

```
|===
```

```
[#job_link]
[.api-collapsible-fifth-title]
job_link
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|uuid
|string
a|The UUID of the asynchronous job that is triggered by a POST, PATCH, or
DELETE operation.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
```

```

a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```



```
:leveloffset: -1
```

```
= Manage security-related accounts
```

```
:leveloffset: +1
```

```
[[ID7b443a52c0f6176458d527ae022329c8]]
```

```
= 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:

- . A management application (SSH, HTTP, console, service_processor, and such like) for user login. HTTP enables REST API access.
- . Scope - either cluster or SVM.
- . Authentication source - password (local, NIS/LDAP, Active Directory), public/private key pair-based, certificate based.
- . 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.

Multi-factor authentication is only possible for SSH application and the only combination possible is password (local or NIS/LDAP) and public key.

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	
HTTP	
password, domain, nsswitch, certificate	
ONTAPI	
password, domain, nsswitch, certificate	
SSH	
password, publickey (key pair), domain, nsswitch	
===	

NOTE: In this table, "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.

== 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.uuid or owner.name are not required to be specified for a cluster-scoped user account.

NOTE: 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.uuid 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": "svm1",
    "_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"
----

[[ID7681a3121d850e4b80e4553697f2f2c1]]
= Retrieve user accounts in the cluster

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/accounts`#

*Introduced In:* 9.6

Retrieves a list of user accounts in the cluster.

== Related ONTAP commands

* `security login show`

```

== Learn more

* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|ssl_ca_certificate

|string

|query

|False

a|Filter by ssl_ca_certificate

* Introduced in: 9.11

|authentication_methods

|string

|query

|False

a|Filter by authentication_methods

* Introduced in: 9.11

|locked

|boolean

|query

|False

a|Filter by locked

* Introduced in: 9.7

|role.name

|string

```
|query
|False
a|Filter by role.name
```

```
* Introduced in: 9.7
```

```
|password_hash_algorithm
|string
|query
|False
a|Filter by password_hash_algorithm
```

```
* Introduced in: 9.11
```

```
|name
|string
|query
|False
a|Filter by name
```

```
* Introduced in: 9.7
```

```
* maxLength: 64
```

```
* minLength: 3
```

```
|applications.application
|string
|query
|False
a|Filter by applications.application
```

```
* Introduced in: 9.7
```

```
|applications.second_authentication_method
|string
|query
|False
a|Filter by applications.second_authentication_method
```

```
* Introduced in: 9.7
```

```
|applications.authentication_methods
|string
```



```
|query
|False
a|Filter by applications.authentication_methods
```

* Introduced in: 9.7

```
|comment
|string
|query
|False
a|Filter by comment
```

* Introduced in: 9.7

```
|ldap_fastbind
|boolean
|query
|False
a|Filter by ldap_fastbind
```

* Introduced in: 9.11

```
|scope
|string
|query
|False
a|Filter by scope
```

* Introduced in: 9.7

```
|owner.uuid
|string
|query
|False
a|Filter by owner.uuid
```

* Introduced in: 9.7

```
|owner.name
|string
|query
|False
```

a|Filter by owner.name

* Introduced in: 9.7

|public_key

|string

|query

|False

a|Filter by public_key

* Introduced in: 9.11

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|max_records

|integer

|query

|False

a|Limit the number of records returned.

|return_records

|boolean

|query

|False

a|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

a|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
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#account[account]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {

```

```

    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "applications": {
      "application": "amqp",
      "authentication_methods": {
      },
      "second_authentication_method": "none"
    },
    "authentication_methods": {
    },
    "comment": "string",
    "name": "joe.smith",
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "password_hash_algorithm": "sha512",
    "role": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "admin"
    },
    "scope": "cluster"
  }
}
=====

```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

```

```

|===

[#account_application]
[.api-collapsible-fifth-title]
account_application

[cols=3*,options=header]
|===
|Name
|Type
|Description

|application
|string
a|Applications

|authentication_methods
|array[string]
a|

|second_authentication_method
|string
a|An optional additional authentication method for MFA. This only works
with SSH as the application. It is ignored for all other applications.

|===

[#owner]
[.api-collapsible-fifth-title]
owner

Owner name and UUID that uniquely identifies the user account.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role]
[.api-collapsible-fifth-title]
role
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|Role name
```

```
|===
```

```
[#account]
[.api-collapsible-fifth-title]
account
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
```



```

|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|authentication_methods
|array[string]
a|

|comment
|string
a|Optional comment for the user account.

|ldap_fastbind
|boolean
a|Optional property that specifies the mode of authentication is LDAP
Fastbind.

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|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
a|Optional property that specifies the password hash algorithm used to
generate a hash of the user's password for password matching.

```

```
|public_key
|string
a|Public key for SSH.
```

```
|role
|link:#role[role]
a|
```

```
|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.
```

```
|ssl_ca_certificate
|string
a|SSL certificate for the chain of certificate authorities (CA) that have
signed this user's client certificate.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID98ee5037858373a089cf3beb0c444a73]]
= Create a new user account

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/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 application. 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.
- * ``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.

== Related ONTAP commands

- * ``security login create``

== Learn more

- * `xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]`

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

```

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|authentication_methods
|array[string]
a|

|comment
|string
a|Optional comment for the user account.

|ldap_fastbind
|boolean
a|Optional property that specifies the mode of authentication is LDAP
Fastbind.

|locked
|boolean
a|Locked status of the account.

```

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|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
a|Optional property that specifies the password hash algorithm used to generate a hash of the user's password for password matching.

|public_key
|string
a|Public key for SSH.

|role
|link:#role[role]
a|

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

|ssl_ca_certificate
|string
a|SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

|===

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": {
    "application": "amqp",
    "authentication_methods": {
    },
    "second_authentication_method": "none"
  },
  "authentication_methods": {
  },
  "comment": "string",
  "name": "joe.smith",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "password_hash_algorithm": "sha512",
  "role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "cluster"
}
====

== Response
```

Status: 201, Created

== Error

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 1261215

| The role was not found.

| 1263343

| Cannot lock user with password not set or non-password authentication method.

| 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.

| 5636140

| Creating a login with application console for a data Vserver is not supported.

| 5636141

| Creating a login with application service-processor for a data Vserver is not supported.

| 5636154

| The second-authentication-method parameter is supported for ssh application.

| 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.

| 5636157

| If the authentication-method is domain, the second-authentication-method cannot be specified.

| 5636164

| If the value for either the authentication-method second-authentication-method is nsswitch or password, the other parameter must differ.

| 5636197

| LDAP fastbind combination for application and authentication method is not supported.

| 5636198

| LDAP fastbind authentication is supported only for nsswitch.

| 7077897

| Invalid character in username.

| 7077898

| The username must contain both letters and numbers.

| 7077899

| The username does not meet length requirements.

| 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.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions

```

```
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_application]
[.api-collapsible-fifth-title]
account_application

[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```

|application
|string
a|Applications

|authentication_methods
|array[string]
a|

|second_authentication_method
|string
a|An optional additional authentication method for MFA. This only works
with SSH as the application. It is ignored for all other applications.

|===

[#owner]
[.api-collapsible-fifth-title]
owner

Owner name and UUID that uniquely identifies the user account.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

```

```

[#role]
[.api-collapsible-fifth-title]
role

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Role name

|===

[#account]
[.api-collapsible-fifth-title]
account

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|authentication_methods
|array[string]
a|

|comment
|string

```

a|Optional comment for the user account.

|ldap_fastbind

|boolean

a|Optional property that specifies the mode of authentication is LDAP Fastbind.

|locked

|boolean

a|Locked status of the account.

|name

|string

a|User or group account name

|owner

|link:#owner[owner]

a|Owner name and UUID that uniquely identifies the user account.

|password

|string

a|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

a|Optional property that specifies the password hash algorithm used to generate a hash of the user's password for password matching.

|public_key

|string

a|Public key for SSH.

|role

|link:#role[role]

a|

|scope

|string

a|Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

|ssl_ca_certificate

|string

a|SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= Manage scoped user accounts
```

```
:leveloffset: +1
```

```
[[ID359711fcf1265133106e3dfe824f259a]]
```

```
= Security accounts owner.uuid name endpoint overview
```

```
== Overview
```

This API displays and manages the configuration of scoped user accounts.

Newly created user accounts might need to be updated for many reasons. For example, a user account might need to use a different application or its role might need to be modified. According to a policy, the password or

authentication source of a user account might need to be changed, or a user account might need to be locked or deleted from the system. This API allows you to make these changes to user accounts.

Specify the owner UUID and the user account name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the user account has been created and can be obtained from the response body of the GET request performed on one of the following APIs:

`_/_api/security/accounts_` for all user accounts

`_/_api/security/accounts/?scope=cluster_` for cluster-scoped user accounts

`_/_api/security/accounts/?scope=svm_` for SVM-scoped accounts

`_/_api/security/accounts/?owner.name={svm-name}_` for a specific SVM

This API response contains the complete URI for each user account that can be used.

== Examples

=== Retrieving the user account details

The API:

GET `"/api/security/accounts/{owner.uuid}/{name}"`

The call:

curl -X GET `"https://<mgmt-ip>/api/security/accounts/aef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1"`

The response:

```
{
  "owner": {
    "uuid": "aef7c38-4bd3-11e9-b238-0050568e2e25",
    "name": "svm1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/aef7c38-4bd3-11e9-b238-0050568e2e25"
      }
    }
  },
  "name": "svm_user1",
  "applications": [
    {
      "application": "ssh",
      "authentication_methods": [
        "password"
      ]
    }
  ]
}
```

```

    "second_authentication_method": "none"
  }
],
"role": {
  "name": "vsadmin",
  "_links": {
    "self": {
      "href": "/api/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25/admin/roles/vsadmin"
    }
  }
},
"locked": false,
"password_hash_algorithm": "sha512",
"scope": "svm",
"_links": {
  "self": {
    "href": "/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1"
  }
}
}
}
-----

```

=== Updating the applications and role in a user account

Specify the desired configuration in the form of tuples (of applications and authentication methods) and the role. All other previously configured applications that are not specified in the "applications" parameter of the PATCH request will be de-provisioned for the user account.

The API:

PATCH "/api/security/accounts/{owner.uuid}/{name}"

The call to update the applications and role:

```

curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1" -d
'{"applications":[{"application":"http","authentication_methods":["domain"]}, {"application":"ontapi","authentication_methods":["password"]}], "role": {"name": "vsadmin-backup"}}'

```

The call to update only the role:

```

curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1" -d '{"role":"vsadmin-protocol"}'

```

==== Updating the password for a user account

The API:
PATCH "/api/security/accounts/{owner.uuid}/{name}"

The call:
curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1" -d '{"password":"newp@ssw@rd2"}'

==== Locking a user account

The API:
PATCH "/api/security/accounts/{owner.uuid}/{name}"
The call:
curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1" -d '{"locked":"true"}'

==== Deleting a user account

The API:
DELETE "/api/security/accounts/{owner.uuid}/{name}"

The call:
curl -X DELETE "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1"

[[ID1b34c0c839dfc85f25d0c21c0ab9d027]]
= Delete a user account

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/security/accounts/{owner.uuid}/{name}`#

Introduced In: 9.6

Deletes a user account.

== Required parameters

- * `name` - Account name to be deleted.
- * `owner.uuid` - UUID of the SVM housing the user account to be deleted.

== Related ONTAP commands

- * `security login delete`

== Learn more

*
xref:{relative_path}security_accounts_owner.uuid_name_endpoint_overview.html[DOC /security/accounts/{owner.uuid}/{name}]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]

== Parameters

[cols=5*,options=header]
|===

Name	Type	In	Required	Description
------	------	----	----------	-------------

owner.uuid	string	path	True	a Account owner UUID
------------	--------	------	------	----------------------

name	string	path	True	a User account name
------	--------	------	------	---------------------

|===

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 5636098  
| Last unlocked account that has an admin role cannot be deleted.  
  
| 5636125  
| The operation is not supported on system accounts.  
  
| 5636146  
| Cannot delete the last console account with admin role.  
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{  
  "error": {  
    "arguments": {
```

```

        "code": "string",
        "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
}
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====


[[IDf1b5242b66b88064ea57060191460750]]
= Retrieve a specific user account


[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/accounts/{owner.uuid}/{name}`#


*Introduced In:* 9.6


Retrieves a specific user account.


== Related ONTAP commands


* `security login show`


== Learn more

```

```

*
xref:{relative_path}security_accounts_owner.uuid_name_endpoint_overview.ht
ml[DOC /security/accounts/{owner.uuid}/{name}]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

```

== Parameters

```

[cols=5*,options=header]
|===

```

```

|Name
|Type
|In
|Required
|Description

```

```

|owner.uuid
|string
|path
|True
a|Account owner UUID

```

```

|name
|string
|path
|True
a|User account name

```

```

|fields
|array[string]
|query
|False
a|Specify the fields to return.

```

```

|===

```

== Response

Status: 200, Ok

```

[cols=3*,options=header]
|===

```



```

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|authentication_methods
|array[string]
a|

|comment
|string
a|Optional comment for the user account.

|ldap_fastbind
|boolean
a|Optional property that specifies the mode of authentication is LDAP
Fastbind.

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|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
a|Optional property that specifies the password hash algorithm used to
generate a hash of the user's password for password matching.

|public_key
|string
a|Public key for SSH.

|role
|link:#role[role]
a|

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|ssl_ca_certificate
|string
a|SSL certificate for the chain of certificate authorities (CA) that have
signed this user's client certificate.

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": {
    "application": "amqp",
    "authentication_methods": {
    },
    "second_authentication_method": "none"
  },
},

```

```

"authentication_methods": {
  },
  "comment": "string",
  "name": "joe.smith",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "password_hash_algorithm": "sha512",
  "role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "cluster"
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]

```

```

=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_application]
[.api-collapsible-fifth-title]
account_application

[cols=3*,options=header]
|===
|Name
|Type
|Description

|application
|string
a|Applications

|authentication_methods
|array[string]
a|

|second_authentication_method
|string
a|An optional additional authentication method for MFA. This only works
with SSH as the application. It is ignored for all other applications.

|===

[#owner]
[.api-collapsible-fifth-title]
owner

Owner name and UUID that uniquely identifies the user account.

[cols=3*,options=header]
|===

```

```

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#role]
[.api-collapsible-fifth-title]
role

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Role name

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

|===

//end collapsible .Definitions block

====

[[IDaca281b0f1ec982817d6a72024842e45]]

= Update a user account

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-block]#`/security/accounts/{owner.uuid}/{name}`#

Introduced In: 9.6

Updates a user account. Locks or unlocks a user account and/or updates the role, applications, and/or password for the user account.

== Required parameters

* `name` - Account name to be updated.

* `owner.uuid` - UUID of the SVM housing the user account to be updated.

== Optional parameters

* `applications` - Array of one or more tuples (of application and authentication methods).

* `role` - RBAC role for the user 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 application. Defaults to `none` if not supplied.

* `comment` - Comment for the user account (e.g purpose of this account).

* `locked` - Set to true/false to lock/unlock the account.

* `ldap_fastbind` - Set to true/false to enable LDAP Fastbind Authentication.

== Related ONTAP commands

* `security login create`

* `security login modify`

* `security login password`

* `security login lock`

* `security login unlock`

== Learn more

*

```
xref:{relative_path}security_accounts_owner.uuid_name_endpoint_overview.html[DOC /security/accounts/{owner.uuid}/{name}]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]
```

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```

```
|owner.uuid
|string
|path
|True
a|Account owner UUID
```

```
|name
|string
|path
|True
a|User account name
```

```
|===
```

== Request Body

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|_links
```

```

|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|authentication_methods
|array[string]
a|

|comment
|string
a|Optional comment for the user account.

|ldap_fastbind
|boolean
a|Optional property that specifies the mode of authentication is LDAP
Fastbind.

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|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
a|Optional property that specifies the password hash algorithm used to
generate a hash of the user's password for password matching.

```

```
|public_key
|string
a|Public key for SSH.
```

```
|role
|link:#role[role]
a|
```

```
|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.
```

```
|ssl_ca_certificate
|string
a|SSL certificate for the chain of certificate authorities (CA) that have
signed this user's client certificate.
```

```
|===
```

.Example request

[%collapsible%closed]

=====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": {
    "application": "amqp",
    "authentication_methods": {
    },
    "second_authentication_method": "none"
  },
  "authentication_methods": {
  },
  "comment": "string",
  "name": "joe.smith",
  "owner": {
```

```

    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svml",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "password_hash_algorithm": "sha512",
  "role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "cluster"
}
====

```

== Response

Status: 200, Ok

```

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 1261215
| The role was not found.
| 1261218
| The user was not found.
| 1263343
| Cannot lock user with password not set or non-password authentication
method.
| 5636096

```

| Cannot perform the operation for this user account since the password is not set.

| 5636097
| The operation for user account failed since user password is not set.

| 5636100
| Modification of a service-processor user's role to a non-admin role is not supported.

| 5636125
| The operation not supported on AutoSupport user account which is reserved.

| 5636129
| The role does not exist.

| 5636154
| The second-authentication-method parameter is supported for ssh application.

| 5636155
| The second-authentication-method parameter can be specified only if the authentication-method password or public key nsswitch.

| 5636156
| Same value cannot be specified for the second-authentication-method and the authentication-method.

| 5636157
| If the authentication-method is domain, the second-authentication-method cannot be specified.

| 5636159
| For a given user and application, if the second-authentication-method is specified, only one such login entry is supported.

| 5636164
| If the value for either the authentication-method second-authentication-method is nsswitch or password, the other parameter must differ.

| 5636197
| LDAP fastbind combination for application and authentication method is not supported.

| 5636198
| LDAP fastbind authentication is supported only for nsswitch.

```
| 7077896
| Cannot lock the account of the last console admin user.

| 7077906
| A role with that name has not been defined for the Vserver.

| 7077911
| The user is not configured to use the password authentication method.

| 7077918
| The password cannot contain the username.

| 7077919
| The minimum length for new password does not meet the policy.

| 7077920
| The new password must have both letters and numbers.

| 7077921
| The minimum number of special characters required do not meet the
policy.

| 7077924
| The new password must be different than last N passwords.

| 7077925
| The new password must be different to the old password.

| 7077929
| Cannot lock user with password not set or non-password authentication
method.

| 7077940
| The password exceeds maximum supported length.

| 7077941
| Defined password composition exceeds the maximum password length of 128
characters.

| 7078900
| An aAdmin password is not set. Set the password by including it in the
request.
|===
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_application]
[.api-collapsible-fifth-title]
account_application

[cols=3*,options=header]
|===
|Name
|Type
|Description

|application
|string
a|Applications

|authentication_methods
|array[string]
a|

|second_authentication_method
|string
a|An optional additional authentication method for MFA. This only works
with SSH as the application. It is ignored for all other applications.

```



```
|===
```

```
[#owner]  
[.api-collapsible-fifth-title]  
owner
```

Owner name and UUID that uniquely identifies the user account.

```
[cols=3*,options=header]  
|===  
|Name  
|Type  
|Description
```

```
|_links  
|link:#_links[_links]  
a|
```

```
|name  
|string  
a|The name of the SVM.
```

```
|uuid  
|string  
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role]  
[.api-collapsible-fifth-title]  
role
```

```
[cols=3*,options=header]  
|===  
|Name  
|Type  
|Description
```

```
|_links  
|link:#_links[_links]
```

```

a|

|name
|string
a|Role name

|===

[#account]
[.api-collapsible-fifth-title]
account

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|authentication_methods
|array[string]
a|

|comment
|string
a|Optional comment for the user account.

|ldap_fastbind
|boolean
a|Optional property that specifies the mode of authentication is LDAP
Fastbind.

|locked
|boolean
a|Locked status of the account.

```

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|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
a|Optional property that specifies the password hash algorithm used to generate a hash of the user's password for password matching.

|public_key
|string
a|Public key for SSH.

|role
|link:#role[role]
a|

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

|ssl_ca_certificate
|string
a|SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

|===

```

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
:leveloffset: -1
```

```
= View suspect files generated by anti-ransomware
```

```
:leveloffset: +1
```

```
[[IDeb2b112b892f2292a85f6ba5660f2252]]
= Security anti-ransomware suspects endpoint overview
```

```
== Retrieving information on suspected files
```

The suspect GET API retrieves a list of recently suspected files potentially attacked by ransomware.

```
[[ID2c506826fec42119275626b714c3db40]]
= Retrieve information on the suspects generated by anti-ransomware analytics
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/anti-ransomware/suspects`#
```

```
*Introduced In:* 9.10
```

Retrieves information on the suspects generated by the anti-ransomware analytics.

== Related ONTAP commands

* `security anti-ransomware volume attack generate-report`

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|file.format

|string

|query

|False

a|Filter by file.format

|file.reason

|string

|query

|False

a|Filter by file.reason

* Introduced in: 9.11

|file.path

|string

|query

|False

a|Filter by file.path

|file.name

|string

|query

|False

a|Filter by file.name

```
|file.suspect_time
|string
|query
|False
a|Filter by file.suspect_time
```

```
|volume.name
|string
|query
|False
a|Filter by volume.name
```

```
|volume.uuid
|string
|query
|False
a|Filter by volume.uuid
```

```
|is_false_positive
|boolean
|query
|False
a|Filter by is_false_positive
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|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

a|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

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


```
|records
|array[link:#anti_ransomware_suspect[anti_ransomware_suspect]]
a|
```

```
|===
```

.Example response

[%collapsible%closed]

```
=====
```

[source,json,subs=+macros]

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "file": {
      "format": "pdf",
      "name": "test_file",
      "path": "d1/d2/d3",
      "reason": "High Entropy",
      "suspect_time": "2021-05-12T11:00:16-04:00"
    },
    "volume": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "volume1",
      "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
    }
  }
}
```

```
=====
```

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

```

```
|===
```

```
[#file]
```

```
[.api-collapsible-fifth-title]
```

```
file
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|format
```

```
|string
```

```
a|File format of the suspected file.
```

```
|name
```

```
|string
```

```
a|Name of the suspected file.
```

```
|path
```

```
|string
```

```
a|Path of the suspected file.
```

```
|reason
```

```
|string
```

```
a|Reason behind this file being suspected
```

```
|suspect_time
```

```
|string
```

```
a|Time when the file was detected as a potential suspect in date-time  
format.
```

```
|===
```

```
[#volume]
```

```
[.api-collapsible-fifth-title]
```

```
volume
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the volume.

|uuid
|string
a|Unique identifier for the volume. This corresponds to the instance-uuid
that is exposed in the CLI and ONTAPI. It does not change due to a volume
move.

* example: 028baa66-41bd-11e9-81d5-00a0986138f7
* Introduced in: 9.6

|===

[#anti_ransomware_suspect]
[.api-collapsible-fifth-title]
anti_ransomware_suspect

File suspected to be potentially attacked by ransomware.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|file
|link:#file[file]

```

```

a|

|is_false_positive
|boolean
a|Specifies whether the suspected ransomware activity is a false positive
or not. This parameter is only used when making a DELETE call.


|volume
|link:#volume[volume]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code


|message
|string
a|Message argument


|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
:leveloffset: -1
```

```
= Delete suspect files
```

```
:leveloffset: +1
```

```
[[ID0b7c93d2f1b9547980b6d7f6d05fd4b8]]
= Security anti-ransomware suspects volume.uuid endpoint overview
```

The suspects DELETE API clears all the suspect files for a volume from the list of potential suspects.

```
[[ID8643c6321241cf9e55b7c9dde800b7fa]]
```

= Clear suspect files of a volume

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/security/anti-ransomware/suspects/{volume.uuid}`#
```

Introduced In: 9.10

Clears either all the suspect files of a volume or suspect files of a volume based on file format or suspect time provided.

== Related ONTAP commands

* `security anti-ransomware volume attack clear-suspect`

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|volume.uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|Identification of the Anti-ransomware suspect file for the deletion.
```

* format: uuid

```
|return_records
```

```
|boolean
```

```
|query
```

```
|False
```

```
a|The default is false. If set to true, the records are returned.
```

* Default value:


```
|return_timeout
|integer
|query
|False
```

a|The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

- * Default value: 1
- * Max value: 120
- * Min value: 0

```
|===
```

```
== Response
```

Status: 202, Accepted

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|job
|link:#job_link[job_link]
a|
```

```
|===
```

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
}
```

```

    "uuid": "string"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#job_link]

```

```
[.api-collapsible-fifth-title]
job_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|The UUID of the asynchronous job that is triggered by a POST, PATCH, or
DELETE operation.

|===

//end collapsible .Definitions block
=====

:leveloffset: -1

= View and update audit settings

:leveloffset: +1

[[ID9bf61b0b567727f03ffe39adafe3d515]]
= Security audit endpoint overview

== Overview

This API controls what is logged to the audit log files. All operations
that make changes are always logged and cannot be disabled. The PATCH
request updates administrative audit settings for GET requests. All fields
are optional for a PATCH request. A GET request retrieves administrative
audit settings for GET requests.
```

```

+

'''

== Examples

=== Retrieving administrative audit settings for GET requests

The following example shows the administrative audit settings for GET
requests.
+

'''

----

# The API:
/api/security/audit

# The call:
curl -X GET "https://<cluster-ip>/api/security/audit"

# The response:
{
  "cli": false,
  "http": false,
  "ontapi": false,
  "_links": {
    "self": {
      "href": "/api/security/audit"
    }
  }
}
----

'''

=== Updating administrative audit settings for GET requests

The following example updates the administrative audit settings for GET
requests
+

'''

----

```

```

# The API:
/api/security/audit

# The call:
curl -X PATCH "https://<cluster-ip>/api/security/audit" -d
'{"cli":"false", "http": "true", "ontapi": "true"}'
----

'''

[[ID06f5dbd5fa1108dae9135a34c29c69d0]]
= Retrieve administrative audit settings for GET requests

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/audit`#

*Introduced In:* 9.6

Retrieves administrative audit settings for GET requests.

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|cli
|boolean
a|Enable auditing of CLI GET Operations. Valid in PATCH

|http
|boolean
a|Enable auditing of HTTP GET Operations. Valid in PATCH

|ontapi
|boolean
a|Enable auditing of ONTAP API GET operations. Valid in PATCH

* Introduced in: 9.6

|snmp
|boolean
a|Enable auditing of SNMP GET operations. Valid in PATCH

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  }
}
```

```

    }
  }
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]

```

```

[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

```



```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
[[ID323f74c1bb9379a46c339f41938c8b80]]
```

= Update administrative audit settings for GET requests

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-block]#`/security/audit`#
```

Introduced In: 9.6

Updates administrative audit settings for GET requests.

All of the fields are optional. An empty body will make no changes.

== Request Body

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|cli
```

```
|boolean
```

```
a|Enable auditing of CLI GET Operations. Valid in PATCH
```

```
|http
```

```
|boolean
```

```
a|Enable auditing of HTTP GET Operations. Valid in PATCH
```

```
|ontapi
```

```
|boolean
```

```
a|Enable auditing of ONTAP API GET operations. Valid in PATCH
```

* Introduced in: 9.6

```
|snmp
```

```
|boolean
```

```
a|Enable auditing of SNMP GET operations. Valid in PATCH
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{  
  "_links": {  
    "self": {  
      "href": "/api/resourcelink"  
    }  
  }  
}
```

```
====
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|cli
```

```
|boolean
```

```
a|Enable auditing of CLI GET Operations. Valid in PATCH
```

```
|http
```

```
|boolean
```

```
a|Enable auditing of HTTP GET Operations. Valid in PATCH
```

```
|ontapi
```

```
|boolean
```

```
a|Enable auditing of ONTAP API GET operations. Valid in PATCH
```

```
* Introduced in: 9.6
```

```
|snmp
|boolean
a|Enable auditing of SNMP GET operations. Valid in PATCH
```

```
|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  }
}
====

== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
```

```

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

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self

```

```

|link:#href[href]
a|

|===

[#security_audit]
[.api-collapsible-fifth-title]
security_audit

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|cli
|boolean
a|Enable auditing of CLI GET Operations. Valid in PATCH

|http
|boolean
a|Enable auditing of HTTP GET Operations. Valid in PATCH

|ontapi
|boolean
a|Enable auditing of ONTAP API GET operations. Valid in PATCH

* Introduced in: 9.6

|snmp
|boolean
a|Enable auditing of SNMP GET operations. Valid in PATCH

|===

[#error_arguments]
[.api-collapsible-fifth-title]

```

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

```

|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Forward audit logs to syslog/splunk servers

:leveloffset: +1

[[IDe26574cbefb5bb9b1b1a8934e9e7f09e]]
= Security audit destinations endpoint overview

== Overview

This API controls the forwarding of audit log information to remote
syslog/splunk servers. Multiple destinations can be configured and all
audit records are forwarded to all destinations.

A GET operation retrieves information about remote syslog/splunk server
destinations.
A POST operation creates a remote syslog/splunk server destination.
A GET operation on /security/audit/destinations/{address}/{port}
retrieves information about the syslog/splunk server destination given its
address and port number.
A PATCH operation on /security/audit/destinations/{address}/{port}
updates information about the syslog/splunk server destination given its
address and port number.
A DELETE operation on /security/audit/destinations/{address}/{port}
deletes a syslog/splunk server destination given its address and port
number.

=== Overview of fields used for creating a remote syslog/splunk
destination

```


The fields used for creating a remote syslog/splunk destination fall into the following categories

==== Required properties

All of the following fields are required for creating a remote syslog/splunk destination

- * `address`

==== Optional properties

All of the following fields are optional for creating a remote syslog/splunk destination

- * `port`
- * `protocol`
- * `facility`
- * `verify_server`

+

'''

== Examples

=== Retrieving remote syslog/splunk server destinations

The following example shows remote syslog/splunk server destinations

+

'''

The API:
/api/security/audit/destinations

The call:
curl -X GET "https://<cluster-ip>/api/security/audit/destinations"

The response:
{
 "records": [
 {
 "address": "1.1.1.1",
 "port": 514,
 "_links": {

```

        "self": {
            "href": "/api/security/audit/destinations/1.1.1.1/514"
        }
    }
},
    "num_records": 1,
    "_links": {
        "self": {
            "href": "/api/security/audit/destinations"
        }
    }
}

```

'''

=== Creating remote syslog/splunk server destinations

The following example creates remote syslog/splunk server destinations.

+

'''

The API:

/api/security/audit/destinations

The call:

```

curl -X POST "https://<cluster-
ip>/api/security/audit/destinations?force=true" -d '{ "address":
"1.1.1.1", "port": 514, "protocol": "udp_unencrypted", "facility":
"kern"}'

```

'''

=== Retrieving a remote syslog/splunk server destination given its destination address and port number

The following example retrieves a remote syslog/splunk server destination given its destination address and port number.

+

'''

```

-----

# The API:
/api/security/audit/destinations/{address}/{port}

# The call:
curl -X GET "https://<cluster-
ip>/api/security/audit/destinations/1.1.1.1/514"

# The response:
{
  "address": "1.1.1.1",
  "port": 514,
  "protocol": "udp_unencrypted",
  "facility": "kern",
  "verify_server": false,
  "_links": {
    "self": {
      "href": "/api/security/audit/destinations/1.1.1.1/514"
    }
  }
}
-----

'''

=== Updating a remote syslog/splunk server destination given its
destination address and port number

The following example updates a remote syslog/splunk server destination
configuration given its destination address and port number.
+

'''

-----

# The API:
/api/security/audit/destinations/{address}/{port}

# The call:
curl -X PATCH "https://<cluster-
ip>/api/security/audit/destinations/1.1.1.1/514" -d '{"facility":
"user"}'

-----

'''

```

=== Deleting a remote syslog/splunk server destination given its destination address and port number

The following example deletes a remote syslog/splunk server destination configuration given its destination address and port number.

+

'''

The API:

/api/security/audit/destinations/{address}/{port}

The call:

curl -X DELETE "https://<cluster-
ip>/api/security/audit/destinations/1.1.1.1/514"

'''

[[IDbd79b9e052170cd2b6353f72e94967b4]]

= Define a remote syslog or splunk server to receive audit information

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/audit/destinations`#

Introduced In: 9.6

Defines a remote syslog/splunk server for sending audit information to.

== Parameters

[cols=5*,options=header]
|===

|Name

|Type

|In

|Required

|Description

```
|protocol
|string
|query
|False
a|Filter by protocol
```

```
|verify_server
|boolean
|query
|False
a|Filter by verify_server
```

```
|facility
|string
|query
|False
a|Filter by facility
```

```
|address
|string
|query
|False
a|Filter by address
```

```
|port
|integer
|query
|False
a|Filter by port
```

```
|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.
```

```
|fields
|array[string]
|query
```

```

|False
a|Specify the fields to return.

|max_records
|integer
|query
|False
a|Limit the number of records returned.

|return_timeout
|integer
|query
|False
a|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

|return_records
|boolean
|query
|False
a|The default is true for GET calls.  When set to false, only the number
of records is returned.

* Default value: 1

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#security_audit_log_forward[security_audit_log_forward]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "facility": "kern",
    "protocol": "udp_unencrypted"
  }
}
=====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```



```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#security_audit_log_forward]
[.api-collapsible-fifth-title]
security_audit_log_forward

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string

```

a|This is the standard Syslog Facility value that is used when sending audit records to a remote server.

|port

|integer

a|Destination Port. The default port depends on the protocol chosen:

For un-encrypted destinations the default port is 514.

For encrypted destinations the default port is 6514.

|protocol

|string

a|Log forwarding protocol

|verify_server

|boolean

a|This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID04a084d8b741b4b38d7289a187013f8d]]
= Define remote syslog or splunk server information

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/audit/destinations`#

```

Introduced In: 9.6

Configures remote syslog/splunk server information.

== Required properties

All of the following fields are required for creating a remote syslog/splunk destination

* `address`

== Optional properties

All of the following fields are optional for creating a remote syslog/splunk destination

* `port`

* `protocol`

* `facility`

* `verify_server` (Can only be "true" when protocol is "tcp_encrypted")

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|force

|boolean

|query

|False

a|Skip the Connectivity Test

* Default value:

|return_timeout

|integer

|query

|False

a|The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

- * Default value: 1
- * Max value: 120
- * Min value: 0

|return_records
|boolean
|query
|False

a|The default is false. If set to true, the records are returned.

- * Default value:

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string

a|Destination syslog\|splunk host to forward audit records to. This can be an IP address (IPv4\|IPv6) or a hostname.

|facility
|string

a|This is the standard Syslog Facility value that is used when sending audit records to a remote server.

|port
|integer

a|Destination Port. The default port depends on the protocol chosen:

For un-encrypted destinations the default port is 514.

For encrypted destinations the default port is 6514.

|protocol

|string

a|Log forwarding protocol

|verify_server

|boolean

a|This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "facility": "kern",
  "protocol": "udp_unencrypted"
}
```

====

== Response

Status: 202, Accepted

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#security_audit_log_forward[security_audit_log_forward]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "facility": "kern",
    "protocol": "udp_unencrypted"
  }
}
=====

== Error

```

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 15661

| The object specified could not be found

| 13114

| Internal error

| 13115

| Invalid input

| 4522285

| Server verification cannot be enabled because it requires a protocol with encryption. Encryption can be selected using the protocol field.

| 9240603

| Cannot ping destination host. Verify connectivity to desired host or skip the connectivity check with the -force parameter.

| 327698

| Failed to create RPC client to destination host

| 9240609

| Cannot connect to destination host.

| 9240604

| Cannot resolve the destination host.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===


```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====
```

== Definitions

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#security_audit_log_forward]
[.api-collapsible-fifth-title]
security_audit_log_forward

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.
```

```

|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce
validation of remote server's certificate.

|===

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===

```

```

|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[ID6cfacfd0c96cf6816ac86f18a3886d54]]
= Delete remote syslog or splunk server information
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/audit/destinations/{address}/{port}`#
```

***Introduced In:** 9.6

Deletes remote syslog/splunk server information.

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
```

```

|In
|Required
|Description

|address
|string
|path
|True
a|IP address of remote syslog/splunk server.

|port
|integer
|path
|True
a|Port number of remote syslog/splunk server.

|===

== Response

```

Status: 200, Ok

```

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{

```

```

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

```

====

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

====

```

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

```

|===

```

[#error]
[.api-collapsible-fifth-title]
error

```

```

[cols=3*,options=header]

```

```

|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====

[[ID44d596f0d2b63f3ae9d9f41733b6c08e]]
= Retrieve remote syslog or splunk server information


[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/audit/destinations/{address}/{port}`#


*Introduced In:* 9.6


Defines a remote syslog/splunk server for sending audit information to.


== Parameters


[cols=5*,options=header]

```

```

|===

|Name
|Type
|In
|Required
|Description

|address
|string
|path
|True
a|IP address of remote syslog/splunk server.

|port
|integer
|path
|True
a|Port number of remote syslog/splunk server.

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

```



```
|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.
```

```
|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.
```

```
|protocol
|string
a|Log forwarding protocol
```

```
|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce
validation of remote server's certificate.
```

```
|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "facility": "kern",
  "protocol": "udp_unencrypted"
}
=====
```

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
```

```

|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code

```

```

|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```

[[ID15412191bec72743ef5e19f44f7eddf2]]
= Update remote syslog or splunk server information

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/audit/destinations/{address}/{port}`#

*Introduced In:* 9.6

Updates remote syslog/splunk server information.

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|address
|string
|path
|True
a|IP address of remote syslog/splunk server.

|port
|integer
|path
|True
a|Port number of remote syslog/splunk server.

|===

== Request Body

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.

|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce
validation of remote server's certificate.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "facility": "kern",
  "protocol": "udp_unencrypted"
}

```

```
====
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.

|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce
validation of remote server's certificate.

|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "facility": "kern",
  "protocol": "udp_unencrypted"
}
====

== Error
```

Status: Default, Default

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====
```

```

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#security_audit_log_forward]
[.api-collapsible-fifth-title]
security_audit_log_forward

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.

|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce

```


validation of remote server's certificate.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

|===

|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
:leveloffset: -1
```

```
= View administrative audit logs
```

```
:leveloffset: +1
```

```
[[IDc19be02bdfcb6fac0973d48627f4947b]]
= Security audit messages endpoint overview
```

```
== Overview
```

These APIs return audit log records. The GET requests retrieves all audit log records. An audit log record contains information such as timestamp, node name, index and so on.

+

'''

```
== Example
```

```
=== Retrieving audit log records
```

The following example shows the audit log records.

```

+

'''

----

# The API:
/api/security/audit/messages

# The call:
curl -X GET "https://<cluster-ip>/api/security/audit/messages"

# The response:
{
  "records": [
    {
      "timestamp": "2019-03-08T11:03:32-05:00",
      "node": {
        "name": "node1",
        "uuid": "bc9af9da-41bb-11e9-a3db-005056bb27cf",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/bc9af9da-41bb-11e9-a3db-005056bb27cf"
          }
        }
      },
      "index": 4294967299,
      "application": "http",
      "location": "172.21.16.89",
      "user": "admin",
      "input": "GET /api/security/audit/destinations/",
      "state": "pending",
      "scope": "cluster"
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/audit/messages"
    }
  }
}

----

'''

```

```
[[ID094b94d6d4e171c8c5e46a9b9a7c8a78]]  
= Retrieve administrative audit log viewer
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/audit/messages`#
```

Introduced In: 9.6

Retrieves the administrative audit log viewer.

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|session_id
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by session_id
```

```
|message
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by message
```

```
|scope
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by scope
```

```
|svm.name  
|string  
|query  
|False  
a|Filter by svm.name
```

```
|timestamp  
|string  
|query  
|False  
a|Filter by timestamp
```

```
|command_id  
|string  
|query  
|False  
a|Filter by command_id
```

```
|state  
|string  
|query  
|False  
a|Filter by state
```

```
|node.uuid  
|string  
|query  
|False  
a|Filter by node.uuid
```

```
|node.name  
|string  
|query  
|False  
a|Filter by node.name
```

```
|application  
|string  
|query  
|False  
a|Filter by application
```

```
|input
|string
|query
|False
a|Filter by input
```

```
|user
|string
|query
|False
a|Filter by user
```

```
|location
|string
|query
|False
a|Filter by location
```

```
|index
|integer
|query
|False
a|Filter by index
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_timeout
|integer
|query
```

```

|False
a|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

|return_records
|boolean
|query
|False
a|The default is true for GET calls.  When set to false, only the number
of records is returned.

* Default value: 1

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer

```

a|Number of records

```
|records
|array[link:#security_audit_log[security_audit_log]]
a|
```

|===

.Example response

[%collapsible%closed]

=====

[source,json,subs=+macros]

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    },
    "application": "internal",
    "command_id": "string",
    "index": 0,
    "input": "string",
    "location": "string",
    "message": "string",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "scope": "svm",
    "session_id": "string",
```



```

    "state": "pending",
    "timestamp": "string",
    "user": "string"
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]

```

```

//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|====
|Name
|Type
|Description

|href
|string
a|

|====

[#\_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name
|Type
|Description

|next
|link:#href\[href\]
a|

|self
|link:#href\[href\]
a|

|====

[#\_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name

```

```
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

Node where the audit message resides.
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|
```

```
|uuid
|string
a|
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

This is the SVM through which the user connected.

```
[cols=3*,options=header]
|===
```

```

|Name
|Type
|Description

|name
|string
a|

|===

[#security_audit_log]
[.api-collapsible-fifth-title]
security_audit_log

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|application
|string
a|This identifies the "application" by which the request was processed.

|command_id
|string
a|This is the command ID for this request.
Each command received on a CLI session is assigned a command ID. This
enables you to correlate a request and response.

|index
|integer
a|Internal index for accessing records with same time/node. This is a 64
bit unsigned value.

|input
|string
a|The request.

```

```
|location
|string
a|This identifies the location of the remote user. This is an IP address
or "console".

|message
|string
a|This is an optional field that might contain "error" or "additional
information" about the status of a command.

|node
|link:#node[node]
a|Node where the audit message resides.

|scope
|string
a|Set to "svm" when the request is on a data SVM; otherwise set to
"cluster".

|session_id
|string
a|This is the session ID on which the request is received. Each SSH
session is assigned a session ID.
Each http/ontapi/snmp request is assigned a unique session ID.

|state
|string
a|State of of this request.

|svm
|link:#svm[svm]
a|This is the SVM through which the user connected.

|timestamp
|string
a|Log entry timestamp. Valid in URL

|user
```

```
|string
a|Username of the remote user.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```

```
[#error]
```

```
[.api-collapsible-fifth-title]
```

```
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|arguments
```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```

a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage data SVM account information

:leveloffset: +1

[[ID7aeb38fe07f8fa2b80d7b3999ca29023]]
= Security authentication cluster ad-proxy endpoint overview

== Overview

This API configures data SVM account information at the Active Directory.
For Active Directory domain-based authentication for cluster accounts, a
data SVM must be configured and registered as a machine account at the
Active Directory. All authentication requests are proxied through this
SVM.

== Examples

=== Creating a data SVM proxy for domain-based authentication for cluster
accounts

```

```

-----

# The API:
POST "/api/security/authentication/cluster/ad-proxy"

# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/ad-
proxy" -d '{"svm.uuid":"13f87d78-70c7-11e9-b722-0050568ec89f"}'
-----

=== Updating a data SVM proxy for domain-based authentication for cluster
accounts

-----

# The API:
PATCH "/api/security/authentication/cluster/ad-proxy"

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/ad-
proxy" -d '{"svm.uuid":"13f87d78-70c7-11e9-b722-0050568ec89f"}'
-----

=== Retrieving a data SVM proxy for domain-based authentication for
cluster accounts

-----

# The API:
GET "/api/security/authentication/cluster/ad-proxy"

# The call:
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/ad-
proxy"

# The response:
{
  "svm": {
    "uuid": "512eab7a-6bf9-11e9-a896-005056bb9ce1",
    "name": "vs2",
    "_links": {
      "self": {
        "href": "/api/svm/svms/512eab7a-6bf9-11e9-a896-005056bb9ce1"
      }
    }
  },
  "_links": {

```



```
"self": {
  "href": "/api/security/authentication/cluster/ad-proxy"
}
}
}
----
```

```
[[ID70ff53a3463abead8623d563846977b8]]
= Delete a data SVM configured as a tunnel
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/cluster/ad-proxy`#
```

Introduced In: 9.7

Deletes the data SVM configured as a tunnel for Active Directory based authentication for cluster user accounts.

== Related ONTAP commands

* `security login domain-tunnel delete`

== Learn more

* xref:{relative_path}security_authentication_cluster_ad-
proxy_endpoint_overview.html[DOC /security/authentication/cluster/ad-
proxy]

* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

== Response

Status: 200, Ok

== Error

Status: Default, Error

```
[cols=3*,options=header]
|===
```

```

|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code

```

```

|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
[[IDd4a75cd6b4e4daae234c3acae4d8214a]]
= Retrieve SVM information configured as an Active Directory domain-tunnel

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/ad-proxy`#

*Introduced In:* 9.7

Retrieves SVM information configured as an Active Directory domain-tunnel.

== Related ONTAP commands

* `security login domain-tunnel show`

== Learn more

* xref:{relative_path}security_authentication_cluster_ad-
proxy_endpoint_overview.html[DOC /security/authentication/cluster/ad-
proxy]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|svm
|link:#svm[svm]
a|
```

```
|===
```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

====

== Error

Status: Default, Error

```
[cols=3*,options=header]
|===
```

```

|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href

```

```

|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

```

```
|===
```

```
[#error_arguments]  
[.api-collapsible-fifth-title]  
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|code  
|string  
a|Argument code
```

```
|message  
|string  
a|Message argument
```

```
|===
```

```
[#error]  
[.api-collapsible-fifth-title]  
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|arguments  
|array[link:#error_arguments[error_arguments]]  
a|Message arguments
```

```
|code  
|string  
a|Error code
```

```
|message
```



```

|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID8166b7413c8dafab43e5f5c3aa912c2f]]
= Update a data SVM configured as a tunnel

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/authentication/cluster/ad-proxy`#

*Introduced In:* 9.7

Updates the data SVM configured as a tunnel for Active Directory based
authentication for cluster user accounts.

== Related ONTAP commands

* `security login domain-tunnel modify`

== Learn more

* xref:{relative_path}security_authentication_cluster_ad-
proxy_endpoint_overview.html[DOC /security/authentication/cluster/ad-
proxy]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

== Request Body

[cols=3*,options=header]
|===

```

```
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|
```

```
|svm
|link:#svm[svm]
a|
```

```
|===
```

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

====

== Response

Status: 200, Ok

== Error

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

```

```
|===
```

```
[#cluster_ad_proxy]  
[.api-collapsible-fifth-title]  
cluster_ad_proxy
```

The SVM configured as proxy for Active Directory authentication of cluster accounts.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|_links  
|link:#_links[_links]  
a|
```

```
|svm  
|link:#svm[svm]  
a|
```

```
|===
```

```
[#error_arguments]  
[.api-collapsible-fifth-title]  
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|code  
|string  
a|Argument code
```

```
|message  
|string  
a|Message argument
```

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID15a4f6a346dd7813dd0479d21a79f1ee]]
= Configure a data SVM as a proxy

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
```

```
block]#`/security/authentication/cluster/ad-proxy`#
```

Introduced In: 9.7

Configures a data SVM as a proxy for Active Directory based authentication for cluster user accounts.

== Required properties

* `svm.name` or `svm.uuid` - Name and UUID of the SVM for a cluster user account.

== Related ONTAP commands

* `security login domain-tunnel create`

== Learn more

* xref:{relative_path}security_authentication_cluster_ad-proxy_endpoint_overview.html[DOC /security/authentication/cluster/ad-proxy]

* xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]

== Request Body

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|svm
```

```
|link:#svm[svm]
```

```
a|
```

```
|===
```

.Example request

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
====

== Response
```

Status: 201, Created

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
```



```

[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type

```

```
|Description
```

```
|self
```

```
|link:#href[href]
```

```
a|
```

```
|===
```

```
[#svm]
```

```
[.api-collapsible-fifth-title]
```

```
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#cluster_ad_proxy]
```

```
[.api-collapsible-fifth-title]
```

```
cluster_ad_proxy
```

The SVM configured as proxy for Active Directory authentication of cluster accounts.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```

|Type
|Description

|_links
|link:#_links[_links]
a|

|svm
|link:#svm[svm]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage LDAP server configuration

:leveloffset: +1

[[ID0b462c11511fac3397bb078627721e1a]]
= Security authentication cluster LDAP endpoint overview

== Overview

LDAP servers are used to centrally maintain user information. LDAP
configurations must be set up
to look up information stored in the LDAP directory on the external LDAP
servers. This API is used to retrieve and manage

```

cluster LDAP server configurations.

== Examples

=== Retrieving the cluster LDAP information

The cluster LDAP GET request retrieves the LDAP configuration of the cluster.

The following example shows how a GET request is used to retrieve the cluster LDAP information:

The API:

/api/security/authentication/cluster/ldap

The call:

```
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/ldap"  
-H "accept: application/hal+json"
```

The response:

```
{  
  "servers": [  
    "10.10.10.10",  
    "domainB.example.com"  
  ],  
  "schema": "ad_idmu",  
  "port": 389,  
  "min_bind_level": "anonymous",  
  "bind_dn": "cn=Administrators,cn=users,dc=domainA,dc=example,dc=com",  
  "base_dn": "dc=domainA,dc=example,dc=com",  
  "base_scope": "subtree",  
  "use_start_tls": true,  
  "session_security": "none",  
  "try_channel_binding": true,  
  "_links": {  
    "self": {  
      "href": "/api/security/authentication/cluster/ldap"  
    }  
  }  
}
```

=== Creating the cluster LDAP configuration

The cluster LDAP POST operation creates an LDAP configuration for the

cluster.

The following example shows how to issue a POST request with all of the fields specified:

The API:

/api/security/authentication/cluster/ldap

The call:

```
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/hal+json" -H "Content-Type: application/json" -d
"{ \"servers\": [ \"10.10.10.10\", \"domainB.example.com\" ], \"schema\":
\"ad_idmu\", \"port\": 389, \"min_bind_level\": \"anonymous\",
\"bind_dn\": \"cn=Administrators,cn=users,dc=domainA,dc=example,dc=com\",
\"bind_password\": \"abc\", \"base_dn\": \"dc=domainA,dc=example,dc=com\",
\"base_scope\": \"subtree\", \"use_start_tls\": false,
\"session_security\": \"none\"}"
```

The following example shows how to issue a POST request with a number of optional fields not specified:

The API:

/api/security/authentication/cluster/ldap

The call:

```
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/hal+json" -H "Content-Type: application/json" -d
"{ \"port\": 389, \"bind_dn\":
\"cn=Administrators,cn=users,dc=domainA,dc=example,dc=com\",
\"bind_password\": \"abc\", \"base_dn\": \"dc=domainA,dc=example,dc=com\",
\"session_security\": \"none\"}"
```

=== Updating the cluster LDAP configuration

The cluster LDAP PATCH request updates the LDAP configuration of the cluster.

The following example shows how a PATCH request is used to update the cluster LDAP configuration:

```

# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\"servers\": [ \"55.55.55.55\" ], \"schema\": \"ad_idmu\", \"port\": 636,
\"use_start_tls\": false }"
-----

=== Deleting the cluster LDAP configuration

The cluster LDAP DELETE request deletes the LDAP configuration of the
cluster.

The following example shows how a DELETE request is used to delete the
cluster LDAP configuration:

-----

# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X DELETE "https://<mgmt-
ip>/api/security/authentication/cluster/ldap" -H "accept:
application/hal+json"
-----

[[ID23eb68c23da31890d218623ada6947f2]]
= Delete the LDAP configuration for the cluster

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/cluster/ldap`#

*Introduced In:* 9.6

Deletes the LDAP configuration of the cluster.

== Response

```

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
```


error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

```

|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID267d98138ccc9f2a9b4ea7ae574fe3c2]]
= Retrieve the LDAP configuration for the cluster

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/ldap`#

*Introduced In:* 9.6

Retrieves the cluster LDAP configuration.

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|base_dn
|string
a|Specifies the default base DN for all searches.

|base_scope
|string
a|Specifies the default search scope for LDAP queries:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|bind_as_cifs_server
|boolean
a|Specifies whether or not CIFS server's credentials are used to bind to
the LDAP server.

|bind_dn
|string
a|Specifies the user that binds to the LDAP servers.

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|group_dn
|string
a|Specifies the group Distinguished Name (DN) that is used as the starting
point in the LDAP directory tree for group lookups.

|group_membership_filter

```

```

|string
a|Specifies the custom filter used for group membership lookups from an
LDAP server.

|group_scope
|string
a|Specifies the default search scope for LDAP for group lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|is_netgroup_byhost_enabled
|boolean
a|Specifies whether or not netgroup by host querying is enabled.

|is_owner
|boolean
a|Specifies whether or not the SVM owns the LDAP client configuration.

|ldaps_enabled
|boolean
a|Specifies whether or not LDAPS is enabled.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|netgroup_byhost_dn
|string
a|Specifies the netgroup Distinguished Name (DN) that is used as the
starting point in the LDAP directory tree for netgroup by host lookups.

|netgroup_byhost_scope
|string
a|Specifies the default search scope for LDAP for netgroup by host

```

```

lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|netgroup_dn
|string
a|Specifies the netgroup Distinguished Name (DN) that is used as the
starting point in the LDAP directory tree for netgroup lookups.

|netgroup_scope
|string
a|Specifies the default search scope for LDAP for netgroup lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|port
|integer
a|The port used to connect to the LDAP Servers.

|query_timeout
|integer
a|Specifies the maximum time to wait for a query response from the LDAP
server, in seconds.

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

```

```

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic


|skip_config_validation
|boolean
a|Indicates whether or not the validation for the specified LDAP
configuration is disabled.


|status
|link:#status[status]
a|


|try_channel_binding
|boolean
a|Specifies whether or not channel binding is attempted in the case of
TLS/LDAPS.


|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.


|user_dn
|string
a|Specifies the user Distinguished Name (DN) that is used as the starting
point in the LDAP directory tree for user lookups.


|user_scope
|string
a|Specifies the default search scope for LDAP for user lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN


|===

```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_scope": "base",
  "group_scope": "base",
  "min_bind_level": "anonymous",
  "netgroup_byhost_scope": "base",
  "netgroup_scope": "base",
  "port": 389,
  "servers": {
  },
  "session_security": "none",
  "status": {
    "code": 65537300,
    "dn_message": {
    },
    "state": "up"
  },
  "user_scope": "base"
}
====

== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|
```

```

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]

```



```

_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#status]
[.api-collapsible-fifth-title]
status

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message.

|dn_message
|array[string]
a|

|message
|string
a|Provides additional details on the status of the LDAP service.

|state
|string
a|Specifies the status of the LDAP service.

|===

```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[IDde87648f129d199ed03794e34bb708e5]]
= Update the LDAP configuration for the cluster
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/authentication/cluster/ldap`#
```

Introduced In: 9.6

Both mandatory and optional parameters of the LDAP configuration can be updated.

IPv6 must be enabled if IPv6 family addresses are specified. Configuring more than one LDAP server is recommended to avoid a single point of failure. Both FQDNs and IP addresses are supported for the `servers` property.

The LDAP servers are validated as part of this operation. LDAP validation fails in the following scenarios:

- . The server does not have LDAP installed.
- . The server is invalid.
- . The server is unreachable.

== Request Body

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|base_dn
```

```
|string
```

```
a|Specifies the default base DN for all searches.
```

```
|base_scope
```

```
|string
```

```
a|Specifies the default search scope for LDAP queries:
```

```
* base - search the named entry only
```

```
* onelevel - search all entries immediately below the DN
```

```
* subtree - search the named DN entry and the entire subtree below the DN
```

```
|bind_as_cifs_server
```

```
|boolean
```

```
a|Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.
```

```
|bind_dn
```

```
|string
```

```
a|Specifies the user that binds to the LDAP servers.
```

```
|bind_password
```

```
|string
```

```
a|Specifies the bind password for the LDAP servers.
```

```
|group_dn
```

```
|string
```

```
a|Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups.
```

```
|group_membership_filter
```

```
|string
```

```
a|Specifies the custom filter used for group membership lookups from an LDAP server.
```

```
|group_scope
```

```
|string
```

```

a|Specifies the default search scope for LDAP for group lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|is_netgroup_byhost_enabled
|boolean
a|Specifies whether or not netgroup by host querying is enabled.

|is_owner
|boolean
a|Specifies whether or not the SVM owns the LDAP client configuration.

|ldaps_enabled
|boolean
a|Specifies whether or not LDAPS is enabled.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|netgroup_byhost_dn
|string
a|Specifies the netgroup Distinguished Name (DN) that is used as the
starting point in the LDAP directory tree for netgroup by host lookups.

|netgroup_byhost_scope
|string
a|Specifies the default search scope for LDAP for netgroup by host
lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

```

```

|netgroup_dn
|string
a|Specifies the netgroup Distinguished Name (DN) that is used as the
starting point in the LDAP directory tree for netgroup lookups.

|netgroup_scope
|string
a|Specifies the default search scope for LDAP for netgroup lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|port
|integer
a|The port used to connect to the LDAP Servers.

|query_timeout
|integer
a|Specifies the maximum time to wait for a query response from the LDAP
server, in seconds.

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic

```

* seal - seal and sign LDAP traffic

|skip_config_validation
|boolean

a|Indicates whether or not the validation for the specified LDAP configuration is disabled.

|status
|link:#status[status]
a|

|try_channel_binding
|boolean

a|Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.

|use_start_tls
|boolean

a|Specifies whether or not to use Start TLS over LDAP connections.

|user_dn
|string

a|Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups.

|user_scope
|string

a|Specifies the default search scope for LDAP for user lookups:

* base - search the named entry only

* onelevel - search all entries immediately below the DN

* subtree - search the named DN entry and the entire subtree below the DN

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

{

```

"_links": {
  "self": {
    "href": "/api/resourcelink"
  }
},
"base_scope": "base",
"group_scope": "base",
"min_bind_level": "anonymous",
"netgroup_byhost_scope": "base",
"netgroup_scope": "base",
"port": 389,
"servers": {
},
"session_security": "none",
"status": {
  "code": 65537300,
  "dn_message": {
  },
  "state": "up"
},
"user_scope": "base"
}
====

```

== Response

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```

|====
| Error Code | Description
|
| 4915203
| The specified LDAP schema does not exist.
|
| 4915208
| The specified LDAP servers contain duplicate server entries.
|
| 4915229
| DNS resolution failed due to an internal error. Contact technical

```


support if this issue persists.

| 4915231
| DNS resolution failed for one or more of the specified LDAP servers.
Verify that a valid DNS server is configured.

| 23724132
| DNS resolution failed for all the specified LDAP servers. Verify that a
valid DNS server is configured.

| 4915234
| Specified LDAP server is not supported because it is one of the
following: multicast, loopback, 0.0.0.0, or broadcast.

| 4915248
| LDAP servers cannot be empty or "-". Specified FQDN is not valid because
it is empty or "-" or it contains either special characters or "-" at the
start or end of the domain.

| 4915251
| STARTTLS and LDAPS cannot be used together

| 4915257
| The LDAP configuration is not valid. Verify that the Distinguished Names
and bind password are correct.

| 4915258
| The LDAP configuration is not valid. Verify that the servers are
reachable and that the network configuration is correct.

| 23724130
| Cannot use an IPv6 name server address because there are no IPv6
interfaces.

| 4915252
| LDAP referral is not supported with STARTTLS, with session security
levels sign, seal or with LDAPS.
|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

```

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#status]
[.api-collapsible-fifth-title]
status

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message.

|dn_message
|array[string]
a|

|message
|string
a|Provides additional details on the status of the LDAP service.

|state
|string
a|Specifies the status of the LDAP service.

```

```

|===

[#cluster_ldap]
[.api-collapsible-fifth-title]
cluster_ldap

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|base_dn
|string
a|Specifies the default base DN for all searches.

|base_scope
|string
a|Specifies the default search scope for LDAP queries:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|bind_as_cifs_server
|boolean
a|Specifies whether or not CIFS server's credentials are used to bind to
the LDAP server.

|bind_dn
|string
a|Specifies the user that binds to the LDAP servers.

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

```

```

|group_dn
|string
a|Specifies the group Distinguished Name (DN) that is used as the starting
point in the LDAP directory tree for group lookups.

|group_membership_filter
|string
a|Specifies the custom filter used for group membership lookups from an
LDAP server.

|group_scope
|string
a|Specifies the default search scope for LDAP for group lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|is_netgroup_byhost_enabled
|boolean
a|Specifies whether or not netgroup by host querying is enabled.

|is_owner
|boolean
a|Specifies whether or not the SVM owns the LDAP client configuration.

|ldaps_enabled
|boolean
a|Specifies whether or not LDAPS is enabled.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|netgroup_byhost_dn
|string

```

a|Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups.

|netgroup_byhost_scope

|string

a|Specifies the default search scope for LDAP for netgroup by host lookups:

- * base - search the named entry only
- * onelevel - search all entries immediately below the DN
- * subtree - search the named DN entry and the entire subtree below the DN

|netgroup_dn

|string

a|Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.

|netgroup_scope

|string

a|Specifies the default search scope for LDAP for netgroup lookups:

- * base - search the named entry only
- * onelevel - search all entries immediately below the DN
- * subtree - search the named DN entry and the entire subtree below the DN

|port

|integer

a|The port used to connect to the LDAP Servers.

|query_timeout

|integer

a|Specifies the maximum time to wait for a query response from the LDAP server, in seconds.

|schema

|string

a|The name of the schema template used by the SVM.

- * AD-IDMU - Active Directory Identity Management for UNIX
- * AD-SFU - Active Directory Services for UNIX
- * MS-AD-BIS - Active Directory Identity Management for UNIX

* RFC-2307 - Schema based on RFC 2307

* Custom schema

|servers

|array[string]

a|

|session_security

|string

a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing

* sign - sign LDAP traffic

* seal - seal and sign LDAP traffic

|skip_config_validation

|boolean

a|Indicates whether or not the validation for the specified LDAP configuration is disabled.

|status

|link:#status[status]

a|

|try_channel_binding

|boolean

a|Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.

|use_start_tls

|boolean

a|Specifies whether or not to use Start TLS over LDAP connections.

|user_dn

|string

a|Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups.

|user_scope

|string

a|Specifies the default search scope for LDAP for user lookups:

- * base - search the named entry only
- * onelevel - search all entries immediately below the DN
- * subtree - search the named DN entry and the entire subtree below the DN

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

|===

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```



```

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[IDd3e7dbb1094b48f0dafdbb386b7205d1]]
= Create the LDAP configuration for the cluster

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/cluster/ldap`#

*Introduced In:* 9.6

A cluster can have only one LDAP configuration. IPv6 must be enabled if
IPv6 family addresses are specified.

== Required properties

* `servers` - List of LDAP servers used for this client configuration.
* `bind_dn` - Specifies the user that binds to the LDAP servers.
* `base_dn` - Specifies the default base DN for all searches.

== Recommended optional properties

* `schema` - Schema template name.
* `port` - Port used to connect to the LDAP Servers.
* `ldaps_enabled` - Specifies whether or not LDAPS is enabled.
* `min_bind_level` - Minimum bind authentication level.
* `bind_password` - Specifies the bind password for the LDAP servers.

```

- * ``base_scope`` - Specifies the default search scope for LDAP queries.
- * ``use_start_tls`` - Specifies whether or not to use Start TLS over LDAP connections.
- * ``session_security`` - Specifies the level of security to be used for LDAP communications.
- * ``bind_as_cifs_server`` - Indicates if CIFS server's credentials are used to bind to the LDAP server.
- * ``query_timeout`` - Maximum time to wait for a query response from the LDAP server, in seconds.
- * ``user_dn`` - User Distinguished Name (DN) used as the starting point in the LDAP directory tree for user lookups.
- * ``user_scope`` - Default search scope for LDAP for user lookups.
- * ``group_dn`` - Group Distinguished Name (DN) used as the starting point in the LDAP directory tree for group lookups.
- * ``group_scope`` - Default search scope for LDAP for group lookups.
- * ``netgroup_dn`` - Netgroup Distinguished Name (DN) used as the starting point in the LDAP directory tree for netgroup lookups.
- * ``netgroup_scope`` - Default search scope for LDAP for netgroup lookups.
- * ``netgroup_byhost_dn`` - Netgroup Distinguished Name (DN) used as the starting point in the LDAP directory tree for netgroup by host lookups.
- * ``netgroup_byhost_scope`` - Default search scope for LDAP for netgroup by host lookups.
- * ``is_netgroup_byhost_enabled`` - Specifies whether netgroup by host querying is enabled.
- * ``group_membership_filter`` - Custom filter used for group membership lookup from an LDAP server.
- * ``skip_config_validation`` - Indicates whether or not the validation for the specified LDAP configuration is disabled.

== Default property values

- * ``schema`` - `_RFC-2307_`
- * ``port`` - `_389_`
- * ``ldaps_enabled`` - `_false_`
- * ``min_bind_level`` - `_simple_`
- * ``base_scope`` - `_subtree_`
- * ``use_start_tls`` - `_false_`
- * ``session_security`` - `_none_`
- * ``query_timeout`` - `_3_`
- * ``user_scope`` - `_subtree_`
- * ``group_scope`` - `_subtree_`
- * ``netgroup_scope`` - `_subtree_`
- * ``netgroup_byhost_scope`` - `_subtree_`
- * ``is_netgroup_byhost_enabled`` - `_false_`
- * ``skip_config_validation`` - `_false_`
- * ``try_channel_binding`` - `_true_`

Configuring more than one LDAP server is recommended to avoid a single point of failure. Both FQDNs and IP addresses are supported for the `servers` property.

The LDAP servers are validated as part of this operation. LDAP validation fails in the following scenarios:

- . The server does not have LDAP installed.
- . The server is invalid.
- . The server is unreachable.

== Request Body

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|base_dn
```

```
|string
```

```
a|Specifies the default base DN for all searches.
```

```
|base_scope
```

```
|string
```

```
a|Specifies the default search scope for LDAP queries:
```

```
* base - search the named entry only
```

```
* onelevel - search all entries immediately below the DN
```

```
* subtree - search the named DN entry and the entire subtree below the DN
```

```
|bind_as_cifs_server
```

```
|boolean
```

```
a|Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.
```

```
|bind_dn
```

```

|string
a|Specifies the user that binds to the LDAP servers.

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|group_dn
|string
a|Specifies the group Distinguished Name (DN) that is used as the starting
point in the LDAP directory tree for group lookups.

|group_membership_filter
|string
a|Specifies the custom filter used for group membership lookups from an
LDAP server.

|group_scope
|string
a|Specifies the default search scope for LDAP for group lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|is_netgroup_byhost_enabled
|boolean
a|Specifies whether or not netgroup by host querying is enabled.

|is_owner
|boolean
a|Specifies whether or not the SVM owns the LDAP client configuration.

|ldaps_enabled
|boolean
a|Specifies whether or not LDAPS is enabled.

|min_bind_level
|string

```

a|The minimum bind authentication level. Possible values are:

- * anonymous - anonymous bind
- * simple - simple bind
- * sasl - Simple Authentication and Security Layer (SASL) bind

|netgroup_byhost_dn

|string

a|Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups.

|netgroup_byhost_scope

|string

a|Specifies the default search scope for LDAP for netgroup by host lookups:

- * base - search the named entry only
- * onelevel - search all entries immediately below the DN
- * subtree - search the named DN entry and the entire subtree below the DN

|netgroup_dn

|string

a|Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.

|netgroup_scope

|string

a|Specifies the default search scope for LDAP for netgroup lookups:

- * base - search the named entry only
- * onelevel - search all entries immediately below the DN
- * subtree - search the named DN entry and the entire subtree below the DN

|port

|integer

a|The port used to connect to the LDAP Servers.

|query_timeout

|integer

a|Specifies the maximum time to wait for a query response from the LDAP server, in seconds.

```

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic

|skip_config_validation
|boolean
a|Indicates whether or not the validation for the specified LDAP
configuration is disabled.

|status
|link:#status[status]
a|

|try_channel_binding
|boolean
a|Specifies whether or not channel binding is attempted in the case of
TLS/LDAPS.

|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.

```

```
|user_dn
|string
a|Specifies the user Distinguished Name (DN) that is used as the starting
point in the LDAP directory tree for user lookups.
```

```
|user_scope
|string
a|Specifies the default search scope for LDAP for user lookups:
```

```
* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_scope": "base",
  "group_scope": "base",
  "min_bind_level": "anonymous",
  "netgroup_byhost_scope": "base",
  "netgroup_scope": "base",
  "port": 389,
  "servers": {
  },
  "session_security": "none",
  "status": {
    "code": 65537300,
    "dn_message": {
    },
    "state": "up"
  },
  "user_scope": "base"
}
```

```
=====
```

== Response

Status: 201, Created

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of LDAP records.

|records
|array[link:#ldap_service[ldap_service]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "base_scope": "base",
```



```

"group_scope": "base",
"min_bind_level": "anonymous",
"netgroup_byhost_scope": "base",
"netgroup_scope": "base",
"port": 389,
"preferred_ad_servers": {
},
"servers": {
},
"session_security": "none",
"status": {
  "code": 65537300,
  "dn_message": {
  },
  "state": "up"
},
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"user_scope": "base"
}
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 4915203
| The specified LDAP schema does not exist.
| 4915207
| The specified LDAP servers contain duplicate server entries.

```

```
| 4915229
| DNS resolution failed due to an internal error. Contact technical
support if this issue persists.

| 4915231
| DNS resolution failed for one or more of the specified LDAP servers.
Verify that a valid DNS server is configured.

| 23724132
| DNS resolution failed for all the specified LDAP servers. Verify that a
valid DNS server is configured.

| 4915234
| The specified LDAP server is not supported because it is one of the
following: multicast, loopback, 0.0.0.0, or broadcast.

| 4915248
| LDAP servers cannot be empty or "-". Specified FQDN is invalid because
it is empty or "-" or it contains either special characters or "-" at the
start or end of the domain.

| 4915251
| STARTTLS and LDAPS cannot be used together.

| 4915257
| The LDAP configuration is invalid. Verify that bind-dn and bind password
are correct.

| 4915258
| The LDAP configuration is invalid. Verify that the servers are reachable
and that the network configuration is correct.

| 13434916
| The SVM is in the process of being created. Wait a few minutes, and then
try the command again.

| 23724130
| Cannot use an IPv6 name server address because there are no IPv6
interfaces.

| 4915252
| LDAP referral is not supported with STARTTLS, with session security
levels sign, seal or with LDAPS.
|===
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#status]
[.api-collapsible-fifth-title]
status

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message.

|dn_message
|array[string]
a|

|message
|string
a|Provides additional details on the status of the LDAP service.

```

```

|state
|string
a|Specifies the status of the LDAP service.

|===

[#cluster_ldap]
[.api-collapsible-fifth-title]
cluster_ldap

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|base_dn
|string
a|Specifies the default base DN for all searches.

|base_scope
|string
a|Specifies the default search scope for LDAP queries:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|bind_as_cifs_server
|boolean
a|Specifies whether or not CIFS server's credentials are used to bind to
the LDAP server.

|bind_dn
|string
a|Specifies the user that binds to the LDAP servers.

```

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|group_dn
|string
a|Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups.

|group_membership_filter
|string
a|Specifies the custom filter used for group membership lookups from an LDAP server.

|group_scope
|string
a|Specifies the default search scope for LDAP for group lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|is_netgroup_byhost_enabled
|boolean
a|Specifies whether or not netgroup by host querying is enabled.

|is_owner
|boolean
a|Specifies whether or not the SVM owns the LDAP client configuration.

|ldaps_enabled
|boolean
a|Specifies whether or not LDAPS is enabled.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind

```

* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|netgroup_byhost_dn
|string
a|Specifies the netgroup Distinguished Name (DN) that is used as the
starting point in the LDAP directory tree for netgroup by host lookups.

|netgroup_byhost_scope
|string
a|Specifies the default search scope for LDAP for netgroup by host
lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|netgroup_dn
|string
a|Specifies the netgroup Distinguished Name (DN) that is used as the
starting point in the LDAP directory tree for netgroup lookups.

|netgroup_scope
|string
a|Specifies the default search scope for LDAP for netgroup lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|port
|integer
a|The port used to connect to the LDAP Servers.

|query_timeout
|integer
a|Specifies the maximum time to wait for a query response from the LDAP
server, in seconds.

|schema

```

```

|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic

|skip_config_validation
|boolean
a|Indicates whether or not the validation for the specified LDAP
configuration is disabled.

|status
|link:#status[status]
a|

|try_channel_binding
|boolean
a|Specifies whether or not channel binding is attempted in the case of
TLS/LDAPS.

|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.

|user_dn
|string
a|Specifies the user Distinguished Name (DN) that is used as the starting

```


point in the LDAP directory tree for user lookups.

|user_scope

|string

a|Specifies the default search scope for LDAP for user lookups:

* base - search the named entry only

* onelevel - search all entries immediately below the DN

* subtree - search the named DN entry and the entire subtree below the DN

|===

[#_links]

[.api-collapsible-fifth-title]

_links

[cols=3*,options=header]

|===

|Name

|Type

|Description

|next

|link:href[href]

a|

|self

|link:href[href]

a|

|===

[#svm]

[.api-collapsible-fifth-title]

svm

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

```

|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#ldap_service]
[.api-collapsible-fifth-title]
ldap_service

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ad_domain
|string
a|This parameter specifies the name of the Active Directory domain
used to discover LDAP servers for use by this client.
This is mutually exclusive with `servers` during POST and PATCH.

|base_dn
|string
a|Specifies the default base DN for all searches.

|base_scope
|string
a|Specifies the default search scope for LDAP queries:

* base - search the named entry only

```

- * onelevel - search all entries immediately below the DN
- * subtree - search the named DN entry and the entire subtree below the DN

|bind_as_cifs_server

|boolean

a|Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.

|bind_dn

|string

a|Specifies the user that binds to the LDAP servers.

|bind_password

|string

a|Specifies the bind password for the LDAP servers.

|group_dn

|string

a|Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups.

|group_membership_filter

|string

a|Specifies the custom filter used for group membership lookups from an LDAP server.

|group_scope

|string

a|Specifies the default search scope for LDAP for group lookups:

- * base - search the named entry only
- * onelevel - search all entries immediately below the DN
- * subtree - search the named DN entry and the entire subtree below the DN

|is_netgroup_byhost_enabled

|boolean

a|Specifies whether or not netgroup by host querying is enabled.

|is_owner

```

|boolean
a|Specifies whether or not the SVM owns the LDAP client configuration.

|ldaps_enabled
|boolean
a|Specifies whether or not LDAPS is enabled.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|netgroup_byhost_dn
|string
a|Specifies the netgroup Distinguished Name (DN) that is used as the
starting point in the LDAP directory tree for netgroup by host lookups.

|netgroup_byhost_scope
|string
a|Specifies the default search scope for LDAP for netgroup by host
lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|netgroup_dn
|string
a|Specifies the netgroup Distinguished Name (DN) that is used as the
starting point in the LDAP directory tree for netgroup lookups.

|netgroup_scope
|string
a|Specifies the default search scope for LDAP for netgroup lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

```

```

|port
|integer
a|The port used to connect to the LDAP Servers.

|preferred_ad_servers
|array[string]
a|

|query_timeout
|integer
a|Specifies the maximum time to wait for a query response from the LDAP
server, in seconds.

|referral_enabled
|boolean
a|Specifies whether or not LDAP referral is enabled.

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic

|skip_config_validation

```

```

|boolean
a|Indicates whether or not the validation for the specified LDAP
configuration is disabled.

|status
|link:#status[status]
a|

|svm
|link:#svm[svm]
a|

|try_channel_binding
|boolean
a|Specifies whether or not channel binding is attempted in the case of
TLS/LDAPS.

|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.

|user_dn
|string
a|Specifies the user Distinguished Name (DN) that is used as the starting
point in the LDAP directory tree for user lookups.

|user_scope
|string
a|Specifies the default search scope for LDAP for user lookups:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

```

```

|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block  
=====
```

```
:leveloffset: -1
```

```
= Manage NIS configuration
```

```
:leveloffset: +1
```

```
[[IDa584acda9bf622344cc8b1afa51d6b4f]]  
= Security authentication cluster NIS endpoint overview
```

```
== Overview
```

NIS servers are used to authenticate user and client computers. NIS domain name and NIS server information is required to configure NIS. This API retrieves and manages NIS server configurations.

```
== Examples
```

```
=== Retrieving cluster NIS information
```

The cluster NIS GET request retrieves the NIS configuration of the cluster.

The following example shows how a GET request is used to retrieve the cluster NIS configuration:

```
----
```

```
# The API:  
/security/authentication/cluster/nis
```

```
# The call:  
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/nis" -H  
"accept: application/hal+json"
```



```
# The response:
{
  "domain": "domainA.example.com",
  "servers": [
    "10.10.10.10",
    "example.com"
  ],
  "bound_servers": [
    "10.10.10.10"
  ]
}
```

=== Creating the cluster NIS configuration

The cluster NIS POST request creates a NIS configuration for the cluster.

The following example shows how a POST request is used to create a cluster NIS configuration:

```
# The API:
/security/authentication/cluster/nis
```

```
# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/nis"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
  \"domain\": \"domainA.example.com\", \"servers\": [
    \"10.10.10.10\", \"example.com\" ]}"
```

=== Updating the cluster NIS configuration

The cluster NIS PATCH request updates the NIS configuration of the cluster.

The following example shows how to update the domain:

```
# The API:
/security/authentication/cluster/nis
```

```
# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/nis"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
```

```
\\"domain\\": \\"domainC.example.com\\", \\"servers\\": [ \\"13.13.13.13\\" ]}"
```

The following example shows how to update the server:

The API:

/security/authentication/cluster/nis

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/nis"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\\"servers\\": [ \\"14.14.14.14\\" ]}"
```

== Deleting the cluster NIS configuration

The cluster NIS DELETE request deletes the NIS configuration of the cluster.

The following example shows how a DELETE request is used to delete the cluster NIS configuration:

The API:

/security/authentication/cluster/nis

The call:

```
curl -X DELETE "https://<mgmt-ip>/api/security/authentication/cluster/nis"
-H "accept: application/hal+json"
```

'''

```
[[ID77e9cf4470728e1af425d7cce83ee52b]]
```

= Delete the NIS configuration for the cluster

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/cluster/nis`#
```

Introduced In: 9.6

Deletes the NIS configuration of the cluster. NIS can be removed as a source from ns-switch if NIS is not used for lookups.

== Response

Status: 200, Ok

== Error

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====

== Definitions
```

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[IDc994ba7f23f78d989cf8af0a52816e38]]
= Retrieve the NIS configuration for the cluster
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/nis`#
```

***Introduced In:* 9.6**

Retrieves the NIS configuration of the cluster. Both NIS domain and servers are displayed by default.
The ``bound_servers`` property indicates the successfully bound NIS servers.

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```

```
|fields
|array[string]
|query
|False
```

a|Specify the fields to return.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|binding_details

|array[link:#binding_details[binding_details]]

a|An array of objects where each object represents the NIS server and it's status for a given NIS domain. It is an advanced field.

|bound_servers

|array[string]

a|

|domain

|string

a|The NIS domain to which this configuration belongs.

|servers

|array[string]

a|A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```

{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "binding_details": {
  },
  "bound_servers": {
  },
  "servers": {
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

```

    }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#binding_status]
[.api-collapsible-fifth-title]

```



```

binding_status

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Code corresponding to the server's binding status.

|message
|string
a|Detailed description of the server's binding status.

|===

[#binding_details]
[.api-collapsible-fifth-title]
binding_details

[cols=3*,options=header]
|===
|Name
|Type
|Description

|server
|string
a|Hostname/IP address of the NIS server in the domain.

|status
|link:#binding_status[binding_status]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
[[IDbe525dd6a1249045d22bdc59571de443]]
```

```
= Update the NIS configuration for the cluster
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-  
block]#`/security/authentication/cluster/nis`#
```

```
*Introduced In:* 9.6
```

Both NIS domain and servers can be updated. Domains and servers cannot be empty. Both FQDNs and IP addresses are supported for the 'servers' field. If the domain is updated, NIS servers must also be specified. IPv6 must be enabled if IPv6 family addresses are specified for the `servers` property.

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|binding_details
```

```
|array[link:#binding_details[binding_details]]
```

a|An array of objects where each object represents the NIS server and it's status for a given NIS domain. It is an advanced field.

```
|bound_servers
```

```
|array[string]
```

```
a|
```

```
|domain
|string
a|The NIS domain to which this configuration belongs.

|servers
|array[string]
a|A list of hostnames or IP addresses of NIS servers used
by the NIS domain configuration.
```

```
|===
```

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "binding_details": {
  },
  "bound_servers": {
  },
  "servers": {
  }
}
====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

```
ONTAP Error Response Codes
```

```
|===
```

Error Code	Description
1966253	IPv6 is not enabled in the cluster .
3276964	The NIS domain name or NIS server domain is too long. The maximum supported for domain name is 64 characters and the maximum supported for NIS server domain is 255 characters.
3276933	A maximum of 10 NIS servers can be configured per SVM.
23724109	DNS resolution failed for one or more specified servers.
23724112	DNS resolution failed due to an internal error. Contact technical support if this issue persists.
23724132	DNS resolution failed for all the specified servers.
23724130	Cannot use an IPv6 name server address because there are no IPv6 interfaces

===

[cols=3*,options=header]		
===		
Name	Type	Description
error		
link:#error[error]		
a		

===

.Example error

[%collapsible%closed]

====

[source,json,subs=+macros]

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

====

== Definitions

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
```

====

```
[#href]
[.api-collapsible-fifth-title]
href
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|href
|string
a|
```

|===

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```

|self
|link:#href[href]
a|

|===

[#binding_status]
[.api-collapsible-fifth-title]
binding_status

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Code corresponding to the server's binding status.

|message
|string
a|Detailed description of the server's binding status.

|===

[#binding_details]
[.api-collapsible-fifth-title]
binding_details

[cols=3*,options=header]
|===
|Name
|Type
|Description

|server
|string
a|Hostname/IP address of the NIS server in the domain.

|status
|link:#binding_status[binding_status]

```

```

a|

|===

[#cluster_nis_service]
[.api-collapsible-fifth-title]
cluster_nis_service

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|binding_details
|array[link:#binding_details[binding_details]]
a|An array of objects where each object represents the NIS server and it's
status for a given NIS domain. It is an advanced field.

|bound_servers
|array[string]
a|

|domain
|string
a|The NIS domain to which this configuration belongs.

|servers
|array[string]
a|A list of hostnames or IP addresses of NIS servers used
by the NIS domain configuration.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```



```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block
```

```
=====
```

```
[[IDabf1cc73d089aa128b719125158f1995]]
```

```
= Create the NIS configuration for the cluster
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/authentication/cluster/nis`#
```

```
*Introduced In:* 9.6
```

The cluster can have one NIS server configuration. Specify the NIS domain and NIS servers as input. Domain name and servers fields cannot be empty. Both FQDNs and IP addresses are supported for the `server` property. IPv6 must be enabled if IPv6 family addresses are specified in the `server` property. A maximum of ten NIS servers are supported.

```
== Required properties
```

```
* `domain` - NIS domain to which this configuration belongs.
```

```
* `servers` - List of hostnames or IP addresses of NIS servers used by the  
NIS domain configuration.
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|binding_details
```

```
|array[link:#binding_details[binding_details]]
```

a|An array of objects where each object represents the NIS server and it's status for a given NIS domain. It is an advanced field.

|bound_servers

|array[string]

a|

|domain

|string

a|The NIS domain to which this configuration belongs.

|servers

|array[string]

a|A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "binding_details": {
  },
  "bound_servers": {
  },
  "servers": {
  }
}
```

====

== Response

Status: 201, Created

[cols=3*,options=header]

```

|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of NIS domain records.

|records
|array[link:#cluster_nis_service[cluster_nis_service]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "binding_details": {
    },
    "bound_servers": {
    },
    "servers": {
    }
  }
}

```

```
}  
}  
====  
  
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 1966253  
| IPv6 is not enabled in the cluster.  
  
| 3276964  
| The NIS domain name or NIS server domain is too long. The maximum  
supported for domain name is 64 characters and the maximum supported for  
NIS server domain is 255 characters.  
  
| 3276933  
| A maximum of 10 NIS servers can be configured per SVM.  
  
| 13434916  
| The SVM is in the process of being created. Wait a few minutes, and then  
try the command again.  
  
| 23724109  
| DNS resolution failed for one or more specified servers.  
  
| 23724112  
| DNS resolution failed due to an internal error. Contact technical  
support if this issue persists.  
  
| 23724132  
| DNS resolution failed for all the specified servers.  
  
| 23724130  
| Cannot use an IPv6 name server address because there are no IPv6  
interfaces.  
|===
```

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#binding_status]
[.api-collapsible-fifth-title]
binding_status

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Code corresponding to the server's binding status.

|message
|string
a|Detailed description of the server's binding status.

|===

```

```

[#binding_details]
[.api-collapsible-fifth-title]
binding_details

[cols=3*,options=header]
|===
|Name
|Type
|Description

|server
|string
a|Hostname/IP address of the NIS server in the domain.

|status
|link:#binding_status[binding_status]
a|

|===

[#cluster_nis_service]
[.api-collapsible-fifth-title]
cluster_nis_service

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|binding_details
|array[link:#binding_details[binding_details]]
a|An array of objects where each object represents the NIS server and it's
status for a given NIS domain. It is an advanced field.

|bound_servers
|array[string]
a|

|domain

```



```

|string
a|The NIS domain to which this configuration belongs.

|servers
|array[string]
a|A list of hostnames or IP addresses of NIS servers used
by the NIS domain configuration.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
:leveloffset: -1
```

```
= Manage SAML service
```

```
:leveloffset: +1
```

```
[[ID2c58d353e914b7e54ec257c59e4dc974]]
```

```
= Security authentication cluster saml-sp endpoint overview
```

```
== Overview
```

This API is used to retrieve and display relevant information pertaining to the SAML service provider configuration in the cluster. The POST request creates a SAML service provider configuration if there is none present. The DELETE request removes the SAML service provider configuration. The PATCH request enables and disables SAML in the cluster. Various responses are shown in the examples below.

```
+
```

```
'''
```

```
== Examples
```

```
=== Retrieving the SAML service provider configuration in the cluster
```

The following output shows the SAML service provider configuration in the cluster.

```
+
```

```
'''
```

```
----
```

```
# The API:
```

```
/api/security/authentication/cluster/saml-sp
```

```
# The call:
```

```
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp" -H "accept: application/hal+json"
```

```
# The response:
```

```
{
```

```

"idp_uri": "https://examplelab.customer.com/idp/Metadata",
"enabled": true,
"host": "172.21.74.181",
"certificate": {
  "ca": "cluster1",
  "serial_number": "156F10C3EB4C51C1",
  "common_name": "cluster1"
},
"_links": {
  "self": {
    "href": "/api/security/authentication/cluster/saml-sp"
  }
}
}

```

'''

=== Creating the SAML service provider configuration

The following output shows how to create a SAML service provider configuration in the cluster.

+

'''

The API:

/api/security/authentication/cluster/saml-sp

The call:

```

curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp?return_records=true" -H "accept: application/hal+json" -d '{ "idp_uri": "https://examplelab.customer.com/idp/Metadata", "host": "172.21.74.181", "certificate": { "ca": "cluster1", "serial_number": "156F10C3EB4C51C1" } }'

```

'''

=== Updating the SAML service provider configuration

The following output shows how to enable a SAML service provider configuration in the cluster.

Disabling the configuration requires the client to be authenticated through SAML prior to performing the operation.

```

+

'''

----

# The API:
/api/security/authentication/cluster/saml-sp

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/saml-
sp/" -d '{ "enabled": true }'
----

'''

=== Deleting the SAML service provider configuration

'''

----

# The API:
/api/security/authentication/cluster/saml-sp

# The call:
curl -X DELETE "https://<mgmt-
ip>/api/security/authentication/cluster/saml-sp/"
----

'''

[[IDd2a20e3fb0072ae8497b7eccfa30326b]]
= Delete a SAML service provider configuration

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/cluster/saml-sp`#

*Introduced In:* 9.6

Deletes a SAML service provider configuration.

```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 12320803  
| SAML must be disabled before the configuration can be removed.  
|===
```

```
[cols=3*,options=header]
```

```
|===  
|Name  
|Type  
|Description
```

```
|error  
|link:#error[error]  
a|
```

```
|===
```

.Example error

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

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

```

    }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[IDad14333b5bd1c0a2e25421f023611b93]]
= Retrieve a SAML service provider configuration
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/saml-sp`#
```

***Introduced In:** 9.6

Retrieves a SAML service provider configuration.

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```



```
|idp_uri
|string
|query
|False
a|Filter by idp_uri
```

* Introduced in: 9.7

```
|enabled
|boolean
|query
|False
a|Filter by enabled
```

* Introduced in: 9.7

```
|certificate.serial_number
|string
|query
|False
a|Filter by certificate.serial_number
```

* Introduced in: 9.7

* maxLength: 40

* minLength: 1

```
|certificate.common_name
|string
|query
|False
a|Filter by certificate.common_name
```

* Introduced in: 9.7

```
|certificate.ca
|string
|query
|False
a|Filter by certificate.ca
```

* Introduced in: 9.7

* maxLength: 256

* minLength: 1

```
|host
|string
|query
|False
a|Filter by host

* Introduced in: 9.7

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|certificate
|link:#certificate[certificate]
a|

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

|host
|string
a|The SAML service provider host.
```

```
|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.
```

```
|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-
06/FederationMetadata.xml"
}
====
```

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===
```

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|ca
|string
a|Server certificate issuing certificate authority (CA). This cannot be
used with the server certificate common name.

|common_name
|string
a|Server certificate common name. This cannot be used with the
certificate authority (CA) or serial_number.

|serial_number
|string
a|Server certificate serial number. This cannot be used with the server
certificate common name.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```

```
[#error]
```

```
[.api-collapsible-fifth-title]
```

```
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|arguments
```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

====

[[IDae76d2b0e1fdaa48f36dd47f5be6efb9]]

= Update a SAML service provider configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-block]#`/security/authentication/cluster/saml-sp`#

Introduced In: 9.6

Updates a SAML service provider configuration.

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|certificate

|link:#certificate[certificate]

a|

|enabled

|boolean

a|The SAML service provider is enabled. Valid for PATCH and GET operations only.

|host

```

|string
a|The SAML service provider host.

|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-
06/FederationMetadata.xml"
}
=====

== Response

```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description

```



```

| 12320791
| SAML can only be disabled using the console or a SAML-authenticated
application.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]

```

```

href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|ca
|string
a|Server certificate issuing certificate authority (CA). This cannot be
used with the server certificate common name.

```

```

|common_name
|string
a|Server certificate common name. This cannot be used with the
certificate authority (CA) or serial_number.

|serial_number
|string
a|Server certificate serial number. This cannot be used with the server
certificate common name.

|===

[#security_saml_sp]
[.api-collapsible-fifth-title]
security_saml_sp

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|certificate
|link:#certificate[certificate]
a|

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

|host
|string
a|The SAML service provider host.

|idp_uri
|string

```

a|The identity provider (IdP) metadata location. Required for POST operations.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

|===

|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
[[ID383cfb6331d0faa2d1677a12f4a9e04b]]
```

```
= Create a SAML service provider configuration
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/authentication/cluster/saml-sp`#
```

```
*Introduced In:* 9.6
```

Creates a SAML service provider configuration. Note that "common_name" is mutually exclusive with "serial_number" and "ca" in POST. SAML will initially be disabled, requiring a patch to set "enabled" to "true", so that the user has time to complete the setup of the IdP.

```
== Required properties
```

```
* `idp_uri`
```

```
== Optional properties
```

```
* `certificate`
```

```
* `enabled`
```

```
* `host`
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|verify_metadata_server
```

```
|boolean
```

```
|query
```

```
|False
```

```
a|Verify IdP metadata server identity.
```

```
* Default value: 1
```

```
|return_timeout
```

```
|integer
```

```
|query
```

```
|False
```

```
a|The number of seconds to allow the call to execute before returning.
```

When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

```
* Default value: 1
```

```
* Max value: 120
```

```
* Min value: 0
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```

|link:#_links[_links]
a|

|certificate
|link:#certificate[certificate]
a|

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

|host
|string
a|The SAML service provider host.

|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-
06/FederationMetadata.xml"
}
====

== Response

```

Status: 202, Accepted

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|job
|link:#job_link[job_link]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
====

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 12320789
| Failed to download data file from specified URI.

| 12320794
| The host parameter provided must be the cluster management interface's
```


IP address. If the cluster management interface is not available, the node management interface's IP address must be used.

| 12320795

| A valid cluster or node management interface IP address must be provided.

| 12320805

| The certificate information provided does not match any installed certificates.

| 12320806

| The certificate information entered does not match any installed certificates.

| 12320814

| An invalid IDP URI has been entered.

| 12320815

| An IDP URI must be an HTTPS or FTPS URI.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },

```

```

    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self
|link:#href[href]
a|

```

```

|===

```

```

[#certificate]
[.api-collapsible-fifth-title]
certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|ca
|string
a|Server certificate issuing certificate authority (CA). This cannot be
used with the server certificate common name.

|common_name
|string
a|Server certificate common name. This cannot be used with the
certificate authority (CA) or serial_number.

|serial_number
|string
a|Server certificate serial number. This cannot be used with the server
certificate common name.

|===

[#security_saml_sp]
[.api-collapsible-fifth-title]
security_saml_sp

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|certificate

```

```

|link:#certificate[certificate]
a|

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

|host
|string
a|The SAML service provider host.

|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.

|===

[#job_link]
[.api-collapsible-fifth-title]
job_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|The UUID of the asynchronous job that is triggered by a POST, PATCH, or
DELETE operation.

|===

[#error_arguments]

```

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
:leveloffset: -1
```

```
= Update user account password
```

```
:leveloffset: +1
```

```
[[ID45de4ced975cc1ef9f6c04dc61525b7f]]
= Security authentication password endpoint overview
```

```
== Overview
```

This API changes the password for a local user account.

Only cluster administrators with the `_"admin"_` role can change the password for other cluster or SVM user accounts. If you are not a cluster administrator, you can only change your own password.

```
== Examples
```

```
=== Changing the password of another cluster or SVM user account by a
cluster administrator
```

Specify the user account name and the new password 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.

For an SVM-scoped account, along with new password and user account name, specify either the SVM name as the `owner.name` or SVM uuid as the `owner.uuid` in the body of the POST request. These indicate the SVM for which the user account is created and can be obtained from the response

body of a GET request performed on the `_/api/svm/svms_` API.

The API:

POST `"/api/security/authentication/password"`

The call to change the password of another cluster user:

```
curl -X POST "https://<mgmt-ip>/api/security/authentication/password" -d  
'{"name":"cluster_user1","password":"hello@1234"}'
```

The call to change the password of another SVM user:

```
curl -X POST "https://<mgmt-ip>/api/security/authentication/password" -d  
'{"owner.name":"svm1","name":"svm_user1","password":"hello@1234"}'
```

The call to change the password hash algorithm of the cluster user:

```
curl -X POST "https://<mgmt-ip>/api/security/authentication/password" -d  
'{"name":"cluster_user1","password":"hello@1234","password_hash_algorithm"  
:"sha256"}'
```

The call to change the password hash algorithm of another SVM user:

```
curl -X POST "https://<mgmt-ip>/api/security/authentication/password" -d  
'{"owner.name":"svm1","name":"svm_user1","password":"hello@1234","password_  
_hash_algorithm":"sha256"}'
```

=== Changing the password of an SVM-scoped user

NOTE: The IP address in the URI must be same as one of the interfaces owned by the SVM.

The API:

POST `"/api/security/authentication/password"`

The call:

```
curl -X POST "https://<SVM-ip>/api/security/authentication/password" -d
```

```
'{"name":"svm_user1","password":"new1@1234"}'
```

'''

```
[[ID63bdaa371c712cf768e58789a7c83636]]
```

= Update the user account password

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/authentication/password`#
```

Introduced In: 9.6

Updates the password for a user account.

== Required parameters

* `name` - User account name.

* `password` - New password for the user account.

== Optional parameters

* `owner.name` or `owner.uuid` - Name or UUID of the SVM for an SVM-scoped user account.

* `password_hash_algorithm` - Optional property that specifies the password hash algorithm used to generate a hash of the user's password for password matching. Default value is "sha512".

== Related ONTAP commands

* `security login password`

== Learn more

*

xref:{relative_path}security_authentication_password_endpoint_overview.htm
l[DOC /security/authentication/password]

* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

== Parameters


```
[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.
```

* Default value:

```
|===
```

== Request Body

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|name
|string
a|The user account name whose password is being modified.
```

```
|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account. This
field is optional and valid only when a cluster administrator is executing
the API to uniquely identify the account whose password is being modified.
The "owner" field is not required to be specified for SVM user accounts
trying to modify their password.
```

```
|password
|string
a|The password string
```

```
|password_hash_algorithm
|string
a|Optional property that specifies the password hash algorithm used to
generate a hash of the user's password for password matching.
```

```
|===
```

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "password_hash_algorithm": "sha512"
}
====
```

```
== Response
```

Status: 201, Created

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

Error Code	Description
7077918	The password cannot contain the username.
7077919	

```

| The minimum length for new password does not meet the policy.

| 7077920
| The new password must have both letters and numbers.

| 7077921
| The minimum number of special characters required do not meet the
policy.

| 7077924
| The new password must be different than last N passwords.

| 7077925
| The new password must be different to the old password.

| 7077940
| The password exceeds maximum supported length.

| 7077941
| Defined password composition exceeds the maximum password length of 128
characters.
|===

```

```

[cols=3*,options=header]

```

```

|===

```

```

|Name

```

```

|Type

```

```

|Description

```

```

|error

```

```

|link:#error[error]

```

```

a|

```

```

|===

```

```

.Example error

```

```

[%collapsible%closed]

```

```

====

```

```

[source,json,subs=+macros]

```

```

{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    }
  }
}

```

```

    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the user account. This field is optional and valid only when a cluster administrator is executing the API to uniquely identify the account whose password is being modified. The "owner" field is not required to be specified for SVM user accounts trying to modify their password.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#account_password]
[.api-collapsible-fifth-title]
account_password
```

The password object

```
[cols=3*,options=header]
|===
|Name
|Type
```

```

|Description

|name
|string
a|The user account name whose password is being modified.

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account. This
field is optional and valid only when a cluster administrator is executing
the API to uniquely identify the account whose password is being modified.
The "owner" field is not required to be specified for SVM user accounts
trying to modify their password.

|password
|string
a|The password string

|password_hash_algorithm
|string
a|Optional property that specifies the password hash algorithm used to
generate a hash of the user's password for password matching.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string

```

```

a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

```

```
= Manage authentication keys (for admins)
```

```
:leveloffset: +1
```

```
[[IDe846bcd03166780fdb35be3cf4b3420]]
```

```
= Security authentication publickeys endpoint overview
```

```
== Overview
```

This API configures the public keys for user accounts.

For secure shell (SSH) access, public-private key pair based authentication is possible by associating the public key with a user account.

Prerequisites:

You must have generated the SSH key.

You must be a cluster or SVM administrator to perform the user's public key.

```
== Examples
```

```
=== Creating a public key for cluster-scoped user accounts
```

Specify the user account name, public key, index, and comment in the body of the POST request. The owner.uuid or owner.name are not required for a cluster-scoped user account.

```
----
```

```
# The API:
```

```
POST "/api/security/authentication/publickey"
```

```
# The call
```

```
curl -k https://<mgmt-ip>/api/security/authentication/publickeys --request  
POST --data '{ "account": "pubuser2", "comment": "Cserver-  
Creation", "index": 0, "public_key": "ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQDWJTerK2xXi3Lkrqrm6Q67aNmNDNKgpezwzl9Ap+DxtM  
xmocHC52CuwEcJjIUel21uAi0myscaJmC5Y0BzSnYuwcJ3/82kconFUwtK0h6QUTGqbc0vb4MZ  
39yIiiItCOBWtTot3msJYfZB+dgCxCxMZ+0bl9YwZXrWMWP6XDJw/ai/EfWTZHC7e8Xe1mfp+C0c  
GMhlxRvgfGjhzqU85DBfdGD5Tu/67vD13Q+817Jf8iBxgrEFiqirnkWNX5dj+jkMlEVC3s6dY  
ciJNBEiMxNkSFGTnkG74S61pvZNFD6mSznV/28hl3zSjwWiuacsP3BelydeG8nEcCRN5Ap7vMd  
Vd" }'
```

```
----
```


=== Creating a public key for SVM-scoped user accounts

For a SVM-scoped account, specify either the SVM name as the owner.name or the SVM UUID as the owner.uuid along with other parameters for the user account. These parameters indicate the SVM that contains the user account for the public key being created and can be obtained from the response body of the GET request performed on the API"/api/svm/svms".

The API:

POST "/api/security/authentication/publickey"

The call

```
curl -k https://<mgmt-ip>/api/security/authentication/publickeys --request
POST --data '{ "account": "pubuser4", "comment": "Vserver-
Creation", "index": 0, "owner.uuid": "513a78c7-8c13-11e9-8f78-
005056bbf6ac", "owner.name": "vs0", "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDWTerk2xXi3Lkrqrm6Q67aNmNDNKgpezwzl9Ap+DxtM
xmocHC52CuWecJjIUe121uAi0myscaJmC5Y0BzSnYuwcJ3/82kconFUwtK0h6QUTGqbc0vb4MZ
39yIiiItCOBWTot3msJYfZB+dgCXMZ+0bl9YwZXrWMWP6XDJw/ai/EfWTZHC7e8Xe1mfp+C0c
GMhlxRvgfeGjhZqU85DBfdGD5Tu/67vD13Q+817Jf8iBxgrEFiqirnkWNX5dj+jkM1EVC3s6dY
ciJNBEiMxNkSFGTnkG74S61pvZNFD6mSznV/28hl3zSjwWiuacsP3BelydeG8nEcCRN5Ap7vMd
Vd" }'
```

=== Retrieving the configured public key for user accounts

Retrieves all public keys associated with the user accounts or a filtered list (for a specific user account name, a specific SVM and so on) of public keys.

The API:

GET "/api/security/authentication/publickeys"

The call to retrieve all the user accounts configured in the cluster:

```
curl -k https://<mgmt-ip>/api/security/authentication/publickeys
----
```

[[IDdb2a2701b38e46d56de8a66993780e40]]

= Retrieve the public keys configured for user accounts

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/authentication/publickeys`#
```

Introduced In: 9.7

Retrieves the public keys configured for user accounts.

== Related ONTAP commands

* `security login publickey show`

== Learn more

*

xref:{relative_path}security_authentication_publickeys_endpoint_overview.html[DOC /security/authentication/publickeys]

* xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]

== Parameters

```
[cols=5*,options=header]
|==
```

|Name

|Type

|In

|Required

|Description

|sha_fingerprint

|string

|query

|False

a|Filter by sha_fingerprint

|index

|integer

|query

|False

a|Filter by index

* Max value: 99

* Min value: 0

```
|obfuscated_fingerprint
|string
|query
|False
a|Filter by obfuscated_fingerprint
```

```
|account.name
|string
|query
|False
a|Filter by account.name
```

```
|comment
|string
|query
|False
a|Filter by comment
```

```
|scope
|string
|query
|False
a|Filter by scope
```

```
|owner.uuid
|string
|query
|False
a|Filter by owner.uuid
```

```
|owner.name
|string
|query
|False
a|Filter by owner.name
```

```
|public_key
|string
|query
```

```

|False
a|Filter by public_key

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|max_records
|integer
|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|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
a|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.

* Max value: 120
* Min value: 0
* Default value: 1

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.

```

Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|num_records

|integer

a|Number of records

|records

|array[link:#publickey[publickey]]

a|

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

{

 "_links": {

 "next": {

 "href": "/api/resourcelink"

 },

 "self": {

 "href": "/api/resourcelink"

 }

 },

 "records": {

 "_links": {

 "self": {

```

        "href": "/api/resourcelink"
    }
},
"account": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "name": "joe.smith"
},
"comment": "string",
"obfuscated_fingerprint": "string",
"owner": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"scope": "cluster",
"sha_fingerprint": "string"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

```

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]

```

```

|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_reference]
[.api-collapsible-fifth-title]
account_reference

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```



```
|name
|string
a|User account
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the public key.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#publickey]
[.api-collapsible-fifth-title]
publickey
```

The public key for the user account (to access SSH).

```
[cols=3*,options=header]
|===
```

```

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).

```

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

|===

|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[ID61c3ae00de2f90610a4e718b93f17f0d]]
= Create a public key for a user account
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/publickeys`#
```

```
*Introduced In:* 9.7
```

Creates a public key for a user account.

== Required properties

- * `owner.uuid` - UUID of the account owner.
- * `name` - User account name.
- * `index` - Index number for the public key (where there are multiple keys for the same account).
- * `public_key` - The publickey details for the creation of the user account.

== Related ONTAP commands

- * `security login publickey create`

== Learn more

*

xref:{relative_path}security_authentication_publickeys_endpoint_overview.h
tml[DOC /security/authentication/publickeys]

```
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]
```

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|return_records
```

```
|boolean
```

```
|query
```

```
|False
```

```
a|The default is false. If set to true, the records are returned.
```

* Default value:

```
|===
```

== Request Body

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|account
```

```
|link:#account_reference[account_reference]
```

```
a|
```

```
|comment
```

```
|string
```

```
a|Optional comment for the public key.
```

```
|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).
```

```
|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).
```

```
|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.
```

```
|public_key
|string
a|The public key
```

```
|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.
```

```
|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).
```

```
|===
```

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "account": {
```

```

    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "cluster",
  "sha_fingerprint": "string"
}
====

```

== Response

Status: 201, Created

```

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

```

.Example error

```

[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===

```



```
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#account_reference]
[.api-collapsible-fifth-title]
account_reference
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|User account
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the public key.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
```

```

|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#publickey]
[.api-collapsible-fifth-title]
publickey

The public key for the user account (to access SSH).

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

```

```

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string

```

```

a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

```

```
= Manage authentication keys (end-users)
```

```
:leveloffset: +1
```

```
[[IDa16b667c76a55b880bd3b382479333b9]]
```

```
= Security authentication publickeys owner.uuid account.name index  
endpoint overview
```

== Overview

This API configures the public keys for end-user (non-cluster admin) accounts.

Specify the owner UUID, the user account name, and the index in the URI path. The owner UUID corresponds to the UUID of the SVM containing the user account associated with the public key and can be obtained from the response body of the GET request performed on the API `"/api/svm/svms"`.

The index value corresponds to the public key that needs to be modified or deleted (it is possible to create more than one public key for the same user account).

== Examples

=== Retrieving the specific configured public key for user accounts

The API:

GET

`"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}"`

The call:

`curl -k https://<mgmt-ip>/api/security/authentication/publickeys/513a78c7-8c13-11e9-8f78-005056bbf6ac/pubuser4/0`

=== Updating the public key and comment for user accounts

The API:

PATCH

`"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}"`

```

x}"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/publickeys/d49de271-
8c11-11e9-8f78-005056bbf6ac/pubuser1/0 --request PATCH --data '{
"comment": "Cserver-modification", "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCMsLP/FeiT1J4Fb4GNVO4ioa1NIUHWeG08+anDbFke3J
cFT5JqBn0QZiG0uF0bqepken/moVKZg8iQnglarjP4ULhhje/LwDuUbaB7kvtPL2gyzAX1qFYn
BJ5R1LXja25Z4xeeaXUBJjhUmvpfque0TxbvpaG5V9rFTzVg9ccjBnkBchg3EkhF4VtHmrZNpT
DAUOBaz69FRYXYz2ExoCHWqElHBJep9D0DLN0XtzQA0IF9hJck6xja5RcAQ6f9pLMCol9vJiqp
cBAjkUmglqH5ZNHsgDQ7dtGNGJw45zqXHPAy9z8yKJuIsdK2/4iVYLDL8mlHFEIgeADn6OSxui
j1" }'
----

=== Deleting the public key for user accounts

----

# The API:
DELETE
"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{inde
x}"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/publickeys/d49de271-
8c11-11e9-8f78-005056bbf6ac/pubuser1/0 --request DELETE
----

[[IDc8b5c03bbe4e871bec0e481049fcfde1]]
= Delete a public key for a user account

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/publickeys/{owner.uuid}/{account.name}/{i
ndex}`#

*Introduced In:* 9.7

Deletes the public key for a user account.

== Related ONTAP commands

* `security login publickey delete`

```

== Learn more

*

xref:{relative_path}security_authentication_publickeys_owner.uuid_account.
name_index_endpoint_overview.html[DOC
/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|owner.uuid
|string
|path
|True
a|Account owner UUID

|account.name
|string
|path
|True
a|User account name

|index
|integer
|path
|True
a|Index number for the public key (where there are multiple keys for the
same account).

* Max value: 99
* Min value: 0

|===

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
```



```

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[ID1ce706ddfaec4adbf90fdb955d36e52c]]
= Retrieve the public keys configured for a user account
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/publickeys/{owner.uuid}/{account.name}/{i
ndex}`#
```

```
*Introduced In:* 9.7
```

Retrieves the public keys configured for a user account.

== Related ONTAP commands

* `security login publickey show`

== Learn more

```
*
xref:{relative_path}security_authentication_publickeys_owner.uuid_account.
name_index_endpoint_overview.html[DOC
/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]
```

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
```

```

|Required
|Description

|owner.uuid
|string
|path
|True
a|Account owner UUID


|account.name
|string
|path
|True
a|User account name


|index
|integer
|path
|True
a|Index number for the public key (where there are multiple keys for the
same account).

* Max value: 99
* Min value: 0


|fields
|array[string]
|query
|False
a|Specify the fields to return.


|max_records
|integer
|query
|False
a|Limit the number of records returned.


|return_records
|boolean
|query
|False
a|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

a|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.

* Max value: 120
* Min value: 0
* Default value: 1

|order_by
|array[string]
|query
|False

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

```

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {

```

```

        "href": "/api/resourcelink"
    }
},
"account": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "name": "joe.smith"
},
"comment": "string",
"obfuscated_fingerprint": "string",
"owner": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"scope": "cluster",
"sha_fingerprint": "string"
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error

```

```

[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===

```

```
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#account_reference]
[.api-collapsible-fifth-title]
account_reference
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|User account
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the public key.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
```



```

|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===

//end collapsible .Definitions block
====

[[ID3778c30d2cc806637fcb81c00562284c]]
= Update a public key for a user account


[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/authentication/publickeys/{owner.uuid}/{account.name}/{i
ndex}`#


*Introduced In:* 9.7


Updates the public key for a user account.


== Related ONTAP commands


* `security login publickey modify`


== Learn more

```

```

*
xref:{relative_path}security_authentication_publickeys_owner.uuid_account.
name_index_endpoint_overview.html[DOC
/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

```

== Parameters

```

[cols=5*,options=header]
|===

```

```

|Name
|Type
|In
|Required
|Description

```

```

|owner.uuid
|string
|path
|True
a|Account owner UUID

```

```

|account.name
|string
|path
|True
a|User account name

```

```

|index
|integer
|path
|True
a|Index number for the public key (where there are multiple keys for the
same account).

```

```

* Max value: 99
* Min value: 0

```

```

|===

```

== Request Body

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

```

```
|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).
```

```
|===
```

```
.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "account": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "cluster",
  "sha_fingerprint": "string"
}
=====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_reference]
[.api-collapsible-fifth-title]
account_reference

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|User account

```

```
|===
```

```
[#owner]  
[.api-collapsible-fifth-title]  
owner
```

Owner name and UUID that uniquely identifies the public key.

```
[cols=3*,options=header]  
|===  
|Name  
|Type  
|Description
```

```
|_links  
|link:#_links[_links]  
a|
```

```
|name  
|string  
a|The name of the SVM.
```

```
|uuid  
|string  
a|The unique identifier of the SVM.
```

```
|===
```

```
[#publickey]  
[.api-collapsible-fifth-title]  
publickey
```

The public key for the user account (to access SSH).

```
[cols=3*,options=header]  
|===  
|Name  
|Type  
|Description
```



```

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).

|===

```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```

```
[#error]
```

```
[.api-collapsible-fifth-title]
```

```
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|arguments
```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= Manage Azure Key Vaults
```

```
:leveloffset: +1
```

```
[[IDac8cala0787d4e1fd986e9fd0c82a425]]
```

```
= Security azure-key-vaults endpoint overview
```

```
== Overview
```

Azure Key Vault (AKV) is a cloud key management service (KMS) that provides a secure store for secrets. This feature

allows ONTAP to securely store its encryption keys using AKV.

In order to use AKV with ONTAP, you must first deploy an Azure application with the appropriate access to an AKV and then provide

ONTAP with the necessary details, such as key vault name, application ID so that ONTAP can communicate with the deployed Azure application.

The properties "state", "azure_reachability" and "ekmip_reachability" are considered advanced properties and are populated only when explicitly requested.

```
== Examples
```

```
=== Creating an AKV for a cluster using the client secret authentication method
```

The example AKV is configured at the cluster-scope. Note the `_return_records=true_` query parameter is used to obtain the newly created key manager configuration.

The API:

POST /api/security/azure-key-vaults

The call:

```
curl -X POST 'https://<mgmt-ip>/api/security/azure-key-  
vaults?return_records=true' -H 'accept: application/hal+json' -d "{  
  \"client_id\": \"client1\", \"tenant_id\": \"tenant1\", \"name\":  
  \"https://mykeyvault.azure.vault.net/\", \"key_id\": \"https://keyvault-  
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74\",  
  \"client_secret\" : \"myclientPwd\" }"
```

The response:

```
{  
  "num_records": 1,  
  "records": [  
    {  
      "uuid": "85619643-9a06-11ea-8d52-005056bbeba5",  
      "client_id": "client1",  
      "tenant_id": "tenant1",  
      "name": "https://mykeyvault.azure.vault.net/",  
      "key_id": "https://keyvault-test.vault.azure.net/keys/key1",  
      "_links": {  
        "self": {  
          "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-  
005056bbeba5"  
        }  
      }  
    }  
  ]  
}
```

'''

=== Creating an AKV for an SVM using the certificate authentication method

The example AKV is configured for a specific SVM. Note the `_return_records=true_` query parameter is used to obtain the newly created key manager configuration.

```

----

# The API:
POST /api/security/azure-key-vaults

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/azure-key-
vaults?return_records=true' -H 'accept: application/hal+json' -d "{
  \"svm\": { \"uuid\": \"4f7abf4c-9a07-11ea-8d52-005056bbeba5\" },
  \"client_id\": \"client1\", \"tenant_id\": \"tenant1\", \"name\":
  \"https://mykeyvault.azure.vault.net/\", \"key_id\": \"https://keyvault-
test.vault.azure.net/keys/key1\", \"client_certificate\" :
  \"MIIQKQIBAZCCD+8GCSqGSIB3DQEHAaCCD+AEgg/cMIIP2DCCBg8GCSqGSIB3DQEBqCCBgAw
ggX8AgEAMIIF9QYJKoZIhvcNAQcBMBwGCiqGSIB3DQEMAQYwDgQIWkY7ojViJDYCAggAgIIFyJ
PjIfmM6yTCKVw5ep2oZLwwVRca8pKhISVjw+WjWngh/f6Py/Ty0CwCjDFUZPsUUdSmk78E7SAz
0CpQyBwmUuFJQShjZjftHLKRWld3O4sJKB8DzH9Yw1C7En94cyJ1rT4WYoVFmeJcmOXx6h+NFH
c7njtXVsKwxc5BF88K3+3kHdV3WyVdXoeXe7yY/+EjFfjtBryp81juielX/NF1h5kowhoj+yxn
00c1/0OI1iV3mTIOTXD8qrZVp9ZhAxSTRBd5uDyWMfppqxW2L+9vCUU+ZgmRxtU3VsRLOp/T14
0OP7Sn1Ch2OE0bIrbYYtcpi04QcUtfEJBm1bbTbJPHDAtiO2KIQKviZL4QMZgho9NNgL4MUPIb
NSzDCbuIC+nNMxfghs0nPZewY+b43H/tMmnZ8Q4kiCFwrUqbFbflBiPMOaJsS0eQaJhDmzM90Q
EgbesHWgPreAcfMUcN1+BaqHFLHUxLXDxQix6zYiCatDX6/EKlirRh1TFpmFX2PBd+X6uODhmw
m4ub9RKj3In8t5qgtN4q/mTBXjAVDAbTIIIEgobBRaXGSSXCbc9W/jRed0DRZD9Bm8T/nV39sZN
ducwZa5ojYTX8fFMA0cfY6IFivXHjB00coHEEGdgCfC0G8vACqLbb+2NuhMJPtR7Ig50iAPUMc
670Z5ItOTQhyYOZ/KagOtvV8sKPCzeAkcMoHlsm189V79zt1fCJQTVWnaGiMj5Orcbssk6vCxh
DGeU6q1kgvXJKXOYRF8/wIpv8Y7/rEpnGwE/I0ZOXzdIDHXqA53B1zyOVem25ezWCD+kpoH89X
JssY1NjIMJhjVRED61w/DbSXg2yFu/v3ckGapVvTuyAiz5hWUNfl3pt++da6GoekKnLqtL4G/R
GXCnebLbXg838dlTGBznoCwGTVxXDeVYafz8AjI10qYtTMcbN56ya9kK7IHSkrnFX24xQRQOfm
D0Vob71pjdZ8r1aXKvD/1X2TkYJHoeEHq0nWpU8vWDG/xhv4YgKJGN9qsEZgiTXETUh5gak8e1
tGNkP+fum+1Oql05oS+Swna5/eB8eFeJ120i48Xi5UapaTRHPFp6kZfPXOu9cEjhILowRIi6gl
g7FUBmoJcu50vDIyP9JlyQklw2VtgNlmlQOIvzRenXmy18XnP50NTxx2cIwby8tIcdSn2C2qhj
8Gk7q8oxVZGiBgtz4BwyzyKkypwm60BBRrHpAKLw6JM5RISeZnYQfIsId0tGgb61go0RJf0sFt
buvZcSvLI+2Onj8KH1TlmmMR4dbuCWE9Ym4sVRmD1D6/f6BoNH0DRg7TJKEfbOadJsNPGzHbKte
LdaSMGTNUZ3hEDQeomakQMfvCgypbOLxrtTqfbenHRTn+iFNYW0zCUW6EJoAXp+lqFnwQL52I1
2QxwZike01P2k0GharzAJkXnNaFGnmHIIP6wJrCCSDZwDmr7GI2R5evDlRi17QUg2sulxQV0U8
zezzwIUgEe/Whf0ngGJv/QcsL2jyri/tSQbUWs4g+yep4S1E3iddhfqSJzI2iKdAE+HLiHGVO1
z70fGES06dPLnmh4eoWidgZi9N/SoBy1aT0JpIQ6z6N5ImPfdWu9Y6TWXUg1iyOIXGsxiQVIgU
NoB5Ru/ApDxpYpFLk0fH9k9OnEWK5Im33puOQKLno1uwrOmdBG8+x1EY8wc9FvkHGH0Zh4Hydi
CVUcYSdiGWUxVmgm4OgyiYzcpB+Ar2dzikGc4pBg8fa1a1HN5Q3TK3w4h/HeOulm4vWOYuVO1
H93ILGP6Pwfkgu+1Tam6+8yD0W5meiz0UIZR8TF/9gDb4+4wTFnPgwfTrggEauA8tt8uJtiyBC
rYexgZTXIZGTUj/86KXQaJKCreRr/kqWJOWqkNW4CGUVzw7LiI+sArOZqUp/TsxnbnC73XCMN1
PsnByb2zCeK13V26Crl84U9sDuqQTJRaIse01MN9AAjpa2QWEwgggnBBgkqhkiG9w0BBwGgggmy
BIIJrjCCaowggmmBgsqhkiG9w0BDAoBAqCCCW4wgg1qMBwGCiqGSIB3DQEMAQMwDgQIEjm88b
1+pnkCAGgABIIJSDD3P+vn11SolmQvmYgZVfV37T3KpurJvMxQScPvalWiF7Q1Iwasf/+N0hKK
Nr2j/aGZLunLkaG6mLPeBP212LCwnUxDu5kYffVVE90WX/bXewbYQribwFNkNhUrSgen8BfhnR
lvDrzbBLoHivDrUFszSVBCYh31Vwgu8p9SjC8K/XlumcLdjSFko85XpoK23euhowjWH+X0kRoY
GzorcdNE8z03BKvfR61W2XWzTSaWQ6eZHG6UrnX5Fe/w50U9tMIi3BCCCqgapUHVdmHqKkmWL

```

ikX8LssUcN30JVekM2aJ9v4YO6CoegKAMVDs0tVSov3KbGC3GNX6lgHu4y1LOZPlPLfPXb0wDH
qavlXK3zpHl8sIRzuX3HXSdEdenHYAkSV/IQZ89h+CZUkf0nu/og8eoA8ATDA5g7fj3HXpQ6cY
drUBaHc7ruxHOiWR0GcT4XK4TTz7zZTO1wWPViprUo6ayw0dYZSG22MeDA027YirM044Ifosn9
CsqnNLZoOWvA2ao4ippDoBRqv5Hv6n0I3fOAYS5nPq3jJtKQ5neqUYo0MrAkoKHo0h6zn0Bfvi
syB88aM9N0mPD76ykbAERq7151biKbA2tk8bb9dy/sJmk2ojM/D/W1YtrNL4iM6azL2kVN5eiC
hxCof33/RuRpXfGR8YNeJTl7bq42wL70QKDBRoG1TPcLqdVqz74oshlRspfqvZsbsUatbASBt2
T0YG4zfgfGh7sb2ezyoungVvzdp77wAJ6n39dc/ZLDdYDzFkQb07984y8LlhIM1AcwFcMh43gWp
6A8CJ02174ednirSqSVOPZ7K9dRw6Y0X8MB4/WGzEcvFeHYIGLBcXi1sBY5wjWnbeuhlWLiSkM
DQRB6oGOvF7bJsilKx5PwgWbbqw8KUSuU01skbMAA5T8Hkm4OiSTf2a78E0zIKLGZg7yu9FDII
tWYWokG96MXEBAdOuH+wWYmaEexh51ONrfFwKDuDMZh7MO20TTEQU8oQdjRRoAofXvTcj22GSM
TY6XleskZX2ZKxSqdd1tCtkjGRKHSTYza3zLHbBiJTIJw4z6sw9FyTTApG66UAKntiMalr9nqT
TNaxRWEXMEQVRLzAL2F9aqjgW65xrbYXu/J9Y/SYTCyBX2SRA/JkQ+Y8F68K0oS1pvK1p5/FcE
DvprTNDs4lf+aJ3HNWuK5wOsrpBhMlb2IfLuK/9QwPh9IC/RhHRfimyTPRXAf73cehNdp8DpKw
Lm+jr30vazFwICpvSbi6Etb6GXfPkKaX7ztpQBqG92m2/0g3LWfPt1lzwrPHPBz8y1qQMU268D
oo8YvWtI4KGaDAFb6XQhR6t6mqoq/3IP6/g//PZVENsYUVsPLDJLLF9fiOWtBMZnaiscKv8SGE
s//B9JkKrdSRRQRZcnnPjJnJLILblRVAZGuXpSKSYVPzYmOjUx3sSeLSiPoSOcqRIJ0X3s4ED0
92W3tR4ZXK3fnkFyrIVtRJsB3k/2smiQ6Pc1VuKHh1yTzYjXKRQcDaY3EDP9IWFtjiUfZQoZci
jMWt6YXim23m2aN2Ed8qIedikR6OjFHE4Kus/2yegTszSs5CrM7NamKWzeIeNNth/cTcmT++GD
umsGNTBAsHHSq1KYpqLi4GKLHzU7WNCQRdAcIDEvMZH/CHlmZK7bzb9z038rPf/D5WZrcK1ttD
5BjTJjj7GerS0xLkvYIklaJqurjMdWYmQtT4JAHF90/zRKqFFVpSiW074bRQ+PfaLI5C+TwoX5
lYD+R91A0qyGKIkJfITa8hZFY+Up+rSuREqnpAvdAVL9/gLPF6I+5+D+sVBsGRbw2rFVRbCHdwa
TQcAVPeJJy0f/+sOs/PXoejr3siORpf8iLLYOaziGYf1EtunFcCLj8PEOznaUyouJ+lm9YKPBs
LULC/sVvy6XUARyFjfq0Ag3lYXpJeWPBORxVP/VCm8d/sNjWTQXGN/IjNZaZulixNgq5nRkPBK
wF23ZUYG4pLGpGR0Lup9nLSgEbpiDmN1Gq/IHSfI/8HpG/yRAoCdqUdre3yL/f9caj8RBBHRYb
bfRxtYQ9u2vsrqoloZ7F+Mu+kjuc9BxCMvJ7JaKwvQJckAkzTo6t10t6MzwiqJ7Au+2oOJ2Ukb
/985+TFGS219fmqWfwisOfpuvSkjRj8vIDBBm9itKIS+pVpfz+Mg7kl3WmkUrgF3yjTH5/C51u
aSzK2KeEVoWPx/Ps2CX7ATo6AsETp8Na38dT6d+Dm4WM4sBieKt/yOEFhiBNkgpVKAqawKRvLW
3U73OIKC8VLFhnhU+ogGxcUq5mZXvMbNDIaU2LvtmtPPo/qL0bOYu76TKc1ZX0R6AXkeImQgRP
sdeXPPANTw3la585oZbYxUXRfEIEkmkcv3eSGnPCVesbxxd1SaIJe2j7H9MbHdjYkeFQuECnUh
Kxg63BVPl/qAEIO5+OKBzm7ctuP8apeGWliHAueKzJXc5IEFS/3iwkfDLRkrGzBeNIL0IINO3C
oGSvn95Z8+LhNSopyqt3uB4rQksUYIwXgkfrEVYujCO0T5dSkk5j10X7WlDm4DHZVLJH+GtL6v
9A6xFJNDQfQF0hS+wLXkTkMq7pUiX+Qohf8QRJZEyU5VWo2CesR63j1MFpkB3xybpbjt8oI47X
C20GEn3uCjwMwq/3K4ibHnqi16pPPRgI/u3R9TVfvOC2e0xgl1rFG6cKUfoguXoxHqP1KKjUw
23bpd9L09LzSDdSHcoDPokWzDee0ZP/Z6VH3rdjQR71kw4VBeT8nKfLP2dGBd0tpWDQhCFK7I9
axxxthnv0v09x/J7jhyoLRt5e8lMEfrqtnMWdqjFgYVEQndthZ+9/Xvfnk6f5MD8fDheMuvbNT
hduFSZEcZCLlW4GWKneVji4wdBrV3aCrzAzxy0H7y7nnkyCEvac503UDtr1bk1VJIVsYfYrN2S
2DPbp3H2E8r/n6jfbilwFyp3JTJvnRqQTcYHXDieW8Njq46JO6O6wsPwKQTKMfHGxxTRJdRe5y
vJD54xvFWwlYEJ/Q2c8cr1NNXEN32e5psfIJ7o48k6bsiyXnbHKSjK781Z5h8Hc3FbUF2U2p5J
qLwcD7+bknEunsbWSC37iMk7oweF3hMhKRMm9iYJ8tpxMRcWCot7ador+Y2fYWBSu/bwXwcRI0
8TElMCMGCSqGSib3DQeJFTEWBBRymjnEbJmrRwh4sRnwudfSQP6KDAXMCEwCQYFKw4DAhFAA
QU+YFhgKEYjfxN/cL70yRrJSHFgUwECHeCTQnUEU0BAgIIAA==\" }"

```
# The response:
{
  "num_records": 1,
  "records": [
```

```

{
  "uuid": "024cd3cf-9a08-11ea-8d52-005056bbeba5",
  "svm": {
    "uuid": "4f7abf4c-9a07-11ea-8d52-005056bbeba5",
    "name": "vs0"
  },
  "client_id": "client1",
  "tenant_id": "tenant1",
  "name": "https://mykeyvault.azure.vault.net/",
  "key_id": "https://keyvault-test.vault.azure.net/keys/key1",
  "_links": {
    "self": {
      "href": "/api/security/azure-key-vaults/024cd3cf-9a08-11ea-8d52-005056bbeba5"
    }
  }
}
]
}

```

'''

=== Retrieving the AKVs configured for all clusters and SVMs

The following example shows how to retrieve all configured AKVs along with their configurations.

The API:

GET /api/security/azure-key-vaults

The call:

curl -X GET 'https://<mgmt-ip>/api/security/azure-key-vaults?fields=*

The response:

```

{
  "records": [
    {
      "uuid": "024cd3cf-9a08-11ea-8d52-005056bbeba5",
      "scope": "svm",
      "svm": {
        "uuid": "4f7abf4c-9a07-11ea-8d52-005056bbeba5",
        "name": "vs0"
      }
    },

```

```

    "client_id": "client1",
    "tenant_id": "tenant1",
    "name": "https://mykeyvault.azure.vault.net/",
    "key_id": "https://keyvault-test.vault.azure.net/keys/key1",
    "authentication_method": "client_secret",
    "_links": {
      "self": {
        "href": "/api/security/azure-key-vaults/024cd3cf-9a08-11ea-8d52-005056bbbeba5"
      }
    }
  },
  {
    "uuid": "85619643-9a06-11ea-8d52-005056bbbeba5",
    "scope": "cluster",
    "client_id": "client1",
    "tenant_id": "tenant1",
    "name": "https://mykeyvault.azure.vault.net/",
    "key_id": "https://keyvault-test.vault.azure.net/keys/key1",
    "authentication_method": "certificate",
    "_links": {
      "self": {
        "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbbeba5"
      }
    }
  }
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/security/azure-key-vaults?fields=*"
  }
}
}
}
-----
'''

```

=== Retrieving the AKV configured for a specific SVM

The following example retrieves a configured AKV for a specific SVM.

The API:


```
GET /api/security/azure-key-vaults
```

```
# The call:
```

```
curl -X GET 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5?fields=*
```

```
# The response:
```

```
{
  "uuid": "85619643-9a06-11ea-8d52-005056bbeba5",
  "scope": "cluster",
  "client_id": "client1",
  "tenant_id": "tenant1",
  "name": "https://mykeyvault.azure.vault.net/",
  "key_id": "https://keyvault-test.vault.azure.net/keys/key1",
  "authentication_method": "client_secret",
  "_links": {
    "self": {
      "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5"
    }
  }
}
```

```
----
```

```
'''
```

=== Retrieving the advanced properties of an AKV configured for a specific SVM

The following example retrieves the advanced properties of a configured AKV for a specific SVM.

```
----
```

```
# The API:
```

```
GET /api/security/azure-key-vaults
```

```
# The call:
```

```
curl -X GET 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5?fields=state,azure_reachability,ekmip_reachability'
```

```
{
  "uuid": "fc0b7718-18c9-11eb-88e3-005056bb605d",
  "name": "https://10.234.237.18",
  "state": {
    "cluster_state": true,
```

```

    "message": "",
    "code": 0
  },
  "azure_reachability": {
    "reachable": true,
    "message": "",
    "code": 0
  },
  "ekmip_reachability": [
    {
      "node": {
        "uuid": "d208115f-7721-11eb-bf83-005056bb150e",
        "name": "node1",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/d208115f-7721-11eb-bf83-005056bb150e"
          }
        }
      },
      "reachable": true,
      "message": "",
      "code": 0
    },
    {
      "node": {
        "uuid": "e208115f-7721-11eb-bf83-005056bb150e",
        "name": "node2",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/e208115f-7721-11eb-bf83-005056bb150e"
          }
        }
      },
      "reachable": true,
      "message": "",
      "code": 0
    }
  ],
  "_links": {
    "self": {
      "href": "/api/security/azure-key-vaults/fc0b7718-18c9-11eb-88e3-005056bb605d"
    }
  }
}

```

```
}  
----
```

```
'''
```

=== Updating the client secret of a specific SVM

The following example updates the client secret of a configured AKV for a specific SVM.

```
----
```

```
# The API:
```

```
PATCH /api/security/azure-key-vaults
```

```
# The call:
```

```
curl -X PATCH 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-  
9a06-11ea-8d52-005056bbeba5' -d "{ \"client_secret\": \"newSecret\" }"
```

```
----
```

```
'''
```

=== Updating the client certificate and key of a specific SVM

The following example updates the client certificate and key of a configured AKV for a specific SVM.

```
----
```

```
# The API:
```

```
PATCH /api/security/azure-key-vaults
```

```
# The call:
```

```
curl -X PATCH 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-  
9a06-11ea-8d52-005056bbeba5' -d "{ \"client_certificate\":  
\"MIIQKQIBAzCCD+8GCSqGSIB3DQEHAaCCD+AEgg/cMIIP2DCCBg8GCSqGSIB3DQEBqCCBgAw  
ggX8AgEAMIIIF9QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIWkY7ojViJDYCAggAgIIFyJ  
PjIfmM6yTCKVw5ep2oZLwwvRca8pKhISVjw+WjWngh/f6Py/Ty0CwCjDFUZPsUUdSmk78E7SAz  
0CpQyBwmUuFJQShjZjftHLKRWld3O4sJKB8DzH9Yw1C7En94cyJ1rT4WYoVFmeJcmOXx6h+NFH  
c7njtXVsKwxc5BF88K3+3kHdV3WyVdXoeXe7yY/+EjFfjtBryp8ljuielX/NFlh5kowhoj+yxn  
00c1/0OI1iV3mTIOTXD8qrZVp9ZhAxSTRBd5uDyWMfppqxW2L+9vCUU+ZgmRxtU3VsRLOp/T14  
0OP7Sn1Ch2OE0bIrbYYtcpi04QcUtefEJBMlbbTbJPHDAtiO2KIQKviZL4QMZgho9NNgL4MUpIb  
NSzDCbuIC+nNMxfghs0nPZewY+b43H/tMmnZ8Q4kiCfwrUqbFbflBiPMOaJsS0eQaJhDmzM90Q  
EgbesHWgPreAcfMUcN1+BaqHFLHUxLXDxQix6zYiCAtdX6/EKlirRh1TFpmFX2PBd+X6uODhwm  
m4ub9RKj3In8t5qgtN4q/mTBXjAVDAbTIIIEgobBRaXGSSXCBC9W/jRed0DRZD9Bm8T/nV39sZN  
ducwZa5ojYTX8fFMA0cfY6IFivXHjB00coHEEGdgCfC0G8vACqLbb+2NuhMJPtR7Ig50iAPUMc  
670Z5ItOTQhyYOZ/KagOtvV8sKPCzeAkcMoHlsm189V79zt1fCJQTVWnaGiMj5Orcbskk6vCxh
```

DGeU6q1kgvXJKXOYRF8/wIpv8Y7/rEpnGwE/I0ZOXzdIDHXqA53B1zyOVem25ezWCD+kpoH89X
JssYlNjIMJhjVRED6lw/DbSXg2yFu/v3ckGapVvTuyAiz5hWUNfl3pt++da6GoekKnLqtL4G/R
GXCnebLbXg838dlTGBznoCwGTVxXDeVYafz8AjI10qYtTMcbN56ya9kK7IHSkrnFX24xQRQOfm
D0Vob71lpjdz8r1aXKvD/1X2TkYJHoeEHq0nWpU8vwdG/xhv4YgKJGN9qsEZgiTXETUh5gak8e1
tGNkP+fum+1Oql05oS+Swna5/eB8eFeJl2Oi48Xi5UapaTRHPFp6kZfPXOu9cEjhILowRIi6gl
g7FUbmoJcu5OvDIyP9JlyQklw2VtgNlm1QOIvzRenXmy18XnP50NTxx2cIwby8tIcdSn2C2qhj
8Gk7q8oxVZGiBgtz4BwyzyKkypwm60BBRrHpAKLw6JM5RISeZnYQfIsId0tGgb6lgo0RJf0sFt
buvZcSvLI+2Onj8KH1TlmMR4dbuCWE9Ym4sVRmD1D6/f6BoNH0DRg7TJkEFbOadJsNPGzHbKte
LdaSMGTNUZ3hEDQeomakQMfvCgypbOLxrTTqfbenHRTn+iFNYW0zCUW6EJoAXp+lqFnwQL52I1
2QxwZike01P2k0GharzAJkXnNaFGnmHIIP6wJrCCSDZwDmr7GI2R5evDlRi17QUg2sulxQV0U8
zezzwIUgEe/Whf0ngGJv/QcsL2jyri/tSQbUWs4g+yep4S1E3iddhfqSJzI2iKdAE+HLiHGVO1
z70fGES06dPLnmh4eoWidgZi9N/SoBy1aT0JpIQ6z6N5ImPFDWu9Y6TWXUg1iyOIXGsXIQVIgU
NoB5Ru/ApDxpYpFlk0fH9k9OnEWK5Im33puOQKLno1uwrOmdBG8+x1EY8wc9FvkHGH0Zh4Hydi
CVUcYSdiGWUxVmgm4OgyiYzcpB+Ar2dzikGc4pBg8fa1a1HN5Q3TK3w4h/HeOulmA4vWOYuVO1
H93ILGP6PWfkug+1Tam6+8yD0W5meiz0UIZR8TF/9gDb4+4wTFnPwgfTrggEauA8tt8uJtiyBC
rYexgZTXIZGTUj/86KXQaJKCreRr/kqWJOWqkNW4CGUVzw7LiI+sArOZqUp/TsxnbcNC73XCMN1
PsnByb2zCeK13V26Cr184U9sDuqQTRaIse01MN9AAjpa2QWEwggnBBgkqhkiG9w0BBwGgggmy
BIIJrjCCCaowggmmBgsqhkig9w0BDAoBAqCCCW4wgg1qMBwGCiqGSIb3DQEMAQMwDgQIEjm88b
1+pnkCaggABIIJSDD3P+vn1lSolmQvmYgZVfV37T3KpurJvMxQScPvalWiF7Q1Iwasf/+N0hKK
Nr2j/aGZLunLkaG6mLPeBP212LCwnUxDu5kYffVVE90WX/bXewbYQribwFNkNhUrSgen8BfhnR
lvDrzbBLoHivDrUFszSVBCYh31Vwgu8p9SjC8K/XlumcLdjSFko85XpoK23euhowjWH+X0kRoY
GzorcdNE8z03BKvfR61W2XWzTSaWQ6eZHG6UrnX5Fe/w50U9tMIi3BCCCqgapUHVdmHqKkMWL
ikX8LssUcN30JVeK2aJ9v4Y06CoegKAMVDS0tVSov3KbGC3GNX6lgHu4y1LOZPlPLfPXb0wDH
qavlXK3zpHl8sIRzuX3HXSdEdenHYAkSV/IQZ89h+CZUkf0nu/og8eoA8ATDA5g7fj3HXpQ6cY
drUBaHc7ruxHOiWR0GcT4XK4TTz7zZTO1wWPViprUo6ayw0dYZSG22MeDA027YirM044Ifosn9
CsqnNLZoOWvA2ao4ippDoBRqv5Hv6n0I3fOAYS5nPq3jJtKQ5neqUYo0MrAkoKHo0h6zn0Bfvi
syB88aM9N0mPD76ykbAERq7151biKbA2tk8bb9dy/sJmk2ojM/D/W1YtrNL4iM6azL2kVN5eiC
hxCoF33/RuRpXfGR8YNeJt17bq42wL70QKDBRoG1TPcLqdVqz74oshlRspfqvZsbsUatbASBt2
T0YG4zfgfGh7sb2ezyougVvzdp77wAJ6n39dc/ZLDdYDzFkQb07984y8LlhIM1AcwFcMh43gWp
6A8CJ02174ednirSqSVOPZ7K9dRw6Y0X8MB4/WGzEcvFeHYIGLBcXi1sBY5wjWnbeuhlWLiSkM
DQRB6oGOvF7bJsilKx5PwgWbbqw8KUSuU01skbMAA5T8Hkm40iStf2a78E0zIKLGZg7yu9FDII
tWYWOKG96MXEBAdOuH+wWYmaEexh51ONrfFwKDuDMZh7MO20TTEQU8oQdjRRoAofXvTcj22GSM
TY6XleskZX2ZKxSQdD1tCtkjGRKHSTYza3zLHbBiJTIJw4z6sw9FyTTApG66UakNtiMa1r9nqT
TNaxRWEXMEQVRLzAL2F9aqjgW65xrbYXu/J9Y/SYTcybX2SRA/JkQ+Y8F68KOoS1pvK1p5/FcE
DvprTNDS4lf+aj3HNWuK5wOsrpBhMlb2IfLuK/9QwPh9IC/RhHRfimyTPRXAf73cehNdp8DpKw
Lm+jr30vazFwICpvSbi6Etb6GXfPkKaX7ztpQBqG92m2/0g3LWfPt1lzwRPHPBz8y1qQMU268D
oo8YvWtI4KGaDAFb6XQhR6t6mqoq/3IP6/g//PZVENsYUVsPLDJ1LF9fiOWTbMZnaiscKv8SGE
s//B9JkKrdSrrQRZcnnPjJnJLILblRVAZGuXpSKSYVPzYmOjUx3sSeLSiPoSOcqRIJ0X3s4ED0
92W3tR4ZXK3fnkFyrIVtRJsB3k/2smiQ6PclVuKHh1yTzYjXKRQcDaY3EDP9IWFtjiUfZQoZci
jMWt6YXim23m2a2Ed8qIedikR6OjFHE4Kus/2yegTszSs5CrM7NamKWzeIeNNth/cTcmT++GD
umsGNTBAsHHSq1KYpqLi4GKLHzU7WNCQRdAcIDEvMZH/CHlmZK7bzb9z038rPf/D5WZrcK1ttD
5BjTJjj7GerS0xLkvYiklaJqurjMdWYmQtT4JAHF90/zRKqFFVpSiW074bRQ+PfaLI5C+TwoX5
lYD+R91A0qyGKIkiFITA8hZFY+Up+rSuREqnpAvdAVL9/gLPF6I+5+D+sVBsGRbw2rFVRbCHdwa
TQcAVPeJJy0f/+sOs/PXoejr3siorpf8iLLYOaziGYf1EtunFcCLj8PEOznaUyouJ+lm9YKPBS
LULC/sVvy6XUARyFjfq0Ag31YXpJeWPBORxVP/VCm8d/sNjWTQXGN/IjNZaZuliXNgq5nRkPBK
wF23ZUYG4pLGpGROLup9nLSgEbpiDmN1Gq/IHSfi/8HpG/yRAoCdqUdre3yL/f9caj8RBBHRYb

```
bfRxytQ9u2vsrqoloz7F+Mu+kjuc9BxCMvJ7JaKwvQJckAkzTo6t10t6MzwiqJ7Au+2oOJ2Ukb
/985+TFGS219fmqWfwisOfpuvSkjRj8vIDBBm9itKIS+pVpfz+Mg7kl3WmkUrgF3yjTH5/C51u
aSzK2KeEVoWPx/Ps2CX7ATo6AsETp8Na38dT6d+Dm4WM4sBieKt/yOEFhiBNkgpVKAqawKRvLW
3U73OIKC8VLFhnnU+ogGxcUq5mZXvMbNDIaU2LvtmtPPo/qL0bOYu76TKc1ZX0R6AXkeImQgRP
sdeXPPANTW31a585oZbYxUXRfEIEKmkcv3eSGnPCVesbxxdlSaIJe2j7H9MbHdjYkeFQuECnUh
Kxg63BVP1/qAEIO5+OKBzM7ctuP8apeGW1iHAueKzJXc5IeFS/3iwkfDLRkrgzBeNIL0IINo3C
oGSvn95Z8+LhNSopyqt3uB4rQksUYIwXgkfrEVYujCO0T5dSkk5j10X7WlDm4DHZVLJH+GtL6v
9A6xFJNDQfQF0hS+w1XkTkMq7pUiX+Qohf8QRJZEyU5VWo2CesR63j1MFpkB3xybpbjt8oI47X
C20GEn3uCjwMwq/3K4ibHnqi16pPPRgI/u3R9TVfvOC2e0xgllrFG6cKUfoguUaXoxHqP1KKjUw
23bpd9L09LzSDdSHcoDPokWzDee0ZP/Z6VH3rdjQR71kw4VBeT8nKfLP2dGBd0tpWDQhCFK7I9
axxxthnv0v09x/J7jhYoLrt5e8lMEfrqtnMWdqjFgYVEQndthZ+9/Xvfnk6f5MD8fDheMuvbNT
hduFSZEcZCL1W4GWKneVji4wdBrV3aCrzAzxy0H7y7nnkyCEvac503UDtr1bk1VJIVsYfYrN2S
2DPbp3H2E8r/n6jfbilwFyp3JTJvnRqQTcYHXDieW8Njq46JO6O6wsPwKQTKMfHGxxTRJdRe5y
vJD54xvFWw1YEJ/Q2c8cr1NNXEN32e5psfIJ7o48k6bsiyXnbHKSjK781Z5h8Hc3FbUF2U2p5J
qLwcD7+bknEunsbWSC37iMk7oweF3hMhKRMm9iYJ8tpxMRcWCot7ador+Y2fYWBSu/bwXwcRI0
8TElMCMGCSqGSib3DQEJFTEWBBRymjnEbJmrRwh4sRnwudfSQP6KDAxMCEwCQYFKw4DAhFAA
QU+YFhgKEYjfxN/cL70yRrJSHFgUwECHeCTQnUEU0BAgIIAA==\" }"
```

'''

=== Deleting an AKV configuration for a specific SVM

The following example deletes a configured AKV for a specific SVM.

The API:

```
DELETE /api/security/azure-key-vaults
```

The call:

```
curl -X DELETE 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-
9a06-11ea-8d52-005056bbeba5'
```

'''

=== Restoring the keys for a specific SVM configured with an AKV

The following example restores all the keys of a specific SVM configured with an AKV.

The API:

```
POST security/azure-key-vaults/{uuid}/restore
```

```
# The call:
curl -X POST 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5/restore'
```

```
# The response:
{
  "job": {
    "uuid": "6ab6946f-9a0c-11ea-8d52-005056bbeba5",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6ab6946f-9a0c-11ea-8d52-005056bbeba5"
      }
    }
  }
}
}
-----

'''
```

=== Rekeying the internal key for a specific SVM configured with an AKV

The following example rekeys the internal key of a specific SVM configured with an AKV.

```
# The API:
POST security/azure-key-vaults/{uuid}/rekey-internal
```

```
# The call:
curl -X POST 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5/rekey-internal'
```

```
# The response:
{
  "job": {
    "uuid": "6ab6946f-9a0c-11ea-8d52-005056bbeba5",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6ab6946f-9a0c-11ea-8d52-005056bbeba5"
      }
    }
  }
}
}
}
-----
```

```

[[ID135726beb2704926d089f12c8b5d1605]]
= Retrieve AKVs configured for all clusters and SVMs

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/azure-key-vaults`#

*Introduced In:* 9.8

Retrieves AKVs configured for all clusters and SVMs.

== Related ONTAP commands

* `security key-manager external azure show`
* `security key-manager external azure check`

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|authentication_method
|string
|query
|False
a|Filter by authentication_method

* Introduced in: 9.10

|scope
|string
|query
|False
a|Filter by scope

```

```
|svm.uuid  
|string  
|query  
|False  
a|Filter by svm.uuid
```

```
|svm.name  
|string  
|query  
|False  
a|Filter by svm.name
```

```
|proxy_port  
|integer  
|query  
|False  
a|Filter by proxy_port
```

```
|name  
|string  
|query  
|False  
a|Filter by name
```

```
|state.message  
|string  
|query  
|False  
a|Filter by state.message
```

```
|state.available  
|boolean  
|query  
|False  
a|Filter by state.available
```

```
|state.code  
|integer  
|query
```



```
|False
a|Filter by state.code

|key_id
|string
|query
|False
a|Filter by key_id

|client_id
|string
|query
|False
a|Filter by client_id

|proxy_type
|string
|query
|False
a|Filter by proxy_type

|uuid
|string
|query
|False
a|Filter by uuid

|proxy_username
|string
|query
|False
a|Filter by proxy_username

|azure_reachability.message
|string
|query
|False
a|Filter by azure_reachability.message

|azure_reachability.code
```

```
|integer
|query
|False
a|Filter by azure_reachability.code

|azure_reachability.reachable
|boolean
|query
|False
a|Filter by azure_reachability.reachable

|tenant_id
|string
|query
|False
a|Filter by tenant_id

|proxy_host
|string
|query
|False
a|Filter by proxy_host

|ekmip_reachability.message
|string
|query
|False
a|Filter by ekmip_reachability.message

|ekmip_reachability.code
|integer
|query
|False
a|Filter by ekmip_reachability.code

|ekmip_reachability.reachable
|boolean
|query
|False
a|Filter by ekmip_reachability.reachable
```

```
|ekmip_reachability.node.uuid
|string
|query
|False
a|Filter by ekmip_reachability.node.uuid
```

```
|ekmip_reachability.node.name
|string
|query
|False
a|Filter by ekmip_reachability.node.name
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_timeout
|integer
|query
|False
a|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
```

```
|return_records
|boolean
|query
|False
```

a|The default is true for GET calls. When set to false, only the number of records is returned.

* Default value: 1

|order_by
|array[string]
|query
|False

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#azure_key_vault[azure_key_vault]]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{

```

    "_links": {
      "next": {
        "href": "/api/resourcelink"
      },
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "records": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "authentication_method": "client_secret",
      "azure_reachability": {
        "code": 346758,
        "message": "AKV service is not reachable from all nodes - reason."
      },
      "client_certificate":
"MI IQKQIBAzCCD+8GCSqGS Ib3DQEHAaCCD+AEgg/cMI IP2DCCBg8GCSqGS Ib3DQEHBqCCBgAwg
gX8AgEAMIIF9QYJKoZIhvcNAQcBMBwGCiqGS Ib3DQEMAQYwDgQIWKY7ojViJDYCAggAgIIFyJP
jIfmM6yTCKVw5ep2oZLwvRca8pKhISVjw+WjWngh/f6Py/Ty0CwCjDFUZPsUUdSmk78E7SAz0
CpQyBwmUuFJQShjZjftHLKRWld3O4sJKB8DzH9Yw1C7En94cyJ1rT4WYoVFmeJcmOXx6h+NFHc
7njtXVsKwxc5BF88K3+3kHdV3WyVdXoeXe7yY/+EjFfjtBryp8ljuielX/NFlh5kowhoj+yxnO
0c1/0OIliV3mTIOTXD8qrZVp9ZhAxSTRBd5uDyWMfppqxW2L+9vCUU+ZgmRxtU3VsRLOp/T140
OP7Sn1Ch2OE0bIrbYYtcpi04QcUtfEJBMlbbTbJPHDAtiO2KIQKviZL4QMZgho9NNgLMUpIbN
SzDCbuIC+nNMxfGfs0nPZewY+b43H/tMmnZ8Q4kiCFwrUqbFbflBiPMOaJsS0eQaJhDmzM90QE
gbesHWgPreAcfMUCn1+BaqHFLHUxLXDxQix6zYiCatDX6/EKlirRh1TFpmFX2PBd+X6uODhmwm
4ub9RKj3In8t5qgtN4q/mTBXjAVDABTII EGobBRaXGSSXCBC9W/jRed0DRZD9Bm8T/nV39sZNd
ucwZa5ojYTX8fFMA0cfY6IFivXHjB00coHEEGdGcFC0G8vACqLbb+2NuhMJPtR7Ig50iAPUMc6
70Z5ItOTQhyYOZ/KagOtvV8sKPCzeAkcMoHlsm189V79zt1fCJQTVWnaGiMj5Orcbskk6vCxhD
GeU6q1kgvXJKXOYRF8/wIpv8Y7/rEpnGwE/I0ZOXzdIDHXqA53B1zyOVem25ezWCD+kpoH89XJ
ssY1nJIMJhjVRED61w/DbSXg2yFu/v3ckGapVvTuyAiz5hWUNfl3pt++da6GoekKnLqtL4G/RG
XCnebLbXg838dlTGBznoCwGTVxXDeVYafz8AjI10qYtTMcbN56ya9kK7IHSkrnFX24xQRQOfmD
0Vob71pjdZ8rlaXKvD/1X2TkYJHoeEHq0nWpU8vwdG/xhv4YgKJGN9qsEZgiTXETUh5gak8elt
GNkP+fum+1OqlO5oS+Swna5/eB8eFeJl2Oi48Xi5UapaTRHPFp6kZfPXOu9cEjhILowRIi6glg
7FubmoJcu5OvDIyP9JlyQklw2VtgNlm1QOIvzRenXmy18XnP50NTxx2cIwby8tIcdSn2C2qhj8
Gk7q8oxVZGiBgtz4BwyzyKkypwm60BBRrHpAKLw6JM5RISeZnYQfIsId0tGgb61go0RJf0sFtb
uvZcSvLI+2Onj8KH1TlmMR4dbuCWE9Ym4sVRmD1D6/f6BoNH0DRg7TJkEFbOadJsNPGzHbKteL
daSMGTNUZ3hEDQeomakQMfvCgypbOLxrtTqfbenHRtN+iFNYW0zCUW6EJoAXp+lqFnwQL52Il2
QxwZike01P2k0GharzAJkXnNaFGnmHIIP6wJrCCSDZwDmr7GI2R5evDlRi17QUg2sulxQV0U8z
ezzwIUgEe/Whf0ngGJv/QcsL2jyri/tSQbUWs4g+yep4SlE3iddhfqSJzI2iKdAE+HLiHGVO1z
70fGES06dPLnmh4eoWidgZi9N/SoBylaT0JpIQ6z6N5ImpFDWu9Y6TWXUg1iyOIXGsxiQVIgUN
oB5Ru/ApDxpYpFLk0fH9k9OnEWK5Im33puOQKLno1uwrOmdBG8+x1EY8wc9FvkHGH0Zh4HydiC
VUCYSdiGWUxVmgm4OgyiYzcpB+Ar2dzikGc4pBg8fa1a1HN5Q3TK3w4h/HeOulmA4vWOYuVO1H

```

93ILGP6PWfkg+1Tam6+8yD0W5meiZ0UIZR8TF/9gDb4+4wTFnPwgfTrggEauA8tt8uJtiyBCr
YexgZTXIZGTUj/86KXQaJKCreRr/kqwJOWqkNW4CGUVzw7LiI+sArOZqUp/TsxnbcNC73XCMNlP
snByb2zCeK13V26Cr184U9sDuqQTJRaIse0lMN9AAjpa2QWEwgggnBBgkqhkiG9w0BBwGgggmyB
IIJrjCCCaowggmmBgsqhkig9w0BDAoBAqCCCW4wgg1qMBwGciqGSib3DQEMAQMwDgQIEjm88b1
+pnkCAggABIIJSDDD3P+vn1lSolmQvmYgZVfV37T3KpurJvMxQScPvalWiF7Q1Iwasf/+N0hKKN
r2j/aGZLunLkaG6mLPeBP2l2LCwnUxDu5kYffVVE90WX/bXewbYQribwFNkNhUrSgen8BfhnRl
vDrzbBLoHIvDrUFszSVBCYh31Vwgu8p9SjC8K/XlumcLdjSFko85XpoK23euhowjWH+X0kRoYG
zorcdNE8z03BKvfR6lW2XWzTSaWQ6eZHG6Urn5Fe/w50U9tMIi3BCCCqgapUHVdmHqKkmWLi
kX8LssUcn30JvekM2aJ9v4YO6CoegKAMVDs0tVSov3KbGC3GNX6lgHu4y1LOZPLPLfPXb0wDHq
avlxK3zphl8sIRzuX3HXSdEdenHYAkSV/IQZ89h+CZUkf0nu/og8eoA8ATDA5g7fj3HXpQ6cYd
rUBaHc7ruxHOiWR0GcT4XK4TTz7zZTO1wWPViprUo6ayw0dYZSG22MeDA027YirM044Ifosn9C
sqnNLZoOWvA2ao4ippDoBRqv5Hv6n0I3fOAys5nPq3jJtKQ5neqUYo0MrAkoKHO0h6zn0Bfvis
yB88aM9N0mPD76ykbAERq7151biKbA2tk8bb9dy/sJmk2ojM/D/W1YtrNL4iM6azL2kVN5eiCh
xCof33/RuRpXfGR8YNeJTl7bq42wL70QKDBRoG1TPcLqdVqz74oshlRspfqvZsbsUatbASBt2T
0YG4zfGfGh7sb2ezyougVvzdp77wAJ6n39dc/ZLDDyDzFkQb07984y8LlhIM1AcwFcMh43gWp6
A8CJ02l74ednirSqSVOPZ7K9dRw6Y0X8MB4/WGzEcVFeHYIGLBcXilSBY5wjWnbeuhlwLiSkMD
QRB6oGOvF7bJsilkx5PwgWbbqw8KUSuU01skbMAa5T8Hkm4OiSTf2a78E0zIKLGZg7yu9FDIIt
WYWOKG96MXEBADouH+wWYmaEexh5lONrfFwKDuDMZh7MO20TTEQU8oQdjRRoAofXvTcj22GSMT
Y6XleskZX2ZKxSQdDlctCtkjGRKHSTYza3zLHbBiJTIJw4z6sw9FyTTApG66UAkNtiMalr9nqTT
NaxRWEXMEQVRLzAL2F9aqjgW65xrbYXu/J9Y/SYTcybX2SRA/JkQ+Y8F68KOoS1pvK1p5/FcED
vprTNDs4lf+aj3HNWuK5wOsrpBhMlb2IfLuK/9QwPh9IC/RhHRfimyTPRXAf73cehNdp8DpKwL
m+jr30vazFwICpvSbi6Etb6GXfPkKaX7ztpQBqG92m2/0g3LWfPtilzwrPHPBz8y1qQMU268Do
o8YvWtI4KGaDAFb6XQhR6t6mqoq/3IP6/g//PZVENsYUVsPLDJlLF9fiOwTbMZnaiscKv8SGEs
//B9JkKrdSrRQRZcnnPjJnJLILblRVAZGuXpSKSYVPzYmOjUx3sSeLSiPoSocqRIJ0X3s4ED09
2W3tr4ZXK3fnkFyrIVtRJsB3k/2smiQ6PclVuKHhlyTzYjXKRQcDaY3EDP9IWftjiUfZQoZcij
MWt6YXim23m2aNEd8qIedikR6OjFHE4Kus/2yegTszSs5CrM7NamKWzeIeNnth/cTcmT++GDu
msGNTBAShHsq1KYpqli4GKLHzU7WNCQRdAcIDEvMZH/CHlmZK7bzb9z038rPf/D5WZrcKl1ttd5
BjTJjj7GerS0xLkvYiklAJqurjMdWYmQtT4JAHF90/zRKqFFVpSiW074bRQ+PfaLI5C+TwoX5l
YD+R91A0qyGKIkJfITa8hZFY+Up+rSuREqnpAvdAVL9/gLPF6I+5+D+sVBsGRbw2rFVRbCHdwaT
QcAVPeJJy0f/+sOs/PXoejr3siORpf8iLLYOaziGYf1EtunFcCLj8PEOznaUyouJ+lm9YKPBSL
ULC/sVVy6XUARyFJfQ0Ag31YXpJeWPBORxVP/VCm8d/sNjWTQXGN/IjNZaZuliXNgq5nRkPBKw
F23ZUYG4pLGpGROLup9nLSgEbpIDmN1Gq/IHSfI/8HpG/yRAoCdqUdre3yL/f9caj8RBBHRYbb
fRxytQ9u2vsrqoloZ7F+Mu+kjuc9BxCMvJ7JaKwvQJckAkzTo6t10t6MzwiQJ7Au+2oOJ2Ukb/
985+TFGS219fmqWfwisOfpuvSkjRj8vIDBBm9itKIS+pVpfz+Mg7kl3WmkUrgF3yjTH5/C51ua
SzK2KeEVoWPx/Ps2CX7ATo6AsETp8Na38dT6d+Dm4WM4sBieKt/yOEFhiBNkgpVKAqawKRvLW3
U73OIKC8VLFhnnU+ogGxcUq5mZXvMbNDIaU2LvtmtPPo/qL0bOYu76TKclZX0R6AXkeImQgRPs
deXPPANtW3la585oZbYxUXRfEIEKmkcv3eSGnPCVesbxxdlSaIJe2j7H9MbHdjYkeFQuECnUhK
xg63BVPl/qAEIO5+OKBz7ctuP8apeGW1iHAueKzJXc5IeFS/3iwkfDLRkrgzBeNIL0IINo3Co
GSvn95Z8+LhNSopyqt3uB4rQksUYIwXgkfrEVYujCO0T5dSkk5j10X7WlDm4DHZVLJH+GtL6v9
A6xFJNDQfQF0hS+w1XkTkMq7pUiX+Qohf8QRJZEyU5VWo2CesR63j1MFpkB3xybpbjt8oI47XC
20GEn3uCjwMwq/3K4ibHnqil6pPPRGi/u3R9TVfvOC2e0xgllrFG6cKUfoguAoxHqP1KKjUw2
3bpd9L09LzSDdSHcoDPokWzDee0ZP/Z6VH3rdjQR71kw4VBet8nKfLP2dGBd0tpWDQhCFK7I9a
xxxthnv0v09x/J7jhhyLRt5e8lMEfrqtnMWdqjFgYVEQndthZ+9/XvfNk6f5MD8fDheMuvbNTh
duFSZEczCLlW4GWKnevji4wdBrV3aCrzAzxy0H7y7nnkyCEvac503UDtr1bk1VJIVsYfyYrN2S2
DPbp3H2E8r/n6jfbilwFyp3JTJvnRqQTcYHXDieW8Njq46JO6O6wsPwKQTKMfHGxxTRJdRe5yv
JD54xvFWw1YEJ/Q2c8cr1NNXEN32e5psfIJ7o48k6bsiyXnbHKSjK781Z5h8Hc3FbUF2U2p5Jq

```

LwcD7+bknEunsbWSC37iMk7oweF3hMhKRMm9iYJ8tpxMRcWCot7ador+Y2fYWBSu/bwXwcRI08
TElMCMGCSqGSib3DQEJFTEWBBRymjnEbJmrRwh4sRnwudfSQP6KDAxMCEwCQYFKw4DAhoFAAQ
U+YFhgKEYjfXN/cL70yRrJSHFgUwECHeCTQnUEU0BAgIIAA==",
  "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
  "client_secret": "abcdef",
  "ekmip_reachability": {
    "code": 346758,
    "message": "embedded KMIP server status unavailable on node.",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  },
  "key_id": "https://keyvault1.vault.azure.net/keys/key1",
  "name": "https://kmip-akv-keyvault.vault.azure.net/",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "svm",
  "state": {
    "code": 346758,
    "message": "Top-level internal key protection key (KEK) is
unavailable on the following nodes with the associated reasons: Node:
node1. Reason: No volumes created yet for the SVM. Wrapped KEK status will
be available after creating encrypted volumes."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzz",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
}

```

```
====
```

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```
    "arguments": {
```

```
      "code": "string",
```

```
      "message": "string"
```

```
    },
```

```
    "code": "4",
```

```
    "message": "entry doesn't exist",
```

```
    "target": "uuid"
```

```
  }
```

```
}
```

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
====
```

```
[#href]
```

```
[.api-collapsible-fifth-title]
```

```
href
```



```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]

```

a|

|===

[#azure_reachability]
[.api-collapsible-fifth-title]
azure_reachability

Indicates whether or not the AKV service is reachable from all the nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|integer

a|Code corresponding to the status message. Returns a 0 if AKV service is reachable from all nodes in the cluster.

|message
|string

a|Error message set when reachability is false.

|reachable
|boolean

a|Set to true when the AKV service is reachable from all nodes of the cluster.

|===

[#node]
[.api-collapsible-fifth-title]
node

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|
```

```
|uuid
```

```
|string
```

```
a|
```

```
|===
```

```
[#ekmip_reachability]
```

```
[.api-collapsible-fifth-title]
```

```
ekmip_reachability
```

Provides the connectivity status for the given SVM on the given node to all EKMIP servers configured on all nodes of the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|integer
```

a|Code corresponding to the error message. Returns a 0 if a given SVM is able to communicate to the EKMIP servers of all of the nodes in the cluster.

```
|message
```

```

|string
a|Error message set when cluster-wide EKMIP server availability from the
given SVM and node is false.

|node
|link:#node[node]
a|

|reachable
|boolean
a|Set to true if the given SVM on the given node is able to communicate to
all EKMIP servers configured on all nodes in the cluster.

|===

[#state]
[.api-collapsible-fifth-title]
state

Indicates whether or not the AKV wrapped internal key is available cluster
wide.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|available
|boolean
a|Set to true when an AKV wrapped internal key is present on all nodes of
the cluster.

|code
|integer
a|Code corresponding to the status message. Returns a 0 if AKV wrapped key
is available on all nodes in the cluster.

```

```
|message
|string
a|Error message set when top-level internal key protection key (KEK)
availability on cluster is false.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#azure_key_vault]
[.api-collapsible-fifth-title]
azure_key_vault
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```

|_links
|link:#_links[_links]
a|

|authentication_method
|string
a|Authentication method for the AKV instance.

|azure_reachability
|link:#azure_reachability[azure_reachability]
a|Indicates whether or not the AKV service is reachable from all the nodes
in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|client_certificate
|string
a|PKCS12 Certificate used by the application to prove its identity to AKV.

|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.

|client_secret
|string
a|Secret used by the application to prove its identity to AKV.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|key_id
|string
a|Key Identifier of AKV key encryption key.

|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.

```

```
* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri
* Introduced in: 9.8
* readCreate: 1
```

```
|proxy_host
|string
a|Proxy host.
```

```
|proxy_password
|string
a|Proxy password. Password is not audited.
```

```
|proxy_port
|integer
a|Proxy port.
```

```
|proxy_type
|string
a|Type of proxy.
```

```
|proxy_username
|string
a|Proxy username.
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|state
|link:#state[state]
a|Indicates whether or not the AKV wrapped internal key is available
cluster wide.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.
```

```

|svm
|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

```



```

|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====

[[ID3c33e800f12bc2bddb2972e84d11cffc]]
= Create an AKV configuration for all clusters and SVMs

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/azure-key-vaults`#

*Introduced In:* 9.8

Configures the AKV configuration for all clusters and SVMs.

== Required properties

* `svm.uuid` or `svm.name` - Existing SVM in which to create a AKV.
* `client_id` - Application (client) ID of the deployed Azure application

```

with appropriate access to an AKV.

- * `tenant_id` - Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV.
- * `client_secret` - Secret used by the application to prove its identity to AKV.
- * `client_certificate` - PKCS12 Certificate used by the application to prove its identity to AKV.
- * `key_id` - Key Identifier of AKV encryption key.
- * `name` - Name of the deployed AKV used by ONTAP for storing keys.

== Optional properties

- * `proxy_type` - Type of proxy (http, https etc.) if proxy configuration is used.
- * `proxy_host` - Proxy hostname if proxy configuration is used.
- * `proxy_port` - Proxy port number if proxy configuration is used.
- * `proxy_username` - Proxy username if proxy configuration is used.
- * `proxy_password` - Proxy password if proxy configuration is used.

== Related ONTAP commands

- * `security key-manager external azure enable`
- * `security key-manager external azure update-config`

== Parameters

[cols=5*,options=header]
|===

Name
Type
In
Required
Description

return_records
boolean
query
False

a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|authentication_method
|string
a|Authentication method for the AKV instance.

|azure_reachability
|link:#azure_reachability[azure_reachability]
a|Indicates whether or not the AKV service is reachable from all the nodes
in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|client_certificate
|string
a|PKCS12 Certificate used by the application to prove its identity to AKV.

|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.

|client_secret
|string
a|Secret used by the application to prove its identity to AKV.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

```

```
|key_id
|string
a|Key Identifier of AKV key encryption key.
```

```
|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.
```

```
* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri
* Introduced in: 9.8
* readCreate: 1
```

```
|proxy_host
|string
a|Proxy host.
```

```
|proxy_password
|string
a|Proxy password. Password is not audited.
```

```
|proxy_port
|integer
a|Proxy port.
```

```
|proxy_type
|string
a|Type of proxy.
```

```
|proxy_username
|string
a|Proxy username.
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```

|state
|link:#state[state]
a|Indicates whether or not the AKV wrapped internal key is available
cluster wide.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|svm
|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "authentication_method": "client_secret",
  "azure_reachability": {
    "code": 346758,
    "message": "AKV service is not reachable from all nodes - reason."
  },
  "client_certificate":
  "MIIQKQIBAzCCD+8GCSqGSIB3DQEHAaCCD+AEgg/cMIIP2DCCBg8GCSqGSIB3DQEHbqCCBgAwg
gX8AgEAMIIIF9QYJKoZIhvcNAQcBMBwGCiqGSIB3DQEMAQYwDgQIWkY7ojViJDYCAggAgIIFyJP

```

jIfmM6yTCKVw5ep2oZLwvRca8pKhISVjw+WjWngh/f6Py/Ty0CwCjDFUZPsUUDSmk78E7SAz0
CpQyBwmUuFJQShjZjftHLKRWld3O4sJKB8DzH9Yw1C7En94cyJ1rT4WYoVFmeJcmOXx6h+NFHc
7njtXVsKwxc5BF88K3+3kHdV3WyVdXoeXe7yY/+EjFfjtBryp81juielX/NFlh5kowhoj+yxnO
0c1/0OIi1v3mTIOtXDX8qrZVp9ZhAxSTRBd5uDyWMfppqxW2L+9vCUU+ZgmRxtU3VsRLOp/T140
OP7Sn1Ch2OE0bIrbYYtcpi04QcUtfeJBMlbbTbJPHDAtiO2KIQKviZL4QMZgho9NNgL4MUPIbN
SzDCbuIC+nNMXfgfs0nPZewY+b43H/tMmnZ8Q4kiCFwrUqbFbflBiPMOaJsS0eQaJhDmzM90QE
gbesHWgPreAcfMUcN1+BaqHFLHUxLXDxQix6zYiCatDX6/EKlirRh1TFpmFX2PBd+X6uODhmwm
4ub9RKj3In8t5qgtN4q/mTBXjAVDABTIIegobBRaXGSSXCBC9W/jRed0DRZD9Bm8T/nV39sZNd
ucwZa5ojYTX8fFMA0cfY6IFivXHjB00coHEEGdgCfC0G8vACqLbb+2NuhMJPT7Ig50iAPUMc6
70Z5ItOTQhyYOZ/KagOtvV8sKPCzeAkcMoHlsm189V79zt1fCJQTVWnaGiMj5Orcbskk6vCxD
GeU6q1kgvXJKXOYRF8/wIpv8Y7/rEpnGwE/I0ZOXzdIDHXqA53B1zyOVem25ezWCD+kpoH89XJ
ssY1NjIMJhjVRED61w/DbSXg2yFu/v3ckGapVvTuyAiz5hWUNfl3pt++da6GoekKnLqtL4G/RG
XCnebLbXg838dlTGBznoCwGTVxXDeVYafz8AjI10qYtTmcbN56ya9kK7IHSkrnFX24xQRQOfmD
0Vob71pjdZ8r1aXKvD/1X2TkYJHoeEHq0nWpU8vwDG/xhv4YgKJGN9qsEZgiTXETUh5gak8elt
GNKp+fum+1OqlO5oS+Swna5/eB8eFeJl2Oi48Xi5UapaTRHPFp6kZfPXOu9cEjhILowRIi6glg
7FubmoJcu50vDIyP9JlyQklw2VtgNlm1QOIvzRenXmy18XnP50NTxx2cIwby8tIcdSn2C2qhj8
Gk7q8oxVZGiBgtz4BwzyKkypwm60BBRrHpAKLw6JM5RISeZnYQfIsId0tGgb61go0RJf0sFtb
uvZcSvLI+2Onj8KH1TlmMR4dbuCWE9Ym4sVRmD1D6/f6BoNH0DRg7TJkEFbOadJsNPGzHbKteL
daSMGTNUZ3hEDQeomakQMfvcGypbOLxrTTqfbenHRtN+iFNyW0zCUW6EJoAXp+lqFnwQL52I12
QxwZikE01P2k0GharzAJkXnNaFGnmHIIP6wJrCCSDZwDmr7GI2R5evDlRi17QUg2sulxQV0U8z
ezzwIUgEe/Whf0ngGJv/QcsL2jyri/tSQbUWs4g+yep4SlE3iddhfqSJzI2iKdAE+HLiHGVO1z
70fGES06dPLnmh4eoWidgZi9N/SoBy1aT0JpIQ6z6N5ImPfDWu9Y6TWXUgliyOIXGsxiQVIgUN
oB5Ru/APDxpYpFLk0fH9k9OnEWK5Im33puOQKLno1uwrOmdBG8+x1EY8wc9FvkHGH0Zh4HydiC
VUCYSdiGWUxVmgm4OgyiYzcpB+Ar2dzikGc4pBg8fa1a1HN5Q3TK3w4h/HeOUlMA4vWOYuV01H
93ILGP6PWfkug+1Tam6+8yD0W5meiZ0UIZR8TF/9gDb4+4wTFnPwgfTrggEauA8tt8uJtiyBCr
YexgZTXIZGTUj/86KXQaJKCreRr/kqwJOWqkNW4CGUVzw7LiI+sArOZqUp/TsxnbcNC73XCMN1P
snByb2zCeK13V26Crl84U9sDuqQTJRaIse01MN9AAjpa2QWEwggNBBgkqhkiG9w0BBwGgggmyB
IIJrjCCCawggmmBgsqhkig9w0BDAoBAqCCW4wgglqMBwGCiqGSIB3DQEMAQMwDgQIEjm88b1
+pnkCaggABIIJSDD3P+vnllSolmQvmYgZVfV37T3KpurJvMxQScPvalWiF7Q1Iwasf/+N0hKKN
r2j/aGZLunLkaG6mLPeBP212LCwnUxDu5kyffVVE90WX/bXewBYQribwFNkNhUrSgen8BfhnRl
vDrzbBLoHivDrUFszSVBCYh31Vwgu8p9SjC8K/XlumcLdjSFko85XpoK23euhowjWH+X0kRoYG
zorcdNE8z03BKvFR61W2XWzTSaWQ6eZHG6sUrnX5Fe/w50U9tMIi3BCCCqgapUHVdmHqKkmWLi
kX8LssUcN30JvekM2aJ9v4YO6CoegKAMVDs0tVSov3KbGC3GNX6lgHu4y1LOZPlPlfPXb0wDHq
avlXK3zpHl8sIRzuX3HXSdEdenHYAkSV/IQZ89h+CZUkf0nu/og8eoA8ATDA5g7fj3HXpQ6cYd
rUBaHc7ruxHOiWR0GcT4XK4TTz7zZTO1wWpViprUo6ayw0dYZSG22MeDA027Yirm044Ifosn9C
sqnNLZoOWvA2ao4ippDoBRqv5Hv6n0I3fOAYS5nPq3jJtKQ5neqUYo0MrAkoKHo0h6zn0Bfvis
yB88aM9N0mPD76ykbAERq7151biKbA2tk8bb9dy/sJmk2ojM/D/W1YtrNL4iM6azL2kVN5eiCh
xCof33/RuRpXfGR8YNeJTl7bq42wL70QKDBRoG1TPcLqdVqz74oshlRspfqvZsbsUatbASbt2T
0YG4zfGfGh7sb2ezyougVvzdp77wAJ6n39dc/ZLdYDzFkQb07984y8LlhIM1AcwFcMh43gWp6
A8CJ02174ednirSqSVOPZ7K9dRw6Y0X8MB4/WGzEcVFeHYIGLBcXilSbY5wjWnbeuhlWLiSkMD
QRB6oG0vF7bJsilKx5PwgWbbqw8KUSuU01skbMAa5T8Hkm4OiSTf2a78E0zIKLGZg7yu9FDIIt
WYWoK96MXEBAdOuH+wWYmaEexh51ONrfFwKDuDMZh7MO20TTEQU8oQdjRRoAofXvTcj22GSMT
Y6XleskZX2ZKxSQdD1tCtkjGRKHSTYza3zLHbBiJTIJw4z6sw9FyTTApG66UAkNtiMalr9nqTT
NaxRWEXMEQVRLzAL2F9aqjgW65xrbYXu/J9Y/SYTcYbX2SRA/JkQ+Y8F68KOoS1pvK1p5/FcED
vprTNSD4lf+aj3HNWuK5wOsrpBhMlb2IfLuK/9QwPh9IC/RhHRfimyTPRXAf73cehNdp8DpKwL
m+jr30vazFwICpvSbi6Etb6GXfPkKaX7ztpQBqG92m2/0g3LWfPtilzwrPHPBz8y1qQMU268Do

```

o8YvWtI4KGaDAFb6XQhR6t6mqoq/3IP6/g//PZVENSyUVsPLDJlLF9fiOwTbMZnaiscKv8SGEs
//B9JkKrdsRrQRZcnnPjJnJLlLb1RVAZGuXpSKSYVPzYmOjUx3sSeLSiPoSOcqRIJ0X3s4ED09
2W3tR4ZXK3fnkFyrIVtRJsB3k/2smiQ6PclVuKhh1yTzYjXKRQcDaY3EDP9IWftjiUfZQoZcij
MWt6YXim23m2aN2Ed8qIedikR6OjFHE4Kus/2yegTszSs5CrM7NamKWzeIeNNth/cTcmT++GDu
msGNTBAsHHSq1KYpqLi4GKLHzU7WNCQRdAcIDEvMZH/CHlmZK7bzb9z038rPf/D5WZrcK1tttd5
BjTJjj7GerS0xLkvYIk1AJqurjMdWYmQtT4JAHF90/zRKqFFVpSiW074bRQ+PfaLI5C+TwoX51
YD+R91A0qyGKIkJITa8hZFY+Up+rSuREqnpAvdAVL9/gLPF6I+5+D+sVBsGRbw2rFVRbCHdwaT
QcAVPeJJy0f/+sOs/PXoejr3siORpf8iLLY0aziGYf1EtunFcCLj8PEOznaUyouJ+lm9YKPBSL
ULC/sVVy6XUArYfJfq0Ag31YXpJeWPBORxVP/VCm8d/sNjWTQXGN/IjNZaZuliXNgq5nRkPBKw
F23ZUYG4pLGpGROLup9nLSgEbpiDmN1Gq/IHSfI/8HpG/yRAoCdqUdre3yL/f9caj8RBBHRYbb
fRxtYQ9u2vsrqoloZ7F+Mu+kjuc9BxCmvJ7JaKwvQJckAkzTo6t10t6MzwiqJ7Au+2oOJ2Ukb/
985+TFGS219fmqWfwisOfpuvSkjRj8vIDBBm9itKIS+pVpfz+Mg7kl3WmkUrgF3yjTH5/C51ua
SzK2KeEVoWPx/Ps2CX7ATo6AsETp8Na38dT6d+Dm4WM4sBieKt/yOEFhiBNkgpVKAqawKRvLW3
U73OIKC8VLFhhnU+ogGxcUq5mZXvMbNDIaU2LvtmtPPo/qL0bOYu76TKclZX0R6AXkeImQgRPs
deXPPANTW3la585oZbYxUXRfEIEKmkcv3eSGnPCVesbxxd1SaIJe2j7H9MbHdjYkeFQuECnUhK
xg63BVP1/qAEIO5+OKBz7ctuP8apeGw1iHAueKzJXc5IeFS/3iwkfdLRkrgzBeNIL0IINo3Co
GSvn95Z8+LhNSopyqt3uB4rQksUYIwXgkfrEVYujCO0T5dSkk5j10X7WlDm4DHZVLJH+GtL6v9
A6xFJNDQfQF0hS+w1XkTkMq7pUiX+Qohf8QRJZEyU5VWo2CesR63j1MFpkB3xybpbjt8oI47XC
20GEN3uCjwMwq/3K4ibHnqi16pPPRGi/u3R9TVfvOC2e0xgllrFG6cKUfoguXoxHqP1KKjUw2
3bpd9L09LzSDdSHcoDPokWzDee0ZP/Z6VH3rdjQR71kw4VBet8nKfLP2dGBd0tpWDQhCFK7I9a
xxxthnv0v09x/J7jhYoLRt5e8lMEfrqtnMWdqjFgYVEQndthZ+9/XvfNk6f5MD8fDheMuvbNTh
duFSZEcZCLlW4GWKneVji4wdBrV3aCrzAzxy0H7y7nnkyCEvac503UDtr1bk1VJIVsYfYrN2S2
DPbp3H2E8r/n6jfbilwFyp3JTJvnRqQTcYHXDieW8Njq46JO6O6wsPwKQTKMfHGxxTRJdRe5yv
JD54xvFWw1YEJ/Q2c8cr1NNXEN32e5psfIJ7o48k6bsiyXnbHKSjK781Z5h8Hc3FbUF2U2p5Jq
LwcD7+bknEunsbWSC37iMk7oweF3hMhKRMm9iYJ8tpxMRcWCot7ador+Y2fYWBsu/bwXwcRI08
TElMCMGCSqGSib3DQEJFTEWBBRymjnEbJmrRwh4sRnwudfSQP6KDAxMCEwCQYFKw4DAhoFAAQ
U+YFhgKEYjfxN/cL70yRrJSHFgUwECHeCTQnUEU0BAGIIAA==",
"client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaaa",
"client_secret": "abcdef",
"ekmip_reachability": {
  "code": 346758,
  "message": "embedded KMIP server status unavailable on node.",
  "node": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  }
},
"key_id": "https://keyvault1.vault.azure.net/keys/key1",
"name": "https://kmip-akv-keyvault.vault.azure.net/",
"proxy_host": "proxy.eng.com",
"proxy_password": "proxypassword",

```

```

"proxy_port": 1234,
"proxy_type": "http",
"proxy_username": "proxyuser",
"scope": "svm",
"state": {
  "code": 346758,
  "message": "Top-level internal key protection key (KEK) is unavailable
on the following nodes with the associated reasons: Node: node1. Reason:
No volumes created yet for the SVM. Wrapped KEK status will be available
after creating encrypted volumes."
},
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svml",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"tenant_id": "zzzzzzzz-yyy-zzzz-yyy-zzzzzzzzzzz",
"uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records

```



```
|array[link:#azure_key_vault[azure_key_vault]]
```

```
a|
```

```
|===
```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "authentication_method": "client_secret",
    "azure_reachability": {
      "code": 346758,
      "message": "AKV service is not reachable from all nodes - reason."
    },
    "client_certificate":
```

```
"MIIQKQIBAzCCD+8GCSqGSIB3DQEHAaCCD+AEgg/cMIIP2DCCBg8GCSqGSIB3DQEHbqCCBgAwg
gX8AgEAMIIF9QYJKoZIhvcNAQcBMBwGCiqGSIB3DQEMAQYwDgQIWkY7ojViJDYCAggAgIIFyJP
jIfmM6yTCKVw5ep2oZLwvwRca8pKhISVjw+WjWngh/f6Py/Ty0CwCjDFUZPsUUdSmk78E7SAz0
CpQyBwmUuFJQShjZjftHLKRWld3O4sJKB8DzH9Yw1C7En94cyJ1rT4WYoVFmeJcmOXx6h+NFHc
7njtXVsKwxc5BF88K3+3kHdV3WyVdXoeXe7yY/+EjFfjtBryp8ljuielX/NFlh5kwhoj+yxnO
0c1/0OIliV3mTIOTXD8qrZVp9ZhAxSTRBd5uDyWMfppqxW2L+9vCUU+ZgmRxtU3VsRLOp/T140
OP7Sn1Ch2OE0bIrbYYtcpi04QcUtfEJBMLbbTbJPHDAti02KIQKviZL4QMZgho9NNgL4MUpIbN
SzDCbuIC+nNMxfghs0nPZewY+b43H/tMmnZ8Q4kiCFwrUqbFbflBiPMOaJsS0eQaJhDmzM90QE
gbesHWgPreAcfMUcNl+BaqHFLHUxLXDxQix6zYiCatDX6/EKlirRh1TFpmFX2PBd+X6uODhmwm
4ub9RKj3In8t5qgtN4q/mTBXjAVDAbTIIegobBRaXGSSXCBC9W/jRed0DRZD9Bm8T/nV39sZNd
ucwZa5ojYTX8fFMA0cfY6IFivXHjB00coHEEGdgCfC0G8vACqLbb+2NuhMJPtR7Ig50iAPUMc6
70Z5ItOTQhyYOZ/KagOtvV8sKPCzeAkcMoHlsm189V79zt1fCJQTVWnaGiMj5Orcbskk6vCxhD
GeU6q1kgvXJKXOYRF8/wIpv8Y7/rEpnGwE/I0ZOXzdIDHXqA53B1zyOVem25ezWCD+kpoH89XJ
ssYlNjIMJhjVRED61w/DbSXg2yFu/v3ckGapVvTuyAiz5hWUNfl3pt++da6GoekKnLqtL4G/RG
XCnebLbXg838dlTGBznoCwGTVxXDeVYafz8AjI10qYtTMcbN56ya9kK7IHSkrnFX24xQRQOfmD
```

0Vob71pjdz8r1aXKvD/1X2TkYJHoeEHq0nWpU8vwDG/xhv4YgKJGN9qsEZgiTXETUh5gak8e1t
GNkP+fum+1OqlO5oS+SvNa5/eB8eFeJl2Oi48Xi5UapaTRHPFp6kZfPXOu9cEjhILowRIi6g1g
7FUbmoJcu5OvDIyP9JlyQklw2VtgNlm1QOIvzRenXmy18XnP50NTxx2cIwby8tIcdSn2C2qhj8
Gk7q8oxVZGiBgtz4BwzyKkypwm60BBRrHpAKLw6JM5RISeZnYQfIsId0tGgb61go0RJf0sFtb
uvZcSvLI+2Onj8KH1TlmMR4dbuCWE9Ym4sVRmD1D6/f6BoNH0DRg7TJkEFbOadJsNPGzHbKteL
daSMGTNUZ3hEDQeomakQMfvCgypbOLxrTTqfbenHRtN+iFNyW0zCUW6EJoAXp+lqFnwQL52I12
QxwZikE01P2k0GharzAJkXnNaFGnmHIIP6wJrCCSDZwDmr7GI2R5evDlRi17QUg2sulxQV0U8z
ezzwIUgEe/Whf0ngGJv/QcsL2jyri/tSQbUWs4g+yep4SlE3iddhfqSJzI2iKdAE+HLiHGVO1z
70fGEsO6dPLnmh4eoWidgZi9N/SoBylaT0JpIQ6z6N5ImpfDWu9Y6TWXUg1iyOIXGsxiQVIgUN
oB5Ru/APDxpYpFLk0fH9k9OnEWK5Im33puOQKLno1uwrOmdBG8+x1EY8wc9FvkHGH0Zh4HydiC
VUCYSdiGWUxVmgm4OgyiYzcpB+Ar2dzikGc4pBg8fala1HN5Q3TK3w4h/HeOUlma4vWOYuV01H
93ILGP6PWfkug+1Tam6+8yD0W5meiZ0UIZR8TF/9gDb4+4wTFnPwgftTrggEauA8tt8uJtiyBCr
YexgZTXIZGTUj/86KXQaJKCreRr/kqwJOWqkNW4CGUVzw7LiI+sArOZqUp/TsxnbcNC73XCMN1P
snByb2zCeK13V26Cr184U9sDuqQTJRaIse01MN9AAjpa2QWEwggnBBgkqhkiG9w0BBwGgggmyB
IIJrjCCCawggmmBgsqhkig9w0BDaOBAqCCW4wgg1qMBwGCiGSIb3DQEMAQMwDgQIEjm88b1
+pnkCAggABIIJSD3P+vn11SolmQvmYgZVFV37T3KpurJvMxQScPvalWiF7Q1Iwasf/+N0hKKN
r2j/aGZLunLkaG6mLPeBP212LCwnUxDu5kYffVVE90WX/bXewbYQribwFNkNhUrSgen8BfhnRl
vDrzbBLoHIvDrUFszSVBCYh31Vwgu8p9SjC8K/XlumlDjSFko85XpoK23euhowjWH+X0kRoYG
zorcdNE8z03BKvFR61W2XWzTSaWQ6eZHGS6UrnX5Fe/w50U9tMIi3BCCCqgapUHVdmHqKkmWLi
kX8LssUcN30JvekM2aJ9v4YO6CoegKAMVDs0tVSOv3KbGC3GNX6lgHu4y1LOZPLPLfPXb0wDHq
avlxK3zph18sIRzuX3HXSdEdenHYAkSV/IQZ89h+CZUkf0nu/og8eoA8ATDA5g7fj3HXpQ6cYd
rUBaHc7ruxHOiWR0GcT4XK4TTz7zZTO1wWPViprUo6ayw0dYZSG22MeDA027Yirm044Ifosn9C
sqnNLZoOWvA2ao4ippDoBRqv5Hv6n0I3fOAys5nPq3jJtKQ5neqUYo0MrAkoKHO0h6zn0Bfvis
yB88aM9N0mPD76ykbAERq7151biKbA2tk8bb9dy/sJmk2ojM/D/W1YtrNL4iM6azL2kVN5eiCh
xCoF33/RuRpXfGR8YNeJTl7bq42wL70QKDBRoG1TPcLqdVqz74oshlRspfqvZsbsUatBASbt2T
0YG4zfGfGh7sb2ezyougVvzdp77wAJ6n39dc/ZLDDyDzFkQb07984y8LlhIM1AcwFcMh43gWp6
A8CJ02174ednirSqSVOPZ7K9dRw6Y0X8MB4/WGzEcVFeHYIGLBcXilSbY5wjWnbeuhlWLiSkMD
QRB6oGOvF7bJsilkx5PwgWbbqw8KUSuU01skbMAa5T8Hkm4OiSTf2a78E0zIKLGZg7yu9FDIIt
WYWokG96MXEBAdOuH+wWYmaEexh51ONrffWkDuDMZh7MO20TTEQU8oQdjRRoAofXvTcj22GSMT
Y6XleskZX2ZKxSQdD1tCtkjGRKHSTYza3zLHbBiJTIJw4z6sw9FyTTApG66UAkNtiMalr9nqTT
NaxRWEXMEQVRLzAL2F9aqjgW65xrbYXu/J9Y/SYTCyBx2SRA/JkQ+Y8F68KOoS1pvK1p5/FcED
vprTNDs4lf+aj3HNWuK5wOsrpBhMlb2IfLuK/9QwPh9IC/RhHRfimyTPRXAf73cehNdp8DpKwL
m+jr30vazFwICpvSbi6Etb6GXfPkKaX7ztpQBqG92m2/0g3LWfPtilzwrPHPBz8y1qQMU268Do
o8YvWtI4KGaDAFb6XQhR6t6mqoq/3IP6/g//PZVENsYUVsPLDJlLF9fiOwTbMznaiscKv8SGEs
//B9JkKrdsRrQRZcnnPjJnJLILblRVAZGuXpSKSYVPzYmOjUx3sSeLSiPoSocqRIJ0X3s4ED09
2W3tR4ZXK3fnkFyrIVtRJsB3k/2smiQ6PclVuKHhlyTzYjXKRQcDaY3EDP9IWFtjiUfZQoZcij
MWt6YXim23m2aN2Ed8qIedikR6OjFHE4Kus/2yegTszSs5CrM7NamKWzeIeNNth/cTcmT++GDu
msGNTBAShHSq1KYpQLi4GKLHzU7WNCQRdAcIDEvMZH/CH1mZK7bzb9z038rPf/D5WZrcK1ttd5
BjTJjj7GerS0xLkvYiklAJqurjMdWYmQtT4JAHF90/zRKqFFVpSiW074bRQ+PfaLI5C+TwoX51
YD+R91A0qyGKIkJITa8hZFY+Up+rSuREqnpAvdAVL9/gLPF6I+5+D+sVBsGRbw2rFVRbCHdwaT
QcAVPeJJy0f/+sOs/PXoejr3siORpf8iLLYOaziGYf1EtunFcCLj8PEOznaUyouJ+lm9YKPBSL
ULC/sVVy6XUARyFJfQ0Ag31YXpJeWPBORxVP/VCm8d/sNjWTQXGN/IjNZaZulixNgq5nRkPBKw
F23ZUYG4pLGpGROLup9nLSgEbpIDmN1Gq/IHSfI/8HpG/yRAoCdqUdre3yL/f9caj8RBBHRYbb
fRxtYQ9u2vsrqoloZ7F+Mu+kjuc9BxCMvJ7JaKwvJQckAkzTo6t10t6MzwiqJ7Au+2oOJ2Ukb/
985+TFGS219fmqWfwisOfpuvSkjRj8vIDBBm9itKIS+pVpfz+Mg7kl3WmkUrgF3yJTH5/C51ua
SzK2KeEVoWPx/Ps2CX7ATo6AsETp8Na38dT6d+Dm4WM4sBieKt/yOEFhiBNkgpVKAqawKRvLW3

```

U73OIKC8VLFhhnU+ogGxcUq5mZXvMbNDIaU2LvtmtPPo/qL0bOYu76TKc1ZX0R6AXkeImQgRPs
deXPPANtW3la585oZbYxUXRfEIEKmkcv3eSGnPCVesbxxd1SaIJe2j7H9MbHdjYkeFQuECnUhK
xg63BVP1/qAEIO5+OKBzM7ctuP8apeGW1iHAueKzJXc5IeFS/3iwkfDLRkrgezBeNIL0IINo3Co
GSvn95Z8+LhNSopyqt3uB4rQksUYIwXgkfrEVYujCO0T5dSkk5j10X7WlDm4DHZVLJH+GtL6v9
A6xFJNDQfQF0hS+w1XkTkMq7pUiX+Qohf8QRJZEyU5VWo2CesR63j1MFpkB3xybpbjt8oI47XC
20GEn3uCjwMwq/3K4ibHnqi16pPPRGi/u3R9TVfvOC2e0xgllrFG6cKUfoguXoxHqPlKKjUw2
3bpd9L09LzSDdSHcoDPokWzDee0ZP/Z6VH3rdjQR71kw4VBeT8nKfLP2dGBd0tpWDQhCFK7I9a
xxxthnv0v09x/J7jhyoLRt5e8lMEfrqtnMWdqjFgYVEQndthZ+9/XvfNk6f5MD8fDheMuvbNTh
duFSZEczCLlW4GWKneVji4wdBrV3aCrzAzxy0H7y7nnkyCEvac503UDtr1bk1VJIVsYfYrN2S2
DPbp3H2E8r/n6jfbilwFyp3JTJvnRqQTcYHXDieW8Njq46JO6O6wsPwKQTKMfHGxxTRJdRe5yv
JD54xvFWwlYEJ/Q2c8cr1NNXEN32e5psfIJ7o48k6bsiyXnbHKSjK781Z5h8Hc3FbUF2U2p5Jq
LwcD7+bknEunsbWSC37iMk7oweF3hMhKRMm9iYJ8tpxMRcWCot7ador+Y2fYWBSu/bwXwcRI08
TElMCMGCSqGSib3DQJEJFTEWBBRymjnEbJmrRwh4sRnwudfsQP6KDAxMCEwCQYFKw4DAhoFAAQ
U+YFhgKEYjfxN/cL70yRrJSHFgUwECHeCTQnUEU0BAgIIAA==",
  "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
  "client_secret": "abcdef",
  "ekmip_reachability": {
    "code": 346758,
    "message": "embedded KMIP server status unavailable on node.",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  },
  "key_id": "https://keyvault1.vault.azure.net/keys/key1",
  "name": "https://kmip-akv-keyvault.vault.azure.net/",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "svm",
  "state": {
    "code": 346758,
    "message": "Top-level internal key protection key (KEK) is
unavailable on the following nodes with the associated reasons: Node:
node1. Reason: No volumes created yet for the SVM. Wrapped KEK status will
be available after creating encrypted volumes."
  },
  "svm": {
    "_links": {

```

```

        "self": {
            "href": "/api/resourcelink"
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzz",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
}
====

```

== Error

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description

| 3735553
| Failed to create self-signed certificate.

| 3735664
| The specified key size is not supported in FIPS mode.

| 3735665
| The specified hash function is not supported in FIPS mode.

| 3735700
| The specified key size is not supported.

| 52559972
| The certificates start date is later than the current date.

| 65537500
| A key manager has already been configured for this SVM.

| 65537504
| Internal error. Failed to store configuration in internal database.

| 65537505
| One or more volume encryption keys of the given SVM are stored on a key
manager configured for the admin SVM.

```

```

| 65537506
| AKV is not supported in MetroCluster configurations.

| 65537512
| AKV cannot be configured for the given SVM as not all nodes in the
cluster can enable the Azure Key Vault feature.

| 65537514
| Failed to check if the Azure Key Vault feature is enabled.

| 65537518
| Failed to find an interface with Cluster role.

| 65537523
| Invalid key ID format. Example key ID format":"
"https://mykeyvault.vault.azure.net/keys/key1".

| 65537526
| Failed to enable Azure Key Vault feature.

| 65537567
| No authentication method provided.

| 65537573
| Invalid client certificate.
|===

```

```

[cols=3*,options=header]

```

```

|===

```

```

|Name

```

```

|Type

```

```

|Description

```

```

|error

```

```

|link:#error[error]

```

```

a|

```

```

|===

```

```

.Example error

```

```

[%collapsible%closed]

```

```

====

```

```

[source,json,subs=+macros]

```

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

====

== Definitions

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
```

====

```
[#href]
[.api-collapsible-fifth-title]
href
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|href
|string
a|
```

|===

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#azure_reachability]
[.api-collapsible-fifth-title]
azure_reachability
```

Indicates whether or not the AKV service is reachable from all the nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|integer
```

a|Code corresponding to the status message. Returns a 0 if AKV service is reachable from all nodes in the cluster.

```
|message
|string
```

a|Error message set when reachability is false.

```
|reachable
|boolean
```

a|Set to true when the AKV service is reachable from all nodes of the cluster.

```
|===
```

```
[#node]
[.api-collapsible-fifth-title]
```

node

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|
```

```
|uuid
```

```
|string
```

```
a|
```

```
|===
```

```
[#ekmip_reachability]
```

```
[.api-collapsible-fifth-title]
```

```
ekmip_reachability
```

Provides the connectivity status for the given SVM on the given node to all EKMIP servers configured on all nodes of the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|integer
```

a|Code corresponding to the error message. Returns a 0 if a given SVM is able to communicate to the EKMIP servers of all of the nodes in the cluster.


```

|message
|string
a|Error message set when cluster-wide EKMIP server availability from the
given SVM and node is false.

|node
|link:#node[node]
a|

|reachable
|boolean
a|Set to true if the given SVM on the given node is able to communicate to
all EKMIP servers configured on all nodes in the cluster.

|===

[#state]
[.api-collapsible-fifth-title]
state

Indicates whether or not the AKV wrapped internal key is available cluster
wide.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|available
|boolean
a|Set to true when an AKV wrapped internal key is present on all nodes of
the cluster.

|code
|integer
a|Code corresponding to the status message. Returns a 0 if AKV wrapped key

```

is available on all nodes in the cluster.

```
|message
|string
a|Error message set when top-level internal key protection key (KEK)
availability on cluster is false.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#azure_key_vault]
[.api-collapsible-fifth-title]
azure_key_vault
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
```

```

|Description

|_links
|link:#_links[_links]
a|

|authentication_method
|string
a|Authentication method for the AKV instance.

|azure_reachability
|link:#azure_reachability[azure_reachability]
a|Indicates whether or not the AKV service is reachable from all the nodes
in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|client_certificate
|string
a|PKCS12 Certificate used by the application to prove its identity to AKV.

|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.

|client_secret
|string
a|Secret used by the application to prove its identity to AKV.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|key_id
|string
a|Key Identifier of AKV key encryption key.

|name

```

```

|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.

* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri
* Introduced in: 9.8
* readCreate: 1


|proxy_host
|string
a|Proxy host.


|proxy_password
|string
a|Proxy password. Password is not audited.


|proxy_port
|integer
a|Proxy port.


|proxy_type
|string
a|Type of proxy.


|proxy_username
|string
a|Proxy username.


|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".


|state
|link:#state[state]
a|Indicates whether or not the AKV wrapped internal key is available
cluster wide.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query

```

parameter or GET for all advanced properties is enabled.

```
|svm
|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block
```

```
=====
```

```
[[ID92599f413b8ef7fc543bebb228561e03]]
```

```
= Re-key the external key in the key hierarchy
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/azure-key-vaults/{azure_key_vault.uuid}/rekey-external`#
```

```
*Introduced In:* 9.11
```

Rekeys the external key in the key hierarchy for an SVM with an AKV configuration.

```
== Required properties
```

```
* `key_id`- Key identifier of the new AKV key encryption key.
```

```
== Related ONTAP commands
```

```
* `security key-manager external azure rekey-external`
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|azure_key_vault.uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|UUID of the existing AKV configuration.
```

|return_timeout

|integer

|query

|False

a|The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

* Default value: 1

* Max value: 120

* Min value: 0

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|key_id

|string

a|Key identifier of the AKV key encryption key.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".


```
|svm
|link:#svm[svm]
a|

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "key_id": "https://keyvault1.vault.azure.net/keys/key1",
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
=====

== Response
```

Status: 202, Accepted

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description

| 65537120
| Azure Key Vault is not configured for the given SVM.

| 65537547
| One or more volume encryption keys for encrypted volumes of this data
```

SVM are stored in the key manager configured for the admin SVM. Use the REST API POST method to migrate this data SVM's keys from the admin SVM's key manager to this data SVM's key manager before running the rekey operation.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

====

[source,json,subs=+macros]

{

 "error": {

 "arguments": {

 "code": "string",

 "message": "string"

 },

 "code": "4",

 "message": "entry doesn't exist",

 "target": "uuid"

 }

}

====

== Definitions

[.api-def-first-level]

.See Definitions

[%collapsible%closed]

//Start collapsible Definitions block

====

[#href]

[.api-collapsible-fifth-title]

```

href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name

```

```

|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#azure_key_vault_key]
[.api-collapsible-fifth-title]
azure_key_vault_key

[cols=3*,options=header]
|===
|Name
|Type
|Description

|key_id
|string
a|Key identifier of the AKV key encryption key.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|svm
|link:#svm[svm]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

```

```
//end collapsible .Definitions block
====

[[ID915105d74a79641eccb1f40e25bc5454]]
= Delete an AKV configuration

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/azure-key-vaults/{uuid}`#

*Introduced In:* 9.8

Deletes an AKV configuration.

== Related ONTAP commands

* `security key-manager external azure disable`

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|AKV UUID

|===

== Response
```

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 65536242

| One or more self-encrypting drives are assigned an authentication key.

| 65536243

| Cannot determine authentication key presence on one or more self-encrypting drives.

| 65536817

| Internal error. Failed to determine if key manager is safe to disable.

| 65536827

| Internal error. Failed to determine if the given SVM has any encrypted volumes.

| 65536834

| Internal error. Failed to get existing key-server details for the given SVM.

| 65536867

| Volume encryption keys (VEK) for one or more encrypted volumes are stored on the key manager configured for the given SVM.

| 65536883

| Internal error. Volume encryption key is missing for a volume.

| 65536884

| Internal error. Volume encryption key is invalid for a volume.

| 65536924

| Cannot remove key manager that still contains one or more NSE authentication keys.

| 65537120

| Azure Key Vault is not configured for the given SVM.

| 196608080

```
| One or more nodes in the cluster have the root volume encrypted using  
NVE (NetApp Volume Encryption).
```

```
| 196608301
```

```
| Internal error. Failed to get encryption type.
```

```
| 196608305
```

```
| NAE aggregates found in the cluster.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```
    "arguments": {
```

```
      "code": "string",
```

```
      "message": "string"
```

```
    },
```

```
    "code": "4",
```

```
    "message": "entry doesn't exist",
```

```
    "target": "uuid"
```

```
  }
```

```
}
```

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```



```

//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string

```

a|Error message

|target

|string

a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

====

[[IDb30fb57ccc1d678494ac2ae45f57677c]]

= Retrieve the AKV configuration for an SVM specified by the UUID

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/azure-key-vaults/{uuid}`#

Introduced In: 9.8

Retrieves the AKV configuration for the SVM specified by the UUID.

== Related ONTAP commands

* `security key-manager external azure show`

* `security key-manager external azure check`

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

|True

```
a|AKV UUID
```

```
|fields  
|array[string]  
|query  
|False  
a|Specify the fields to return.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|_links  
|link:#_links[_links]  
a|
```

```
|authentication_method  
|string  
a|Authentication method for the AKV instance.
```

```
|azure_reachability  
|link:#azure_reachability[azure_reachability]  
a|Indicates whether or not the AKV service is reachable from all the nodes  
in the cluster.
```

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|client_certificate  
|string  
a|PKCS12 Certificate used by the application to prove its identity to AKV.
```

```
|client_id
```

```

|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.

|client_secret
|string
a|Secret used by the application to prove its identity to AKV.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|key_id
|string
a|Key Identifier of AKV key encryption key.

|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.

* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri
* Introduced in: 9.8
* readCreate: 1

|proxy_host
|string
a|Proxy host.

|proxy_password
|string
a|Proxy password. Password is not audited.

|proxy_port
|integer
a|Proxy port.

|proxy_type
|string
a|Type of proxy.

```

```
|proxy_username
|string
a|Proxy username.
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|state
|link:#state[state]
a|Indicates whether or not the AKV wrapped internal key is available
cluster wide.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.
```

```
|svm
|link:#svm[svm]
a|
```

```
|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.
```

```
|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).
```

```
|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
```

```

    "self": {
      "href": "/api/resourcelink"
    },
    "authentication_method": "client_secret",
    "azure_reachability": {
      "code": 346758,
      "message": "AKV service is not reachable from all nodes - reason."
    },
    "client_certificate":
    "MIIQKQIBAzCCD+8GCSqGSIB3DQEHAAcCD+AEgg/cMIIIP2DCCBg8GCSqGSIB3DQEHbqCCBgAwg
gX8AgEAMIIIF9QYJKoZIhvcNAQcBMBWGCiqGSIB3DQEMAQYwDgQIWkY7ojViJDYCAggAgIIIFyJP
jIfmM6yTCKVw5ep2oZLwvwRca8pKhISVjw+WjWngh/f6Py/Ty0CwCjDFUZPsUUdSmk78E7SAz0
CpQyBwmUuFJQShjZjftHLKRWld3O4sJKB8DzH9Yw1C7En94cyJ1rT4WYoVFmeJcmOXx6h+NFHc
7njtXVsKwxc5BF88K3+3kHdV3WyVdXoeXe7yY/+EjFfjtBryp8ljuielX/Nflh5kowhoj+yxnO
0c1/0OI1iV3mTIOtXD8qrZVp9ZhAxSTRBd5uDyWMfppqxW2L+9vCUU+ZgmRxtU3VsRLOp/T140
OP7Sn1Ch2OE0bIrbYYtcpi04QcUtfEJBMLbbTbJPHDAtio2KIQKviZL4QMZgho9NNgL4MUpIbN
SzDCbuIC+nNMxfghfs0nPZewY+b43H/tMmnZ8Q4kiCFwrUqbFbflBiPMOaJsS0eQaJhDmzM90QE
gbesHWgPreAcfMUcN1+BaQHFLHUxLXDxQix6zYiCatDX6/EKlirRh1TFpmFX2PBd+X6uODhmwm
4ub9RKj3In8t5qgtN4q/mTBXjAVDAbTIIIEgobBRaXGSSXCBc9W/jRed0DRZD9Bm8T/nV39sZNd
ucwZa5ojYTX8fFMA0cfY6IFivXHjB00coHEEGdgCfC0G8vACqLbb+2NuhMJPr7Ig50iAPUMc6
70Z5ItOTQhyYOZ/KagOtvV8sKPCzeAkcMoHlsm189V79zt1fCJQTVWnaGiMj50rcbskk6vCxD
GeU6q1kgvXJKXOYRF8/wIpv8Y7/rEpnGwE/I0ZOXzdIDHXqA53B1zyOVem25ezWCD+kpoH89XJ
ssYlNjIMJhjVRED61w/DbSXg2yFu/v3ckGapVvTuyAiz5hWUNfl3pt++da6GoekKnLqtL4G/RG
XCnebLbXg838dlTGBznoCwGTVxXDeVYafz8AjI10qYtTMcbN56ya9kK7IHSkrnFX24xQRQOfmD
0Vob71pjdZ8r1aXKvD/1X2TkYJHoeEHq0nWpU8vwDG/xhv4YgKJGN9qsEZgiTXETUh5gak8elt
GNkP+fum+10q105oS+Swna5/eB8eFeJl2Oi48Xi5UapaTRHPFp6kZfPXOu9cEjhILowRIi6glg
7FUbmoJcu5OvDIyP9JlyQklw2VtgNlm1QOIvzRenXmy18XnP50NTxx2cIwby8tIcdSn2C2qhj8
Gk7q8oxVZGiBgtz4BwyzyKkypwm60BBRrHpAKLw6JM5RISeZnYQfIsId0tGgb6lgo0RJf0sFtb
uvZcSvLI+2Onj8KH1TlmMR4dbuCWE9Ym4sVRmD1D6/f6BoNH0DRg7TJkEFbOadJsNPGzHbKteL
daSMGTNUZ3hEDQeomakQMfvcGypbOLxrTTqfbenHRtN+iFNyW0zCUW6EJoAXp+lqFnwQL52I12
QxwZike01P2k0GharzAJkXnNaFGnmHIIP6wJrCCSDZwDmr7GI2R5evDlRi17QUg2sulxQV0U8z
ezzwIUgEe/Whf0ngGJv/QcsL2jyri/tSQbUWs4g+yep4SlE3iddhfqSJzI2iKdAE+HLiHGVO1z
70fGEsO6dPLnmh4eoWidgZi9N/SoBy1aT0JpIQ6z6N5ImpfDWu9Y6TWXUg1iyOIXGsxiQVIgUN
oB5Ru/ApDxpYpFLk0fh9k9OnEWK5Im33puOQKLno1uwrOmdBg8+x1EY8wc9FvkHGH0Zh4HydiC
VUCYSdiGWUxVmgm4OgyiYzcpB+Ar2dzikGc4pBg8fa1a1HN5Q3TK3w4h/HeOUlma4vWOYuVO1H
93ILGP6PWfkug+1Tam6+8yD0W5meiZ0UIZR8TF/9gDb4+4wTFnPwgfTrggEauA8tt8uJtiyBCr
YexgZTXIZGTUj/86KXQaJKCreRr/kqwJOWqkNW4CGUVzw7LiI+sArOZqUp/TsxnbnC73XCMN1P
snByb2zCeK13V26Crl84U9sDuqQTJRaIse01MN9AAjpa2QWEwggnBBgkqhkiG9w0BBWgggmyB
IIJrjCCCaowggmmBgsqhkiG9w0BDAoBAqCCW4wgg1qMBWGCiqGSIB3DQEMAQMwDgQIEjm88b1
+pnkCAggABIIJSSDD3P+vn1lSolmQvmYgZVfV37T3KpurJvMxQScPvalWiF7Q1Iwasf/+N0hKKN
r2j/aGZLunLkaG6mLPeBP212LCwnUxDu5kyffVVE90WX/bXewbYQribwFNkNhUrSgen8BfhnRl
vDrzbBLoHivDrUFsZSVBCYh31Vwgu8p9SjC8K/XlumcLdjSFko85XpoK23euhowjWH+X0kRoYG
zorcdNE8z03BKvFR61W2XWzTSaWQ6eZHGS6UrnX5Fe/w50U9tMIi3BCCCqgapUHVdmHqKkmWLi
kX8LssUcN30JvekM2aJ9v4YO6CoegKAMVDs0tVSov3KbGC3GNX6lgHu4y1LOZPlPLfPXb0wDHq
avlXK3zph18sIRzuX3HXSdEdenHYAKSV/IQZ89h+CZUkf0nu/og8eoA8ATDA5g7fj3HXpQ6cYd

```

rUBaHc7ruxHOiWR0GcT4XK4TTz7zzTO1wWPFviprUo6ayw0dYZSG22MeDA027YirM044Ifosn9C
sqnNLZoOWvA2ao4ippDoBRqv5Hv6n0I3fOAys5nPq3jJtKQ5neqUYo0MrAkoKHO0h6zn0Bfvis
yB88aM9N0mPD76ykbAERq7151biKbA2tk8bb9dy/sJmk2ojM/D/W1YtrNL4iM6azL2kVN5eiCh
xCof33/RuRpXfGR8YNeJTl7bq42wL70QKDBRoG1TPcLqdvQz74oshlRspfqvZsbsUatbASBt2T
0YG4zfGfGh7sb2ezyougVvzdp77wAJ6n39dc/ZLDdYDzFkQb07984y8LlhIM1AcwFcMh43gWp6
A8CJ02l74ednirSqSVOPZ7K9dRw6Y0X8MB4/WGzEcvFeHYIGLBcXilSbY5wjWnbeuhlWLiSkMD
QRB6oGOvF7bJsilKx5PwgWbbqw8KUSuU0lSkbMAa5T8Hkm4OiSTf2a78E0zIKLGZg7yu9FDIIt
WYWOKG96MXEBADouH+wWYmaEexh5lONrfFwKDuDMZh7MO20TTEQU8oQdjRRoAofXvTcj22GSMT
Y6XleskZX2ZKxSQdDl1tCtkjGRKHSTYza3zLHbBiJTIJw4z6sw9FyTTApG66UAkNtiMalr9nqTT
NaxRWEXMEQVRLzAL2F9aqjgW65xrbYXu/J9Y/SYTcYbX2SRA/JkQ+Y8F68KOoS1pvK1p5/FcED
vprTNSD4lf+aj3HNWuK5wOsrpBhMlb2IfluK/9QwPh9IC/RhHRfimyTPRXAf73cehNdp8DpKwL
m+jr30vazFwICpvSbi6Etb6GXfPkKaX7ztpQBqG92m2/0g3LWfPtilzwrPHPBz8y1qQMU268Do
o8YvWtI4KGaDAFb6XQhR6t6mqoq/3IP6/g//PZVENsYUVsPLDJLLF9fiOwTbMZnaiscKv8SGEs
//B9JkKrdSrRQRZcnnPjJnJLILblRVAZGuXpSKSYVPzYmOjUx3sSeLSiPoSOcqRIJ0X3s4ED09
2W3tR4ZXX3fnkFyrIVtRJsB3k/2smiQ6PclVuKHhlyTzYjXKRQcDaY3EDP9IWFtjiUfZQoZcij
MWt6YXim23m2aN2Ed8qIedikR6OjFHE4Kus/2yegTszSs5CrM7NamKWzeIeNNth/cTcmT++GDu
msGNTBAShHSq1KYpqLi4GKLHzU7WNCQRdAcIDEvMZH/CHlmZK7bzb9z038rPf/D5WZrcK1ttd5
BjTJjj7GerS0xLkvYiklAJqurjMdWYmQtT4JAHF90/zRKqFFVpSiW074bRQ+PfaLI5C+TwoX51
YD+R91A0qyGKIkiFITa8hZFY+Up+rSuREqnpAvdAVL9/gLPF6I+5+D+sVBsGRbw2rFVRbCHdwaT
QcAVPeJJy0f/+sOs/PXoejr3siORpf8iLLYOaziGYf1EtunFcCLj8PEOznaUyouJ+lm9YKPBSL
ULC/sVVy6XUArYfJfq0Ag3lYXpJeWPbORxVP/Vcm8d/sNjWTQXGN/IjNZaZuliXNgq5nRkPBKw
F23ZUYG4pLGpGROLup9nLSgEbpDmN1Gq/IHSfI/8HpG/yRAoCdqUdre3yL/f9caj8RBBHRYbb
fRxytQ9u2vsrqoloZ7F+Mu+kjuc9BxCmvJ7JaKwvQJckAkzTo6t10t6MzwiqJ7Au+2oOJ2Ukb/
985+TFGS219fmqWfwisOfpuvSkjRj8vIDBBm9itKIS+pVpfz+Mg7kl3WmkUrgF3yjTH5/C51ua
SzK2KeEVoWPx/Ps2CX7ATo6AsETp8Na38dT6d+Dm4WM4sBieKt/yOEfhiBNkgpVKAqawKRvLW3
U73OIKC8VLFhnnU+ogGxcUq5mZXvMbNDIaU2LvtmtPPo/qL0bOYu76TKclZX0R6AXkeImQgRPs
deXPPANtW3la585oZbYxUXRfEIEKmkcv3eSGnPCVesbxxdlSaIJe2j7H9MbHdjYkeFQuECnUhK
xg63BVPl/qAEIO5+OKBz7ctuP8apeGwliHAueKzJXc5IeFS/3iwkfdLRkrzBeNIL0IINo3Co
GSvn95Z8+LhNSopyqt3uB4rQksUYIwXgkfrEVYujCO0T5dSkk5j10X7WlDm4DHZVLJH+GtL6v9
A6xFJNDQfQF0hS+wLXkTkMq7pUiX+Qohf8QRJZEyU5Vwo2CesR63j1MFpkB3xybpbjt8oI47XC
20GEn3uCjwMwq/3K4ibHnqil6pPPRGi/u3R9TVfvOC2e0xgllrFG6cKUfoguXoxHqP1KKjUw2
3bpd9L09LzSDdSHcoDPokWzDee0ZP/Z6VH3rdjQR71kw4VBeT8nKfLP2dGBd0tpWDQhCFK7I9a
xxxthnv0v09x/J7jhyoLRt5e8lMEfrqtnMWdqjFgYVEQndthZ+9/XvfNk6f5MD8fDheMuvbNTh
duFSZEczCLlW4GwKneVji4wdBrV3aCrzAzxy0H7y7nnkyCEvac503UDtr1bk1VJIVsYfYrN2S2
DPbp3H2E8r/n6jfBilwFyp3JTJvnRqQTcYHXDieW8Njq46JO6O6wsPwKQTKMfHGxxTRJdRe5yv
JD54xvFWw1YEJ/Q2c8cr1NNXEN32e5psfIJ7o48k6bsiyXnbHKSjK781Z5h8Hc3FbUF2U2p5Jq
LwcD7+bknEunsbWSC37iMk7oweF3hMhKRMm9iYJ8tpxMRcWCot7ador+Y2fYWBsu/bwXwcRI08
TElMCMGCSqGSib3DQEJFTEWBBRymjnEbJmrRwh4sRnwudfSQP6KDAxMCEwCQYFKw4DAhFAAQ
U+YFhgKEYjfXN/cL70yRrJSHFgUwECHeCTQnUEU0BAGIIAA==",
"client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
"client_secret": "abcdef",
"ekmip_reachability": {
 "code": 346758,
 "message": "embedded KMIP server status unavailable on node.",
 "node": {
 "_links": {

```

        "self": {
            "href": "/api/resourcelink"
        },
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
},
"key_id": "https://keyvault1.vault.azure.net/keys/key1",
"name": "https://kmip-akv-keyvault.vault.azure.net/",
"proxy_host": "proxy.eng.com",
"proxy_password": "proxypassword",
"proxy_port": 1234,
"proxy_type": "http",
"proxy_username": "proxyuser",
"scope": "svm",
"state": {
    "code": 346758,
    "message": "Top-level internal key protection key (KEK) is unavailable
on the following nodes with the associated reasons: Node: node1. Reason:
No volumes created yet for the SVM. Wrapped KEK status will be available
after creating encrypted volumes."
},
"svm": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"tenant_id": "zzzzzzzz-yyy-zzzz-yyy-zzzzzzzzzzz",
"uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type

```



```

|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

```

```
|===
```

```
[#_links]  
[.api-collapsible-fifth-title]  
_links
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|self  
|link:#href[href]  
a|
```

```
|===
```

```
[#azure_reachability]  
[.api-collapsible-fifth-title]  
azure_reachability
```

Indicates whether or not the AKV service is reachable from all the nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|code  
|integer
```

a|Code corresponding to the status message. Returns a 0 if AKV service is reachable from all nodes in the cluster.

```
|message  
|string
```

a|Error message set when reachability is false.

```
|reachable
|boolean
a|Set to true when the AKV service is reachable from all nodes of the
cluster.
```

```
|===
```

```
[#node]
[.api-collapsible-fifth-title]
node
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|
```

```
|uuid
|string
a|
```

```
|===
```

```
[#ekmip_reachability]
[.api-collapsible-fifth-title]
ekmip_reachability
```

Provides the connectivity status for the given SVM on the given node to all EKMIP servers configured on all nodes of the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the error message. Returns a 0 if a given SVM is
able to communicate to the EKMIP servers of all of the nodes in the
cluster.

|message
|string
a|Error message set when cluster-wide EKMIP server availability from the
given SVM and node is false.

|node
|link:#node[node]
a|

|reachable
|boolean
a|Set to true if the given SVM on the given node is able to communicate to
all EKMIP servers configured on all nodes in the cluster.

|===

[#state]
[.api-collapsible-fifth-title]
state

Indicates whether or not the AKV wrapped internal key is available cluster
wide.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]
|===

```

```

|Name
|Type
|Description

|available
|boolean
a|Set to true when an AKV wrapped internal key is present on all nodes of
the cluster.

|code
|integer
a|Code corresponding to the status message. Returns a 0 if AKV wrapped key
is available on all nodes in the cluster.

|message
|string
a|Error message set when top-level internal key protection key (KEK)
availability on cluster is false.

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

```

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

```
[#error]
```

```
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[ID3c023a87413a52ed5d5cb484a2f35d99]]
= Update the AKV configuration
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/azure-key-vaults/{uuid}`#
```

Introduced In: 9.8

Updates the AKV configuration.

== Optional properties

* `client_secret` - New secret used to prove the application's identity to the AKV.

* `client_certificate` - New PKCS12 certificate used to prove the application's identity to the AKV.

* `proxy_type` - Type of proxy (http, https etc.) if proxy configuration is used.

* `proxy_host` - Proxy hostname if proxy configuration is used.

* `proxy_port` - Proxy port number if proxy configuration is used.

* `proxy_username` - Proxy username if proxy configuration is used.

* `proxy_password` - Proxy password if proxy configuration is used.

* `client_id` - Application (client) ID of the deployed Azure application with appropriate access to an AKV.

* `tenant_id` - Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV.

== Related ONTAP commands

```
* `security key-manager external azure update-client-secret`
* `security key-manager external azure update-credentials`
* `security key-manager external azure update-config`
```

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|AKV UUID
```

```
|return_timeout
```

```
|integer
```

```
|query
```

```
|False
```

a|The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

```
* Default value: 1
```

```
* Max value: 120
```

```
* Min value: 0
```

```
|===
```

== Request Body

```
[cols=3*,options=header]
```



```

|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|authentication_method
|string
a|Authentication method for the AKV instance.

|azure_reachability
|link:#azure_reachability[azure_reachability]
a|Indicates whether or not the AKV service is reachable from all the nodes
in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|client_certificate
|string
a|PKCS12 Certificate used by the application to prove its identity to AKV.

|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.

|client_secret
|string
a|Secret used by the application to prove its identity to AKV.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|key_id
|string
a|Key Identifier of AKV key encryption key.

```

```

|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.

* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri
* Introduced in: 9.8
* readCreate: 1


|proxy_host
|string
a|Proxy host.


|proxy_password
|string
a|Proxy password. Password is not audited.


|proxy_port
|integer
a|Proxy port.


|proxy_type
|string
a|Type of proxy.


|proxy_username
|string
a|Proxy username.


|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".


|state
|link:#state[state]
a|Indicates whether or not the AKV wrapped internal key is available
cluster wide.

```

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|svm
|link:#svm[svm]
a|
```

```
|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.
```

```
|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).
```

```
|===
```

.Example request

[%collapsible%closed]

=====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "authentication_method": "client_secret",
  "azure_reachability": {
    "code": 346758,
    "message": "AKV service is not reachable from all nodes - reason."
  },
  "client_certificate":
  "MIIQKQIBAzCCD+8GCSqGSIb3DQEHAaCCD+AEgg/cMIIIP2DCCBg8GCSqGSIb3DQEHBqCCBgAwg
gX8AgEAMIIF9QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIWkY7ojViJDYCAggAgIIFyJP
jIfmM6yTCKVw5ep2oZLwvvRca8pKhISVjw+WjWngh/f6Py/Ty0CwCjDFUZPsUUdSmk78E7SAz0
CpQyBwmUuFJQShjZjftHLKRWld3O4sJKB8DzH9Yw1C7En94cyJ1rT4WYoVFmeJcmOXx6h+NFHc
7njtXVsKwxc5BF88K3+3kHdV3WyVdXoeXe7yY/+EjFfjtBryp8ljuielX/NFlh5kowhoj+yxnO
0c1/00I1iV3mTIOTXD8qrZVp9ZhAxSTRBd5uDyWMfppqxW2L+9vCUU+ZgmRxtU3VsRLOp/T140
OP7Sn1Ch2OE0bIrbYYtcpi04QcUtfEJBMlbbTbJPHDAtiO2KIQKviZL4QMZgho9NNgL4MUpIbN
```

SzDCbuIC+nNMXfgfs0nPZewY+b43H/tMmnZ8Q4kiCFwrUqbFbflBiPMOaJsS0eQaJhDmzM90QE
gbesHWgPreAcfMUcNl+BaQHFLHUxLXDxQix6zYiCatDX6/EKlirRh1TFpmFX2PBd+X6uODhmwm
4ub9RKj3In8t5qgtN4q/mTBXjAVDABTIIegobBRaXGSSXCbc9W/jRed0DRZD9Bm8T/nV39sZNd
ucwZa5ojYTX8fFMA0cfY6IFivXHjB00coHEEGdgCfC0G8vACqLbb+2NuhMJpTr7Ig50iAPUMc6
70Z5ItOTQhyYOZ/KagOtvV8sKPCzeAkcMoHlsm189V79zt1fCJQTVWnaGiMj5Orcbskk6vCxD
GeU6q1kgvXJKXOYRF8/wIpv8Y7/rEpnGwE/I0ZOXzdIDHXqA53B1zyOVem25ezWCD+kpoH89XJ
ssY1NjIMJhjVRED61w/DbSXg2yFu/v3ckGapVvTuyAiz5hWUNfl3pt++da6GoekKnLqtL4G/RG
XCnebLbXg838dlTGBznoCwGTVxXDeVYafz8AjI10qYtTmcBn56ya9kK7IHSkrnFX24xQRQOfmD
0Vob71pjdZ8r1aXKvD/1X2TkYJHoeEHq0nWpU8vwdG/xhv4YgKJGN9qsEZgiTXETUh5gak8elt
GNkP+fum+1Oql05oS+Swna5/eB8eFeJl2Oi48Xi5UapaTRHPfp6kZfPXOu9cEjhILowRIi6glg
7FubmoJcu5OvDIyP9JlyQklw2VtgNlm1QOIvzRenXmy18XnP50NTxx2cIwby8tIcdSn2C2qhj8
Gk7q8oxVZGiBgtz4BwzyKkypwm60BBRrHpAKLw6JM5RISeZnYQfIsId0tGgb6lgo0RJf0sFtb
uvZcSvLI+2Onj8KH1TlmMR4dbuCWE9Ym4sVRmD1D6/f6BoNH0DRg7TJkEFbOadJsNPGzHbKteL
daSMGTNUZ3hEDQeomakQMfvCgypbOLxrTTqfbenHRtN+iFNYW0zCUW6EJoAXp+lqFnwQL52Il2
QxwZikE01P2k0GharzAJkXnNaFGnmHIIP6wJrCCSDZwDmr7GI2R5evDlRi17QUg2sulxQV0U8z
ezzwIUgEe/Whf0ngGJv/QcsL2jyri/tSQBUws4g+yep4SlE3iddhfqSJzI2iKdAE+HLiHGVO1z
70fGEsO6dPLnmh4eoWidgZi9N/SoBylaT0JpIQ6z6N5ImPfdWu9Y6TWXUg1iyOIXGsxiQVIgUN
oB5Ru/ApDxpYpFLk0fh9k9OnEWK5Im33puOQKLno1uwrOmdBg8+x1EY8wc9FvkHGH0Zh4HydiC
VUCYSdiGWUxVmgm4OgyiYzcpB+Ar2dzikGc4pBg8fa1a1HN5Q3TK3w4h/HeOUlMA4vWOYuVO1H
93ILGP6PWfkug+1Tam6+8yD0W5meiZ0UIZR8TF/9gDb4+4wTFnPwgfTrggEauA8tt8uJtiyBCr
YexgZTXIZGTUj/86KXQaJKCreRr/kqwJOWqkNW4CGUVzw7LiI+sArOZqUp/TsxnbcNC73XCMNlP
snByb2zCeK13V26Crl84U9sDuqQTJRaIse01MN9AAjpa2QWEwgnBBgkqhkiG9w0BBwGgggmyB
IIJrjCCCaowggmmBgsqhkiG9w0BDAoBAqCCCW4wgg1qMBwGCiqGSIb3DQEMAQMwDgQIEjm88b1
+pnkCAggABIIJSD3P+vn11SolmQvmYgZVfV37T3KpurJvMxQScPvalWiF7Q1Iwasf/+N0hKKN
r2j/aGZLunLkaG6mLPeBP212LCwnUxDu5kyffVVE90WX/bXewbYQribwFNkNhUrSgen8BfhnRl
vDrzbBLohIvDrUFszSVBCYh31Vwgu8p9SjC8K/XlumcLdjSFko85XpoK23euhowjWH+X0kRoYG
zorcdNE8z03BKvFR61W2XWzTSaWQ6eZHG56UrnX5Fe/w50U9tMIi3BCCCqgapUHVdmHqKkmWLi
kX8LssUcN30JVEkM2aJ9v4YO6CoegKAMVDs0tVSov3KbGC3GNX6lgHu4y1LOZPLPlfPXb0wDHq
avlXK3zphl8sIRzuX3HXSdEdenHYAkSV/IQZ89h+CZUkf0nu/og8eoA8ATDA5g7fj3HXpQ6cYd
rUBaHc7ruxHOiWR0GcT4XK4TTz7zZTO1wWPViprUo6ayw0dYZSG22MeDA027YirM044Ifosn9C
sqnNLZoOWvA2ao4ippDoBRqv5Hv6n0I3fOAys5nPq3jJtKQ5neqUYo0MrAkoKHO0h6zn0Bfvis
yB88aM9N0mPD76ykbAERq7151biKbA2tk8bb9dy/sJmk2ojM/D/W1YtrNL4iM6azL2kVN5eiCh
xCof33/RuRpXfGR8YNeJTl7bq42wL70QKDBRoG1TPcLqdVqz74oshlRspfqvZsbsUatbASbt2T
0YG4zfGfGh7sb2ezyougVvzdp77wAJ6n39dc/ZLDdYDzFkQb07984y8LlhIM1AcwFcMh43gWp6
A8CJ02174ednirSqSVOPZ7K9dRw6Y0X8MB4/WGzEcVFeHYIGLBcXi1sBY5wjWnbeuhlWLiSkMD
QRB6oGOvF7bJsilkx5PwgWbbqw8KUSuU01skbMAa5T8Hkm4OiSTf2a78E0zIKLGZg7yu9FDIIt
WYWokG96MXEBADouH+wWYmaEexh51ONrfFwKDuDMZh7MO20TTEQU8oQdjRRoAofXvTcj22GSMT
Y6XleskZX2ZKxSQdD1tCtkjGRKHSTYza3zLHbBiJTIJw4z6sw9FyTTApG66UAkNtiMalr9nqTT
NaxRWEXMEQVRLzAL2F9aqjgW65xrbYXu/J9Y/SYTCyBx2SRA/JkQ+Y8F68KOoS1pvK1p5/FcED
vprTNDs4lf+aj3HNWuK5wOsrpBhMlb2IfLuK/9QwPh9IC/RhHRfimyTPRXAf73cehNdp8DpKwL
m+jr30vazFwICpvSbi6Etb6GXfPkKaX7ztpQBqG92m2/0g3LWfPtilzwrPHPBz8y1qQMU268Do
o8YvWtI4KGaDAFb6XQhR6t6mqoq/3IP6/g//PZVENsYUVsPLDJLLF9fiOwTbMZnaiscKv8SGEs
//B9JkKrdSrRQRZcnnPjJnJLILblRVAZGuXpSKSYVPzYmOjUx3sSeLSiPoSOcqRIJ0X3s4ED09
2W3tr4ZXK3fnkFyrIVtrJsb3k/2smiQ6PclVuKhhlyTzYjXKRQcDaY3EDP9IWFtjiUfZQoZcij
MWt6YXim23m2aN2Ed8qIedikR6OjFHE4Kus/2yegTszSs5CrM7NamKWzeIeNNth/cTcmT++GDu
msGNTBAsHHSq1KYpqLi4GKLHzU7WNCQRdAcIDEvMZH/CHlmZK7bzb9z038rPf/D5WZrcK1ttdd5

```

BjTJjj7GerS0xLkvYIk1AJqurjMdWYmQtT4JAHF90/zRKqFFVpSiW074bRQ+PfaLI5C+TwoX5l
YD+R91A0qyGKIkFITa8hZFY+Up+rSuREqnpAvdAVL9/gLPF6I+5+D+sVBsGRbw2rFVRbCHdwaT
QcAVPeJJy0f/+sOs/PXoejr3siORpf8iLLYOaziGYf1EtunFcCLj8PEOznaUyouJ+lm9YKPBSL
ULC/sVVy6XUArYfJfq0Ag3lYXpJeWPbORxVP/VCm8d/sNjWTQXGN/IjNZaZuliXNgq5nRkPBKw
F23ZUYG4pLGpGROLup9nLSgEbpiDmN1Gq/IHSfI/8HpG/yRAoCdqUdre3yL/f9caj8RBBHRYbb
fRxtYQ9u2vsrqoloZ7F+Mu+kjuc9BxCMvJ7JaKwvQJckAkzTo6t10t6MzwiqJ7Au+2oOJ2Ukb/
985+TFGS219fmqWfwisOfpuvSkjRj8vIDBBm9itKIS+pVpfz+Mg7kl3WmkUrgF3yjTH5/C51ua
SzK2KeEVoWPx/Ps2CX7ATo6AsETp8Na38dT6d+Dm4WM4sBieKt/yOEFhiBNkgpVKAqawKRvLW3
U73OIKC8VLFhnnU+ogGxcUq5mZXvMbNDIaU2LvtmtPPo/qL0bOYu76TKc1ZX0R6AXkeImQgRPs
deXPPANtW3la585oZbYxUXRfEIEKmkcv3eSGnPCVesbxxdlSaIJe2j7H9MbHdjYkeFQuECnUhK
xg63BVPl/qAEIO5+OKBzM7ctuP8apeGW1iHAueKzJXc5IeFS/3iwkfDLRkrzBeNIL0IINo3Co
GSvn95Z8+LhNSopyqt3uB4rQksUYIwXgkfrEVYujCO0T5dSkk5j10X7WlDm4DHZVLJH+GtL6v9
A6xFJNDQfQF0hS+w1XkTkMq7pUiX+Qohf8QRJZEyU5VWo2CesR63j1MFpkB3xybpbjt8oI47XC
20GEn3uCjwMwq/3K4ibHnqil6pPPRgi/u3R9TVfvOC2e0xgllrFG6cKUfoguXoxHqP1KKjUw2
3bpd9L09LzSDdSHcoDPokWzDee0ZP/Z6VH3rdjQR71kw4VBeT8nKfLP2dGBd0tpWDQhCFK7I9a
xxxthnv0v09x/J7jhyoLRt5e8lMEfrqtnMWdqjFgYVEQndthZ+9/XvfNk6f5MD8fDheMuvbNTh
duFSZEczCLlW4GWKneVji4wdBrV3aCrzAzxy0H7y7nnkyCEvac503UDtr1bk1VJIVsYfYrN2S2
DPbp3H2E8r/n6jfBilwFyp3JTJvnRqQTcYHXDieW8Njq46JO6O6wsPwKQTKMfHGxxTRJdRe5yv
JD54xvFWw1YEJ/Q2c8cr1NNXEN32e5psfIJ7o48k6bsiyXnbHKSjK781Z5h8Hc3FbUF2U2p5Jq
LwcD7+bknEunsbWSC37iMk7oweF3hMhKRMm9iYJ8tpxMRcWCot7ador+Y2fYWBsu/bwXwcRI08
TElMCMGCSqGSib3DQEJFTEWBBRymjnEbJmrRwh4sRnwudfSQP6KDAxMCEwCQYFKw4DAhoFAAQ
U+YFhgKEYjfXN/cL70YrRJSHFgUwECHeCTQnUEU0BAGIIAA==",
  "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaaa",
  "client_secret": "abcdef",
  "ekmip_reachability": {
    "code": 346758,
    "message": "embedded KMIP server status unavailable on node.",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  },
  "key_id": "https://keyvault1.vault.azure.net/keys/key1",
  "name": "https://kmip-akv-keyvault.vault.azure.net/",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "svm",
  "state": {

```

```

    "code": 346758,
    "message": "Top-level internal key protection key (KEK) is unavailable
on the following nodes with the associated reasons: Node: node1. Reason:
No volumes created yet for the SVM. Wrapped KEK status will be available
after creating encrypted volumes."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzz",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Response

```

Status: 200, Ok

```

== Response

```

Status: 202, Accepted

```

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===

```

```

| Error Code | Description

```

```

| 65537120

```

```

| Azure Key Vault is not configured for the given SVM.

```

```

| 65537504

```

```

| Internal error. Failed to store configuration in internal database.

```

```

| 65537517

```

```

| The field "client_secret" must be specified.

| 65537540
| Invalid client secret.

| 65537541
| No inputs were provided for the patch request.

| 65537547
| One or more volume encryption keys for encrypted volumes of this data
SVM are stored in the key manager configured for the admin SVM. Use the
REST API POST method to migrate this data SVM's keys from the admin SVM's
key manager to this data SVM's key manager before running the rekey
operation.

| 65537573
| Invalid client certificate.

| 65537577
| The AKV certificate authentication method cannot be configured for the
given SVM as not all nodes in the cluster support the AKV certificate
authentication.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",

```

```

        "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
}
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self
|link:#href[href]
a|

```



```
|===
```

```
[#azure_reachability]
[.api-collapsible-fifth-title]
azure_reachability
```

Indicates whether or not the AKV service is reachable from all the nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|integer
```

a|Code corresponding to the status message. Returns a 0 if AKV service is reachable from all nodes in the cluster.

```
|message
|string
```

a|Error message set when reachability is false.

```
|reachable
|boolean
```

a|Set to true when the AKV service is reachable from all nodes of the cluster.

```
|===
```

```
[#node]
[.api-collapsible-fifth-title]
node
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|
```

```
|uuid
|string
a|
```

```
|===
```

```
[#ekmip_reachability]
[.api-collapsible-fifth-title]
ekmip_reachability
```

Provides the connectivity status for the given SVM on the given node to all EKMIP servers configured on all nodes of the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|integer
```

a|Code corresponding to the error message. Returns a 0 if a given SVM is able to communicate to the EKMIP servers of all of the nodes in the cluster.

```
|message
|string
```

a|Error message set when cluster-wide EKMIP server availability from the

given SVM and node is false.

```
|node
|link:#node[node]
a|
```

```
|reachable
|boolean
a|Set to true if the given SVM on the given node is able to communicate to
all EKMIP servers configured on all nodes in the cluster.
```

```
|===
```

```
[#state]
[.api-collapsible-fifth-title]
state
```

Indicates whether or not the AKV wrapped internal key is available cluster wide.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|available
|boolean
```

```
a|Set to true when an AKV wrapped internal key is present on all nodes of
the cluster.
```

```
|code
|integer
```

```
a|Code corresponding to the status message. Returns a 0 if AKV wrapped key
is available on all nodes in the cluster.
```

```
|message
```

```
|string
a|Error message set when top-level internal key protection key (KEK)
availability on cluster is false.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#azure_key_vault]
[.api-collapsible-fifth-title]
azure_key_vault
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
```

```

a|

|authentication_method
|string
a|Authentication method for the AKV instance.


|azure_reachability
|link:#azure_reachability[azure_reachability]
a|Indicates whether or not the AKV service is reachable from all the nodes
in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.


|client_certificate
|string
a|PKCS12 Certificate used by the application to prove its identity to AKV.


|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.


|client_secret
|string
a|Secret used by the application to prove its identity to AKV.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|


|key_id
|string
a|Key Identifier of AKV key encryption key.


|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.

* example: https://kmip-akv-keyvault.vault.azure.net/

```

```
* format: uri
* Introduced in: 9.8
* readCreate: 1
```

```
|proxy_host
|string
a|Proxy host.
```

```
|proxy_password
|string
a|Proxy password. Password is not audited.
```

```
|proxy_port
|integer
a|Proxy port.
```

```
|proxy_type
|string
a|Type of proxy.
```

```
|proxy_username
|string
a|Proxy username.
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|state
|link:#state[state]
a|Indicates whether or not the AKV wrapped internal key is available
cluster wide.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.
```

```
|svm
```

```

|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====


[[ID366c8eece25677fd50c81f88acbb775b]]
= Re-key the internal key in the key hierarchy for an SVM


[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/azure-key-vaults/{uuid}/rekey-internal`#


*Introduced In:* 9.10


Rekeys the internal key in the key hierarchy for an SVM with an AKV
configuration.


== Related ONTAP commands


* `security key-manager external azure rekey-internal`

```


== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True

a|UUID of the existing AKV configuration.

|return_timeout
|integer
|query
|False

a|The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

* Default value: 1
* Max value: 120
* Min value: 0

|return_records
|boolean
|query
|False

a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Response

Status: 202, Accepted

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 65537120
```

```
| Azure Key Vault is not configured for the given SVM.
```

```
| 65537547
```

```
| One or more volume encryption keys for encrypted volumes of this data
SVM are stored in the key manager configured for the admin SVM. Use the
REST API POST method to migrate this data SVM's keys from the admin SVM's
key manager to this data SVM's key manager before running the rekey
operation.
```

```
| 65537559
```

```
| There are no existing internal keys for the SVM. A rekey operation is
allowed for an SVM with one or more encryption keys.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```

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

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====

```

```

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

```

```

|===

```

```

[#error]
[.api-collapsible-fifth-title]
error

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID0a6b3383c9bcb7e7ff43619169bd8d60]]
= Restore keys for an SVM from a configured AKV

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/azure-key-vaults/{uuid}/restore`#

*Introduced In:* 9.10

Restore the keys for an SVM from a configured AKV.

== Related ONTAP commands

* `security key-manager external azure restore`

```

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

|True

a|UUID of the existing AKV configuration.

|return_timeout

|integer

|query

|False

a|The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

* Default value: 1

* Max value: 120

* Min value: 0

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

* Default value:

|==

== Response

Status: 202, Accepted

== Error

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 65537120  
| Azure Key Vault is not configured for the given SVM.  
  
| 65537515  
| Failed to restore keys on some nodes in the cluster.  
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{  
  "error": {  
    "arguments": {  
      "code": "string",  
      "message": "string"  
    },  
  },  
}
```

```

    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

```

```

|===

```

```

[#error]
[.api-collapsible-fifth-title]
error

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

[[IDa2b4a9950d86a89294dd217b9c2ad699]]
= Create a certificate signing request

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/certificate-signing-request`#

*Introduced In:* 9.8

This API generates a Certificate Signing Request(CSR) and a private key
pair. A CSR is a message sent securely to a certificate authority (CA) via
any electronic media to apply for a digital identity certificate. This is
a general utility API for users to generate a CSR.

== Recommended optional properties

* `subject_name` - Subject details of the certificate.

```


- * `security_strength` - Key size of the certificate in bits. Specifying a stronger security strength in bits is recommended when creating a certificate.
- * `hash_function` - Hashing function.
- * `algorithm` - Asymmetric algorithm. Algorithm used to generate a public/private key pair when creating a certificate.
- * `subject_alternatives` - Subject Alternate name extensions.

== Default property values

If not specified in POST, the following default property values are assigned:

- * `security_strength` - `_112_`
- * `hash_function` - `_sha256_`
- * `algorithm` - `_rsa_`

== Related ONTAP commands

- * `security certificate generate-csr``

== Parameters

[cols=5*,options=header]
|===

Name
Type
In
Required
Description

return_records
boolean
query
False

a|The default is false. If set to true, the records are returned.

- * Default value:

|===

== Request Body

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|algorithm
|string
a|Asymmetric Encryption Algorithm.

|csr
|string
a|A Certificate Signing Request (CSR) provided to a CA for obtaining a CA-
signed certificate.

|extended_key_usages
|array[string]
a|A list of extended key usage extensions.

|generated_private_key
|string
a|Private key generated for the CSR.

|hash_function
|string
a|Hashing function.

|key_usages
|array[string]
a|A list of key usage extensions.

|security_strength
|integer
a|Security strength of the certificate in bits.

|subject_alternatives

```

```
|link:#subject_alternatives[subject_alternatives]
a|

|subject_name
|string
a|Subject name details of the certificate. The format is a list of comma
separated key=value pairs.

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "algorithm": "rsa",
  "csr": "string",
  "extended_key_usages": {
  },
  "generated_private_key": "string",
  "hash_function": "sha256",
  "key_usages": {
  },
  "security_strength": 112,
  "subject_alternatives": {
    "dns": {
    },
    "email": {
    },
    "ip": {
    },
    "uri": {
    }
  },
  "subject_name": "C=US,O=NTAP,CN=test.domain.com"
}
=====

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|algorithm
|string
a|Asymmetric Encryption Algorithm.

|csr
|string
a|A Certificate Signing Request (CSR) provided to a CA for obtaining a CA-
signed certificate.

|extended_key_usages
|array[string]
a|A list of extended key usage extensions.

|generated_private_key
|string
a|Private key generated for the CSR.

|hash_function
|string
a|Hashing function.

|key_usages
|array[string]
a|A list of key usage extensions.

|security_strength
|integer
a|Security strength of the certificate in bits.
```

```
|subject_alternatives
|link:#subject_alternatives[subject_alternatives]
a|
```

```
|subject_name
|string
a|Subject name details of the certificate. The format is a list of comma
separated key=value pairs.
```

```
|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "algorithm": "rsa",
  "csr": "string",
  "extended_key_usages": {
  },
  "generated_private_key": "string",
  "hash_function": "sha256",
  "key_usages": {
  },
  "security_strength": 112,
  "subject_alternatives": {
    "dns": {
    },
    "email": {
    },
    "ip": {
    },
    "uri": {
    }
  },
  "subject_name": "C=US,O=NTAP,CN=test.domain.com"
}
```

```
====
```

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 3735554
```

```
| Certificate signing request failed.
```

```
| 3735664
```

```
| Key size is not supported in FIPS mode.
```

```
| 3735665
```

```
| Hash function is not supported in FIPS mode.
```

```
| 3735700
```

```
| Key size is not supported.
```

```
| 3735713
```

```
| Security strength bits length is not supported.
```

```
| 3735714
```

```
| Security strength bits length is not supported in FIPS mode.
```

```
| 3735715
```

```
| Certificate creation requires a common name or SAN extensions.
```

```
| 3735741
```

```
| Key size is not applicable with the EC encryption algorithm.
```

```
| 52560173
```

```
| Hash function is not supported for digital signatures.
```

```
| 52560423
```

```
| Failed to read the relative distinguished names.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```

|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href

```

```

|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#subject_alternatives]
[.api-collapsible-fifth-title]
subject_alternatives

[cols=3*,options=header]
|===
|Name
|Type
|Description

|dns
|array[string]
a|A list of DNS names for Subject Alternate name extension.

|email
|array[string]
a|A list of email addresses for Subject Alternate name extension

|ip
|array[string]
a|A list of IP addresses for Subject Alternate name extension.

```



```
|uri
|array[string]
a|A list of URIs for Subject Alternate name extension.
```

```
|===
```

```
[#certificate_signing_request]
[.api-collapsible-fifth-title]
certificate_signing_request
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|algorithm
|string
a|Asymmetric Encryption Algorithm.
```

```
|csr
|string
a|A Certificate Signing Request (CSR) provided to a CA for obtaining a CA-
signed certificate.
```

```
|extended_key_usages
|array[string]
a|A list of extended key usage extensions.
```

```
|generated_private_key
|string
a|Private key generated for the CSR.
```

```
|hash_function
|string
a|Hashing function.
```

```
|key_usages
|array[string]
a|A list of key usage extensions.
```

```
|security_strength
|integer
a|Security strength of the certificate in bits.
```

```
|subject_alternatives
|link:#subject_alternatives[subject_alternatives]
a|
```

```
|subject_name
|string
a|Subject name details of the certificate. The format is a list of comma
separated key=value pairs.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```

```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

= Manage security certificates

:leveloffset: +1

[[IDb39d2f3c031f0db0796717ff61278562]]
= Security certificates endpoint overview

```

== Overview

This API displays security certificate information and manages the certificates in ONTAP.

== Installing certificates in ONTAP

The security certificates GET request retrieves all of the certificates in the cluster.

== Examples

=== Retrieving all certificates installed in the cluster with their common-names

```
# The API:
/api/security/certificates
```

```
# The call:
curl -X GET "https://<mgmt-
ip>/api/security/certificates?fields=common_name" -H "accept:
application/hal+json"
```

```
# The response:
{
  "records": [
    {
      "svm": {
        "name": "vs0"
      },
      "uuid": "dad2363b-8ac0-11e8-9058-005056b482fc",
      "common_name": "vs0",
      "_links": {
        "self": {
          "href": "/api/security/certificates/dad2363b-8ac0-11e8-9058-
005056b482fc"
        }
      }
    },
    {
      "uuid": "1941e048-8ac1-11e8-9058-005056b482fc",
      "common_name": "ROOT",
      "_links": {
```

```

        "self": {
            "href": "/api/security/certificates/1941e048-8ac1-11e8-9058-005056b482fc"
        }
    },
    {
        "uuid": "5a3a77a8-892d-11e8-b7da-005056b482fc",
        "common_name": "gshanccluster-4",
        "_links": {
            "self": {
                "href": "/api/security/certificates/5a3a77a8-892d-11e8-b7da-005056b482fc"
            }
        }
    }
],
"num_records": 3,
"_links": {
    "self": {
        "href": "/api/security/certificates?fields=common_name"
    }
}
}
}
----
'''

```

=== Retrieving all certificates installed at cluster-scope with their common-names

```
'''
```

```
----
```

```
# The API:
/api/security/certificates

```

```
# The call:
curl -X GET "https://<mgmt-ip>/api/security/certificates?scope=cluster&fields=common_name" -H
"accept: application/hal+json"

```

```
# The response:
{
"records": [

```

```

{
  "uuid": "1941e048-8ac1-11e8-9058-005056b482fc",
  "scope": "cluster",
  "common_name": "ROOT",
  "_links": {
    "self": {
      "href": "/api/security/certificates/1941e048-8ac1-11e8-9058-005056b482fc"
    }
  }
},
{
  "uuid": "5a3a77a8-892d-11e8-b7da-005056b482fc",
  "scope": "cluster",
  "common_name": "gshanccluster-4",
  "_links": {
    "self": {
      "href": "/api/security/certificates/5a3a77a8-892d-11e8-b7da-005056b482fc"
    }
  }
}
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/security/certificates?scope=cluster&fields=common_name"
  }
}
}

```

'''

=== Retrieving all certificates installed on a specific SVM with their common-names

'''

```

# The API:
/api/security/certificates

# The call:
curl -X GET "https://<mgmt-

```

```
ip>/api/security/certificates?svm.name=vs0&fields=common_name" -H "accept:
application/hal+json"
```

```
# The response:
```

```
{
  "records": [
    {
      "svm": {
        "name": "vs0"
      },
      "uuid": "dad2363b-8ac0-11e8-9058-005056b482fc",
      "common_name": "vs0",
      "_links": {
        "self": {
          "href": "/api/security/certificates/dad2363b-8ac0-11e8-9058-
005056b482fc"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/certificates?svm.name=vs0&fields=common_name"
    }
  }
}
```

```
----
```

```
'''
```

```
=== Retrieving a certificate using its UUID for all fields
```

```
'''
```

```
----
```

```
# The API:
```

```
/api/security/certificates/{uuid}
```

```
# The call:
```

```
curl -X GET "https://<mgmt-ip>/api/security/certificates/dad2363b-8ac0-
11e8-9058-005056b482fc?fields=*" -H "accept: application/hal+json"
```

```
# The response:
```

```
{
```

```

"svm": {
  "uuid": "d817293c-8ac0-11e8-9058-005056b482fc",
  "name": "vs0"
},
"uuid": "dad2363b-8ac0-11e8-9058-005056b482fc",
"scope": "svm",
"type": "server",
"common_name": "vs0",
"serial_number": "15428D45CF81CF56",
"ca": "vs0",
"hash_function": "sha256",
"key_size": 2048,
"expiry_time": "2019-07-18T15:29:14-04:00",
"public_certificate": "-----BEGIN CERTIFICATE-----
\nMIIDQjCCAiqqAwIBAgIIFUKNRc+Bz1YwDQYJKoZIhvcNAQELBQAwGzEMMAoGA1UE\nnAxMDdn
MwMQswCQYDVQQGEwJVUzAeFw0xODA3MTgxOTI5MTRaFw0xOTA3MTgxOTI5\nnMTRaMBsxDDAKBg
NVBAMTA3ZzMDELMAkGA1UEBhMCVVMwgGEiMA0GCSqGSIb3DQEB\nnAQUAA4IBDwAwggEKAoIBAQ
CqFQb27th2AComJvWgLh1xRzobSb2ZTQfO561faXQ3\nnIbiT+rnRWXetd/s2+iCv91d9LW0NOM
P3MN2f3SFbyze3dl7WrnVbjLmYuI9MfOxs\nnfmA+Bh6gpap5Yn2YddqoV6rfNGAuUveNLArNl8
wODk/mpawpEQ93QSa1Zfg1gnoH\nnRFRyqiSYT06X5g6RbUuEl4LTGXspz+plU46Za0i6QyxtvZ
4bneibffXN3IigpqI6\nnTGUV8R/J3Ps338VxVmSO9ZXBZmvmvbcJVoySYNICl/oi3fgPZlnBv0tb
swqg4FoZO/\nnWT+XHGHLeP6cr/Aqg7u6C4RfqbCwzB/XFKDIqnmAQkDBAgMBAAGjgYkwgYYwDA
YD\nnVR0TBAUwAwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFN/AnH8qLxocTtumNHIn\nnEN4I
FIDBMEoGA1UdIwRDMEGAFN/AnH8qLxocTtumNHInEN4IFIDBoR+kHTAbMQww\nnCgYDVQQDEwN2
czAxCzAJBgNVBAYTA1VTgggVQo1Fz4HPVjANBgkqhkiG9w0BAQsF\nnAAOCAQEAA0pUEepdeQnd
2Amwg8UFyxayb8eu3E6dlptvtyp+xtjhIC7Dh95CVXhy\nnkJS3Tsu60PGR/b2vc3MZtAUpcL4c
eD8XntKPQgBlqoB4bRogCe1TnlGswRXDX5TS\nngMvRrjaWTBF7ikT4UjR05rSxcDGplQRqjnOt
hqi+yPT+29+8a4Uu6J+3Kdrflj4p\nnl1nSWpuB9EyxtuCILNqXA2ncH7YKtoeNtChKCchhvPcoT
y6Opma6UQn5UMxstkvtGT\nnVGaN5TlRWv0yiqPXIQblSqXi/uQsuRPcHDu7+KWRfn08USa6QVo2
mDs9P7R9dd0K\nn9QAsTjTOF9PlAKgNxGoOJl2y0+48AA==\nn-----END CERTIFICATE-----
\n",
"_links": {
  "self": {
    "href": "/api/security/certificates/dad2363b-8ac0-11e8-9058-
005056b482fc"
  }
}
}
}
-----

```

=== Creating a certificate in a cluster

These certificates can be used to help administrators enable certificate-based authentication and to enable SSL-based communication to the cluster.

```
# The API:
/api/security/certificates
```

```
# The call:
```

```
curl -X POST "https://<mgmt-ip>/api/security/certificates" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
\"common_name\": \"TEST-SERVER\", \"type\": \"server\" }"
```

```
----
```

```
=== Installing a certificate in a cluster
```

These certificates can be used to help administrators enable certificate-based authentication and to enable-SSL based communication to the cluster.

```
----
```

```
# The API:
/api/security/certificates
```

```
# The call:
```

```
curl -X POST "https://<mgmt-ip>/api/security/certificates" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"type\":
\"server_ca\", \"public_certificate\": \"-----BEGIN CERTIFICATE-----
\\nMIIIFYDCCA0igAwIBAgIQCgFCgAAAAUjyES1AAAAAANBgkqhkiG9w0BAQsFADBKMQswCQYD
VQQG\\nEwJVUzESMBAGA1UEChMJSWRlbnRydXN0MScwJQYDVQQDEx5JZGVuVHJlcnQgQ29tbWVy
Y2lhbCBS\\nb290IENBIDEwHhcNMTQwMTE2MTg5MjIzWWhcNzQwMTE2MTg5MjIzWjBKMQswCQYD
VQQGEwJVUzES\\nMBAGA1UEChMJSWRlbnRydXN0MScwJQYDVQQDEx5JZGVuVHJlcnQgQ29tbWVy
Y2lhbCBSb290IENB\\nIDEwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCnUBneP5k9
1DNG8W9RYYKyqU+PZ4ld\\nhNlT3Qwo2dfw/66VQ3KZ+bVdfIrBQuExUHTRgQ18zZshq0PirK1e
hm7zCYofWjK9ouuU+ehcCuz/\\nmNKvcb00U59Oh++SvL3sTzIwiEsXXlfEU8L2ApeN2WIrVYQf
Yo3fw7gps014PJNgiCL8mdo2yMKi\\n1CxUAGclbnO/AljwpN3lsKImesrgNqUZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTE13EASX2MN0C\\nXZ/g1Ue9tOsbobTJSdifWwLziuQkkORiT0/Br4sO
dBeo0XKlIanoBScy0RnnGF7HamB4HWfp1IYVl\\n3ZBWzvurpWCdxJ35UrClvYf5jysjCiN20/cz
4ckA82n5S6LgTrx+kzmEB/dEcH7+B1rlsazRGMzy\\nNeVJSQjKVsk9+w8YfYs7wRPCTY/JTw43
6R+hDmrfYi7LNQZReSzIJTj0+kuniVyc0uMNOYZKdHzV\\nWYfCP04MXFL0PfdSgvHqo6z9STQa
KPNBiDoT7uje/5kdX7rL6B7yuVBgwDHTc+XvvqDtMwt0viAg\\nxGds8AgDelWaf0ZOlqf0Hj7h
9tgJ4TNkK2PXm16f+cB7D3hvl7yTmvmcEpB4eoCHFddyJxVdHix\\nuuFucAS6T6C6aMN7/zHw
cz09lCqxC0EOoP5NiGVreTO0lwIDAQABo0IwQDAOBgNVHQ8BAf8EBAMC\\nAQYwDwYDVR0TAQH/
BAUwAwEB/zAdBgNVHQ4EFgQU7UQZwNPwBovupHu+QucmVMiONnYwDQYJKoZI\\nhvcNAQELBQAD
ggIBAA2ukDL2pkt8RHYZYR4nKM1eVO8lvOMIkPkp165oCOGUAFjvLi5+U1KMtlwH\\n6oi6mYtQ
lNeCgN9hCQCTrQ0U5s7B8jeUeLBfnLOic7iPBZM4zy0+sLj7wM+x8uwtLRvM7Kqas6pg\\nghst
O8OEPVeKlh6cdbhTMM1gCIOQ045U8U1mwF10A0Cj7oV+wh93nAbowacYXVKV7cndJZ5t+qnt\\n
ozo00Fl72u1Q8zW/7esUTTHHYPTa8Yec4kjixsU3+wYQ+nVZZjFHKdp2mhZpgq7vmrlR94gjmm
mV\\nYjz1VYA211QC//G5Xc7UI2/YRYRKW2XviQzdFKcgyxilJbQN+QHwotL0AMh0jqEqSI5l2x
PE4iUX\\nfeu+hlsXIFRRk0pTAwvsXcoz7WL9RccvW9xYoIA55vrX/hMUpu09lEpCdNTDd1lzzY
```

```

9Gv1U47/ro\nkTLq1lgEIt44w8y8bckzOmoKaT+gyOpyj4xjhiO9bTyWnpXgSUyqorkqG5w2gX
jtw+hG4iZZRHUe\n2XWJUc0QhJ1hYMTd+ZciTY6Y5uN/9lu7rs3KSoFrXgvzUeF0K+l+J6fZmU
lO+KWA2yUPHGNiiskz\nZ2s8EIPGrd6ozRaOjfAHN3Gf8qv8QfXBi+wAN10J5U6A7/qxXDgGpR
tK4dw4LTzcqx+QGtVKno7R\ncGzM7vRX+Bi6hG6H\n-----END CERTIFICATE-----\n\"
}
----

'''

=== Installing a certificate on a specific SVM

'''

----

# The API:
/api/security/certificates

# The call:
curl -X POST "https://<mgmt-ip>/api/security/certificates" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"svm\" : {
\"name\" : \"vs0\" }, \"type\": \"server_ca\", \"public_certificate\":
\"-----BEGIN CERTIFICATE-----
\nMIIFYDCCA0igAwIBAgIQCgFCgAAAAUjyESlAAAAjANBgkqhkiG9w0BAQsFADBKMQswCQYD
VQQG\nEwJVUzESMBAGA1UEChMJSWRlb1RydXN0MScwJQYDVQQDEx5JZGVuVHJlc3QgQ29tbWVy
Y2lhbCBS\nb290IENBIDEwHhcNMTQwMTE2MTgxMjIzWhcNMzQwMTE2MTgxMjIzWjBKMQswCQYD
VQQGEwJVUzES\nMBAGA1UEChMJSWRlb1RydXN0MScwJQYDVQQDEx5JZGVuVHJlc3QgQ29tbWVy
Y2lhbCBSb290IENB\nIDEwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCnUBneP5k9
1DNG8W9RYYKqU+PZ4ld\nnhNlT3Qwo2dfw/66VQ3KZ+bVdfIrBQuExUHTRgQl8zZshq0PirKle
hm7zCYofWjK9ouuU+ehcCuz/\nmNKvcbo0U59Oh++SvL3sTzIwiEsXXlfEU8L2ApeN2WIrvyQf
Yo3fw7gpS0l4PJNgiCL8mdo2yMKi\nlCcxUAGclbnO/AljwpN3lsKImesrgNqUZFvX9t++uP0Dl
bVoE/c40yiTcdCMbXTMTEl3EASX2MN0C\nnXZ/g1Ue9tOsobobTJSdifWwLziuQkkORiT0/Br4sO
dBeo0XKIanoBScy0RnnGF7HamB4HWfp1IYVl\nn3ZBWzvurpWCdxJ35UrCLvYf5jysjCiN2O/cz
4ckA82n5S6LgTrx+kzmEB/dEcH7+B1rlsazRGMzy\nnNeVJSQjKVsk9+w8Yfys7wRPCTY/JTw43
6R+hDmrfYi7LNQZReSzIJTj0+kuniVyc0uMNOYZKdHzV\nnWYfCP04MXFL0PfdSgvHqo6z9STQa
KPNBiDoT7uje/5kdX7rL6B7yuVBgwDHTc+XvvqDtMwt0viAg\nnxGds8AgDelWAF0ZOlqf0Hj7h
9tgJ4TNkK2PXMl6f+cB7D3hvl7yTmvmcEpB4eoCHFddyJxVdHix\nnuuFucAS6T6C6aMN7/zHw
cz09lCqxCOEOoP5NiGVreTO0lwIDAQABo0IwQDAOBgNVHQ8BAf8EBAMC\nnAQYwDwYDVR0TAQH/
BAUwAwEB/zAdBgNVHQ4EFgQU7UQZwNPwBovupHu+QucmVMiONnYwDQYJKoZI\nnhvcNAQELBQAD
ggIBAA2ukDL2pkt8RHYZYR4nKM1eVO8lvOMIkPkp165oCOGUAFjvLi5+U1KMtlwH\nn6oi6mYtQ
lNeCgN9hCQCTrQ0U5s7B8jeUeLBfnLOic7iPBZM4zy0+sLj7wM+x8uwtLRvM7Kqas6pg\nnghst
O8OEPVeKlh6cdbhTMM1gCIOQ045U8U1mwF10A0Cj7oV+wh93nAbowacYXVKV7cndJZ5t+qnt\nn
ozo00F172u1Q8zW/7esUTTHHYPTa8Yec4kjixsU3+wYQ+nVZZjFHKdp2mhZpgg7vmrlR94gjmm
mV\nnYjzlvYA211QC//G5Xc7UI2/YRYRKW2XviQzdFKcgyxilJbQN+QHwotL0AMh0jqEqSI5l2x
PE4iUX\nnfeu+hlsXIFRRk0pTAWvsXcoz7WL9RccvW9xYoIA55vrX/hMUpu09lEpCdNTDd1lzzY
9Gv1U47/ro\nkTLq1lgEIt44w8y8bckzOmoKaT+gyOpyj4xjhiO9bTyWnpXgSUyqorkqG5w2gX

```

```
jtw+hG4iZZRHUe\n2XWJUc0QhJlhYMTd+ZciTY6Y5uN/9lu7rs3KSoFrXgvzUeF0K+l+J6fZmU
lO+KWA2yUPHGNIiskz\nZ2s8EIPGrd6ozRaOjfAHN3Gf8qv8QfXBi+wAN10J5U6A7/qxXDgGpR
tK4dw4LTzcx+QGtVKn07R\ncGzM7vRX+Bi6hG6H\n-----END CERTIFICATE-----\n\"
}"
```

'''

=== Deleting a certificate using its UUID

'''

The API:

/api/security/certificates/{uuid}

The call:

```
curl -X DELETE "https://<mgmt-ip>/api/security/certificates/dad2363b-8ac0-
11e8-9058-005056b482fc?fields=*" -H "accept: application/hal+json"
```

=== Signing a new certificate signing request using an existing CA certificate UUID

Once you have created a certificate of type "root_ca", you can use that certificate to act as a local Certificate Authority to sign new certificate signing requests. The following example signs a new certificate signing request using an existing CA certificate UUID. If successful, the API returns a signed certificate.

The API:

/api/security/certificates/{ca.uuid}/sign

The call:

```
curl -X POST "https://<mgmt-ip>/api/security/certificates/253add53-8ac9-
11e8-9058-005056b482fc/sign" -H "accept: application/json" -H "Content-
Type: application/json" -d "{ \"signing_request\": \"-----BEGIN
CERTIFICATE REQUEST-----
\nMIICYTCCAUAkCAQAwhDENMASGA1UEAxMEVEVTVDELMAkGA1UEBhMCVVMwggEiMA0G\nCSqGSI
b3DQEBQUAA4IBDwAwggEKAoIBAQCICuVfbYHNdOO07vjRQja4JqL2cHqK\ndr1Tj5hz9RVqFK
Z7VPh8DSP9LoTbYWsvrTkbuD0Wi715MVQCsbkq/mHos+Y5lfqs\nNP5K92fc6EhBzBDYFgZGFn
tZYJjEG5MPerIUE7CfVy7o6sjWOlxeY33pjefObyvP\nBcJkBHg6SFJK/TDLvIYJkonLkJEOJo
TI6++a3I/1bCMfUeuRtLU9ThWlna1kMMYK\n4T16/Bxgm4bha2U2jtosc0Wltnld/capc+eqRV
07WVbMmEOTtop3cv0h3N0S6lbn\nFkd96DXzeGWbSHFHckeCZ9bOHhnVbfEa/efkPLx7ziMC8G
```

```
tRHhlwbnK7AgMBAAAg\nADANBgkqhkiG9w0BAQsFAAOCAQEaf+rs1i5PHaOSI2HtTM+Hcv/p71
yzgoLL+aeU\ntB0V4iuoXdqY8oQeWoPI92ci0K08JuSpu6D0DwCKlstfwuGkAA2b0Wr7ZDRonT
Uq\nmJ4j3047MLysW4Db2LbGws/AuDScIrBJDWHMpHaqsvRbpMx2xQ/V5oagUw5eGGpN\ne4fg
/E2k9mGkpxwkUzT7wlRZirpND4xL+XTzpzZqgalpXug4yjiXlI5hpRESZ9/\nAkGJSCWxI15I
ZdxxFVXlBcmm6WpJnnboqkcKeXz95GM6Re+oBy9tlgvwv1Vd5s8uHX+bycFiZp09Wsm8Ev727M
ziZ+0II9nxwkDKsdPvam+KLI9hLQ==\n-----END CERTIFICATE REQUEST-----\n",
\"hash_function\": \"sha256\"}"
```

```
# The response:
```

```
{
"public_certificate": "-----BEGIN CERTIFICATE-----
\nMIIDBzCCAe+gAwIBAgIIFUKQpcqeaUAWDQYJKoZIhvcNAQELBQAwdENMAAGA1UE\nFDWDELMAkGA1UEBhMCVVMwHhcNMTgwNzE4MjAzMTA1WhcNMTkwNzE4MjAz\nMTA1WjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcN\nAQEBBQADggEPADCCAQoCggEBBAKIEK5V9tgc1047u+NFCNrgmovZweop2uVOPmHP1\nnFWoUpntU+HwNI/0uhNthay+tORu4PRaLvXkxVAKxuSr+Yeiz5jmV+qw0/kr3Z9zo\nnSEHMENgWBkYWellgmMQbkW96shQTsJ9XLujqyNY6XF5jfemN585vK88FwmQEeDpI\nnUkr9MMu8hgmSicuQkQ4mhMjr75rcj/VsIx9R65G0tT1OFaWdrWQwxgrhPxr8HGCb\n\nhuFrZTaO2ixzRaW2eV39xqlz56pFXTtZVsyYQ502indy/SHc3RLqVucWR33oNfn4\n\nZZtIcUdyR4Jnls4eGdVt8Rr95+Q8vHvOIwLwa1EceXBucrsCAwEAAaNNMEswCQYD\n\nnVR0TBAlwADAdBgNVHQ4EFgQUJMPxjeWlG76TbbD2tXB8dwSpI3MwHwYDVR0jBBGw\n\nFoAUu5aH0mWR4cFoN9i7k96d2op3sPwwDQYJKoZIhvcNAQELBQADggEBAI5ai+Zi\n\nnFQZUXRTqJCgHsgBTHArneVWQYkYpyAXmTR7QeLfld4ZHL33i4xWCqX3uvW7SFJLe\n\nnZajT2AVmgiDbaWIHtDtvqz1BY78PSgUwPH/IyARTEOBeikp6KdwMPraehDIBMAcc\n\nnANY58wXiTBbsl8UMD6tGecgnzw6sxlMmadGvrfJeJmgY4zert6NNvgtTPhcZQdLS\n\nnE0fGzHS6+3ajCCfEEhPNPeR9D0e5Me81i9EsQGENrnJzTci8rzXPuF4bC3ggHrKl\n\nnI1+kmJQ1kLYVUcsntcrIiHmNvtPFJY6stjDgQKS9aDd/THhPpokPtZoCmE6PDxh6\n\nnR+dO6C0hcDKHFzA=\n-----END CERTIFICATE-----\n"
}
```

```
----
```

```
=== Generate a new Certificate Signing Request (CSR)
```

```
----
```

```
# The API:
```

```
/api/security/certificate-signing-request
```

```
# The call:
```

```
curl -X POST "https://<mgmt-ip>/api/security/certificate-signing-request"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\"algorithm\": \"rsa\", \"extended_key_usage\": [\"serverauth\"],
\"hash_function\": \"sha256\", \"key_usage\": [\"digitalsignature\"],
\"security_strength\": \"112\", \"subject_alternatives\": { \"dns\": [
\"*.example.com\", \"*.example1.com\" ], \"email\": [\"abc@example.com\",
\"abc@example1.com\"], \"ip\": [\"10.225.34.223\", \"10.225.34.224\"],
\"uri\": [\"http://example.com\", \"http://example1.com\"] },
\"subject_name\": \"C=US,O=NTAP,CN=test.domain.com\"}"
```

```
{
  "csr": "-----BEGIN CERTIFICATE REQUEST-----\n-----END CERTIFICATE
REQUEST-----\n",
  "generated_private_key": "-----BEGIN PRIVATE KEY-----\n-----END PRIVATE
KEY-----\n"
}
```

'''

```
[[ID2031ea76efe34556aa4dfab311ee2e01]]
```

= Retrieve security certificates

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/certificates`#
```

Introduced In: 9.6

Retrieves security certificates.

== Related ONTAP commands

* `security certificate show`

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|private_key
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by private_key
```

* Introduced in: 9.8

```
|uuid
|string
|query
|False
a|Filter by uuid
```

* Introduced in: 9.8

```
|type
|string
|query
|False
a|Filter by type
```

```
|subject_key_identifier
|string
|query
|False
a|Filter by subject_key_identifier
```

* Introduced in: 9.8

```
|public_certificate
|string
|query
|False
a|Filter by public_certificate
```

* Introduced in: 9.8

```
|ca
|string
|query
|False
a|Filter by ca
```

```
* maxLength: 256
* minLength: 1
```

```
|common_name
```

```
|string
|query
|False
a|Filter by common_name

|authority_key_identifier
|string
|query
|False
a|Filter by authority_key_identifier
```

* Introduced in: 9.8

```
|serial_number
|string
|query
|False
a|Filter by serial_number
```

* maxLength: 40
* minLength: 1

```
|key_size
|integer
|query
|False
a|Filter by key_size
```

```
|intermediate_certificates
|string
|query
|False
a|Filter by intermediate_certificates
```

* Introduced in: 9.8

```
|hash_function
|string
|query
|False
a|Filter by hash_function
```

```
|name  
|string  
|query  
|False  
a|Filter by name
```

* Introduced in: 9.8

```
|expiry_time  
|string  
|query  
|False  
a|Filter by expiry_time
```

```
|scope  
|string  
|query  
|False  
a|Filter by scope
```

```
|svm.uuid  
|string  
|query  
|False  
a|Filter by svm.uuid
```

```
|svm.name  
|string  
|query  
|False  
a|Filter by svm.name
```

```
|fields  
|array[string]  
|query  
|False  
a|Specify the fields to return.
```

```
|max_records  
|integer
```



```

|query
|False
a|Limit the number of records returned.

|return_timeout
|integer
|query
|False
a|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

|return_records
|boolean
|query
|False
a|The default is true for GET calls.  When set to false, only the number
of records is returned.

* Default value: 1

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

```

== Response

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#security_certificate[security_certificate]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "authority_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D7",
    "ca": "string",
    "common_name": "test.domain.com",
    "hash_function": "sha1",
    "intermediate_certificates": {
    },
    "name": "cert1",
    "private_key": "-----BEGIN PRIVATE KEY-----

```

```

MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAKEAu1/a8f3G47cZ6pel
Hd3aONMNkGJ8vSCH5QjicuDm92VtVwkAAACEjIoZSLYlJvPD+odL+lFzVQSmkneW7
VCGqYQIDAQABAKAcfNpg6GCQxoneLOghv1UrRotNZGvqpUOEAvHK3X7AJhz5SU4V
an36qvsAt5ghFMVM2iGvGaXbj0dAd+Jg64pxAiEA32Eh9mPtFSmZhTIUMeGcPmPk
qIYCEuP8a/ZLmI9s4TsCIQDWvLQuvjSVfwPhi0TFAb5wqAET8X5LBFqtGX5QlUep
EwIgFnqM02Gc4wtLoqa2d4qPkYu13+uUW9hLd4XSd6i/OS8CIQDT3elU+Rt+qIwW
u0cFrVvNYSV3HNzDfS9N/IoxTagfewIgPvXADe5c2EWbhCUkhN+ZCf38AKewK9TW
lQcDy4L+f14= -----END PRIVATE KEY-----",
    "public_certificate": "-----BEGIN CERTIFICATE-----
MIIBuzCCAWWgAwIBAgIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQAwhDENMASGA1UE
AxMEVEVTVDELMAkGA1UEBhMCVVMwHhcNMTgwNjA4MTgwOTAxWhcNMTkwNjA4MTgw
OTAxWjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDaPvbqUJJFJ6NNTyK3Yb+ytSjJ9aa3yUmYTD9uMiP+6ycjxHWB
e8u9z6yCHsW03ync+dnhE5c5z8wuDAY0fv15AgMBAAGjgYowgYcwDAYDVR0TBAUw
AwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFMJ7Ev/o/3+YNzYh5XNlqqjnw4zm
MEsGA1UdIwREMEKAFMJ7Ev/o/3+YNzYh5XNlqqjnw4zmoSCkHjAcMQ0wCwYDVQQD
EwRURVNUMQswCQYDVQQGEwJVU4IIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQADQQAv
DovYeyGNknjGI+TVNX6nDbyzf7zUPqnri0KuvObEeybrbPW45sgsnT5dyeE/32U
9Yr6lklkltBtVBDTmLnrc -----END CERTIFICATE-----",
    "scope": "svm",
    "serial_number": "string",
    "subject_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D8",
    "svm": {
        "_links": {
            "self": {
                "href": "/api/resourcelink"
            }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "type": "client",
    "uuid": "string"
}
}
===

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string

```

```

a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#security_certificate]
[.api-collapsible-fifth-title]
security_certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|authority_key_identifier
|string
a|Provides the key identifier of the issuing CA certificate that signed
the SSL certificate.

|ca
|string
a|Certificate authority

```

|common_name
|string
a|FQDN or custom common name. Provide on POST when creating a self-signed certificate.

|expiry_time
|string
a|Certificate expiration time. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.

|hash_function
|string
a|Hashing function. Can be provided on POST when creating a self-signed certificate. Hash functions md5 and sha1 are not allowed on POST.

|intermediate_certificates
|array[string]
a|Chain of intermediate Certificates in PEM format. Only valid in POST when installing a certificate.

|key_size
|integer
a|Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate. Key size of 512 is not allowed on POST.

|name
|string
a|Certificate name. If not provided in POST, a unique name specific to the SVM is automatically generated.

|private_key
|string
a|Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.

|public_certificate
|string

a|Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|serial_number

|string

a|Serial number of certificate.

|subject_key_identifier

|string

a|Provides the key identifier used to identify the public key in the SSL certificate.

|svm

|link:#svm[svm]

a|

|type

|string

a|Type of Certificate. The following types are supported:

* client - a certificate and its private key used by an SSL client in ONTAP.

* server - a certificate and its private key used by an SSL server in ONTAP.

* client_ca - a Certificate Authority certificate used by an SSL server in ONTAP to verify an SSL client certificate.

* server_ca - a Certificate Authority certificate used by an SSL client in ONTAP to verify an SSL server certificate.

* root_ca - a self-signed certificate used by ONTAP to sign other certificates by acting as a Certificate Authority.

* enum: ["client", "server", "client_ca", "server_ca", "root_ca"]

* Introduced in: 9.6

|uuid

|string

a|Unique ID that identifies a certificate.

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

|===

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID45423eeeb0ed24540766ea90fe839981]]
= Create or install security certificates

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/certificates`#

*Introduced In:* 9.6

Creates or installs a certificate.

== Required properties

* `svm.uuid` or `svm.name` - Existing SVM in which to create or install
the certificate.
* `common_name` - Common name of the certificate. Required when creating a
certificate.
* `type` - Type of certificate.
* `public_certificate` - Public key certificate in PEM format. Required
when installing a certificate.
* `private_key` - Private key certificate in PEM format. Required when
installing a CA-signed certificate.

== Recommended optional properties

* `expiry_time` - Certificate expiration time. Specifying an expiration
time is recommended when creating a certificate.
* `key_size` - Key size of the certificate in bits. Specifying a strong
key size is recommended when creating a certificate.
* `name` - Unique certificate name per SVM. If one is not provided, it is

```

automatically generated.

== Default property values

If not specified in POST, the following default property values are assigned:

```
* `key_size` - _2048_  
* `expiry_time` - _P365DT_  
* `hash_function` - _sha256_
```

== Related ONTAP commands

```
* `security certificate create`  
* `security certificate install`
```

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|return_records  
|boolean  
|query  
|False
```

a|The default is false. If set to true, the records are returned.

* Default value:

```
|===
```

== Request Body

```
[cols=3*,options=header]  
|===  
|Name  
|Type  
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|authority_key_identifier
|string
a|Provides the key identifier of the issuing CA certificate that signed
the SSL certificate.
```

```
|ca
|string
a|Certificate authority
```

```
|common_name
|string
a|FQDN or custom common name. Provide on POST when creating a self-signed
certificate.
```

```
|expiry_time
|string
a|Certificate expiration time. Can be provided on POST if creating self-
signed certificate. The expiration time range is between 1 day to 10
years.
```

```
|hash_function
|string
a|Hashing function. Can be provided on POST when creating a self-signed
certificate. Hash functions md5 and sha1 are not allowed on POST.
```

```
|intermediate_certificates
|array[string]
a|Chain of intermediate Certificates in PEM format. Only valid in POST
when installing a certificate.
```

```
|key_size
|integer
a|Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048,
3072. Can be provided on POST if creating self-signed certificate. Key
size of 512 is not allowed on POST.
```

```

|name
|string
a|Certificate name. If not provided in POST, a unique name specific to the
SVM is automatically generated.

|private_key
|string
a|Private key Certificate in PEM format. Only valid for create when
installing a CA-signed certificate. This is not audited.

|public_certificate
|string
a|Public key Certificate in PEM format. If this is not provided in POST, a
self-signed certificate is created.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|serial_number
|string
a|Serial number of certificate.

|subject_key_identifier
|string
a|Provides the key identifier used to identify the public key in the SSL
certificate.

|svm
|link:#svm[svm]
a|

|type
|string
a|Type of Certificate. The following types are supported:

* client - a certificate and its private key used by an SSL client in
ONTAP.
* server - a certificate and its private key used by an SSL server in

```

ONTAP.

- * client_ca - a Certificate Authority certificate used by an SSL server in ONTAP to verify an SSL client certificate.
- * server_ca - a Certificate Authority certificate used by an SSL client in ONTAP to verify an SSL server certificate.
- * root_ca - a self-signed certificate used by ONTAP to sign other certificates by acting as a Certificate Authority.
- * enum: ["client", "server", "client_ca", "server_ca", "root_ca"]
- * Introduced in: 9.6

|uuid
|string
a|Unique ID that identifies a certificate.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "authority_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D7",
  "ca": "string",
  "common_name": "test.domain.com",
  "hash_function": "sha1",
  "intermediate_certificates": {
  },
  "name": "cert1",
  "private_key": "-----BEGIN PRIVATE KEY-----
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAu1/a8f3G47cZ6pel
Hd3aONMNkGJ8vSCH5QjicuDm92VtVwkAAACEjIoZSLYlJvPD+odL+lFzVQSmkneW7
VCGqYQIDAQABAkAcfNpg6GCQxoneLOghv1UrRotNZGvqpUOEAvHK3X7AJhz5SU4V
an36qvsAt5ghFMVM2iGvGaXbj0dAd+Jg64pxAiEA32Eh9mPtFSmZhTIUMeGcPmPk
qIYCEuP8a/ZLmI9s4TsCIQDWvLQuvjSVfwPhi0TFAb5wqAET8X5LBFqtGX5QlUep
EwIgFnqM02Gc4wtLoqa2d4qPkYu13+uUW9hLd4XSd6i/OS8CIQDT3elU+Rt+qIwW
u0cFrVvNYSV3HNzDfS9N/IoxTagfewIgpVxADe5c2EWbhCUkhN+ZCf38AKewK9TW
lQcDy4L+f14= -----END PRIVATE KEY-----",
}
```

```

"public_certificate": "-----BEGIN CERTIFICATE-----
MIIBuzCCAWWgAwIBAgIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQAwhDENMAsgA1UE
AxMEVEVETVDELMAkGA1UEBhMCVVMwHhcNMTgwNjA4MTgwOTAxWhcNMTkwNjA4MTgw
OTAxWjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDaPvbqUJJFJ6NNTyK3Yb+ytSjJ9aa3yUmYTD9uMiP+6ycjxHWB
e8u9z6yCHsW03ync+dnhE5c5z8wuDAY0fv15AgMBAAGjgYowgYcwDAYDVR0TBAUw
AwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFMJ7Ev/o/3+YNzYh5XNlqqjnw4zm
MEsGA1UdIwREMEKAQFMJ7Ev/o/3+YNzYh5XNlqqjnw4zmoSCkhjAcMQ0wCwYDVQQD
EwRURVNUMQswCQYDVQQGEwJVU4IIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQADQQA
vDovYeyGNknkjGI+TVNX6nDbyzf7zUPqnri0KuvObEeybrbPW45sgsnT5dyeE/32U
9Yr6lklnkBTvBDTmLnrc -----END CERTIFICATE-----",
"scope": "svm",
"serial_number": "string",
"subject_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D8",
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"type": "client",
"uuid": "string"
}
=====

```

== Response

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer

```

```
a|Number of records
```

```
|records
```

```
|array[link:#security_certificate[security_certificate]]
```

```
a|
```

```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    },
    "authority_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D7",
    "ca": "string",
    "common_name": "test.domain.com",
    "hash_function": "sha1",
    "intermediate_certificates": {
    },
    "name": "cert1",
    "private_key": "-----BEGIN PRIVATE KEY-----
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAu1/a8f3G47cZ6pel
Hd3aONMNkGJ8vSCH5QjicuDm92VtVwKAACEjIoZSLYlJvPD+odL+lFzVQSmkneW7
VCGqYQIDAQABAKAcfNpg6GCQxoneLOghv1UrRotNZGvqpUOEAvHK3X7AJhz5SU4V
an36qvsAt5ghFMVM2iGvGaXbj0dAd+Jg64pxAiEA32Eh9mPtFSmZhTIUMeGcPmPk
qIYCEuP8a/ZLmI9s4TsCIQDWvLQuvjSVfwPhi0TFAb5wqAET8X5LBFqtGX5QlUep
EwIgFnqM02Gc4wtLoqa2d4qPkYu13+uUW9hLd4XSd6i/OS8CIQDT3elU+Rt+qIwW
u0cFrVvNYSV3HNzDfS9N/IoxTagfewIgPvXADe5c2EWbhCUkhN+ZCf38AKewK9TW
lQcDy4L+f14= -----END PRIVATE KEY-----",
```



```

"public_certificate": "-----BEGIN CERTIFICATE-----
MIIBuzCCAWWgAwIBAgIIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQAwhDENMASGA1UE
AxMEVEVTVDELMAkGA1UEBhMCVVMwHhcNMTgwNjA4MTgwOTAxWhcNMTkwNjA4MTgw
OTAxWjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDaPvbqUJJFJ6NNTyK3Yb+ytSjJ9aa3yUmYTD9uMiP+6ycjxHWB
e8u9z6yCHsW03ync+dnhE5c5z8wuDAY0fv15AgMBAAGjgYowgYcwDAYDVR0TBAUw
AwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFMJ7Ev/o/3+YNzYh5XNlqqjnw4zm
MEsGA1UdIwREMEKAQFMJ7Ev/o/3+YNzYh5XNlqqjnw4zmoSCkHjAcMQ0wCwYDVQQD
EwRURVNUMQswCQYDVQQGEwJVU4IIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQADQQA
vDovYeyGNnknjGI+TVNX6nDbyzf7zUPqnri0KuvObEeybrbPW45sgsnT5dyeE/32U
9Yr6lklnkBTvBDTmLnrc -----END CERTIFICATE-----",
  "scope": "svm",
  "serial_number": "string",
  "subject_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D8",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "client",
  "uuid": "string"
}
}
=====

```

== Error

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 3735645
| Cannot specify a value for serial. It is generated automatically.
| 3735622
| The certificate type is not supported.

```

| 3735664
| The specified key size is not supported in FIPS mode.

| 3735665
| The specified hash function is not supported in FIPS mode.

| 3735553
| Failed to create self-signed Certificate.

| 3735646
| Failed to store the certificates.

| 3735693
| The certificate installation failed as private key was empty.

| 3735618
| Cannot accept private key for server_ca or client_ca.

| 52363365
| Failed to allocate memory.

| 52559975
| Failed to read the certificate due to incorrect formatting.

| 52363366
| Unsupported key type.

| 52560123
| Failed to read the key due to incorrect formatting.

| 52559972
| The certificates start date is later than the current date.

| 52559976
| The certificate and private key do not match.

| 52559973
| The certificate has expired.

| 52363366
| Logic error: use of a dead object.

| 3735696
| Intermediate certificates are not supported with client_ca and server_ca type certificates.

| 52559974

```

| The certificate is not supported in FIPS mode.

| 3735676
| Cannot continue the installation without a value for the common name.
Since the subject field in the certificate is empty, the field
"common_name" must have a value to continue with the installation.

| 3735558
| Failed to extract information about Common Name from the certificate.

| 3735588
| The common name (CN) extracted from the certificate is not valid.

| 3735632
| Failed to extract Certificate Authority Information from the
certificate.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

```

}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#security_certificate]
[.api-collapsible-fifth-title]
security_certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|authority_key_identifier
|string
a|Provides the key identifier of the issuing CA certificate that signed
the SSL certificate.

|ca
|string
a|Certificate authority

```

|common_name
|string
a|FQDN or custom common name. Provide on POST when creating a self-signed certificate.

|expiry_time
|string
a|Certificate expiration time. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.

|hash_function
|string
a|Hashing function. Can be provided on POST when creating a self-signed certificate. Hash functions md5 and sha1 are not allowed on POST.

|intermediate_certificates
|array[string]
a|Chain of intermediate Certificates in PEM format. Only valid in POST when installing a certificate.

|key_size
|integer
a|Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate. Key size of 512 is not allowed on POST.

|name
|string
a|Certificate name. If not provided in POST, a unique name specific to the SVM is automatically generated.

|private_key
|string
a|Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.

|public_certificate

```

|string
a|Public key Certificate in PEM format. If this is not provided in POST, a
self-signed certificate is created.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|serial_number
|string
a|Serial number of certificate.

|subject_key_identifier
|string
a|Provides the key identifier used to identify the public key in the SSL
certificate.

|svm
|link:#svm[svm]
a|

|type
|string
a|Type of Certificate. The following types are supported:

* client - a certificate and its private key used by an SSL client in
ONTAP.
* server - a certificate and its private key used by an SSL server in
ONTAP.
* client_ca - a Certificate Authority certificate used by an SSL server in
ONTAP to verify an SSL client certificate.
* server_ca - a Certificate Authority certificate used by an SSL client in
ONTAP to verify an SSL server certificate.
* root_ca - a self-signed certificate used by ONTAP to sign other
certificates by acting as a Certificate Authority.
* enum: ["client", "server", "client_ca", "server_ca", "root_ca"]
* Introduced in: 9.6

|uuid
|string
a|Unique ID that identifies a certificate.

```

```

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

```



```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID74e33e0960e6cba487d683b837c5f751]]
= Sign security certificates

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/certificates/{ca.uuid}/sign`#

*Introduced In:* 9.6

```

Signs a certificate.

== Required properties

* ``signing_request`` - Certificate signing request to be signed by the given certificate authority.

== Recommended optional properties

* ``expiry_time`` - Certificate expiration time. Specifying an expiration time for a signed certificate is recommended.

* ``hash_function`` - Hashing function. Specifying a strong hashing function is recommended when signing a certificate.

== Default property values

If not specified in POST, the following default property values are assigned:

* ``expiry_time`` - `_P365DT_`

* ``hash_function`` - `_sha256_`

== Related ONTAP commands

* ``security certificate sign``

This API is used to sign a certificate request using a pre-existing self-signed root certificate. The self-signed root certificate acts as a certificate authority within its scope and maintains the records of its signed certificates.

The root certificate can be created for a given SVM or for the cluster using [``POST security/certificates``].

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|ca.uuid

```

|string
|path
|True
a|UUID of the existing certificate authority certificate


|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.


* Default value:


|===


== Request Body


[cols=3*,options=header]
|===
|Name
|Type
|Description

|expiry_time
|string
a|Certificate expiration time. The allowed expiration time range is
between 1 day to 10 years.


|hash_function
|string
a|Hashing function


|signing_request
|string
a|Certificate signing request to be signed by the given certificate
authority. Request should be in X509 PEM format.


|===


.Example request

```

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "hash_function": "sha256",
  "signing_request": "'-----BEGIN CERTIFICATE REQUEST-----
MIICYDCCAUGCAQAwGzEMMAoGA1UEAxMDQUJDMQswCQYDVQQGEwJVUzCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAPF+82SlqT3Vyu3Jx4IAwHcO5EGwLOxy
zQ6KNjz71Fca0n1/A1CbCPyOsSupGVObvdWxX7xLVMJ2SXb7h43GCqYyX6FXJO4F
HOPmLvB+jxdeiW7SDBiZyLUlsvA+oRO/uNlcug773QZdKLjJD64erZZMRUNbUJB8
bARxAUi0FPvgTraSQ0UW5sRLiGKeAyKA4wekYe1VgjHRTBizFbD4dI3njfva/2Bl
jfk+kkulgcLJTUJNtkgeimqMKyraYuleYcYk2K+C//0NuNOuPbDfTXCM7O61vik09
Szi8nLN7OXE9KoAA93U/BCpSfpl8XIb4cGnEr8hgVHOotZSo+KZBFxMCAwEAAaAA
MA0GCSqGSIB3DQEBChUAA4IBAQC2vFYpvgsFrm5GnPx8tOBD1xsTyYjbWJMD8hAF
lFrvF9Sw9QGCTdyacxkwgJhQx8l8JiIS5GOY6WWLB19FMkLQNAhDL9xF3WF7vfYq
RKgrz3bd/Vg96fsRZNYIPLGmoEaqLOh3FOCGc2VbdsR9PwOn3fwthxkIRd6ds6/q
jc5cpSmVsCOgu+OKcpRXikYDbkWXfTZ1AhSfn6njBYFdZ9+PNAu/0JRQh5bX60nO
5heniTcAJLwUZP/CQ8nxHY0Wqy+1rAtM33d5cVmHulBXQSIru/0ZkA/b9fK5Zv8E
ZMADYUoEvIG59VxhyCi8lzYf+Mxl8qBSF+ZdC4yWhzDqZtM9 -----END CERTIFICATE
REQUEST-----'"
}
====

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|public_certificate
|string
a|CA signed public key Certificate

|===

== Error
```

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 3735628

| Failed to use CA certificate for signing.

| 3735665

| The specified hash function is not supported in FIPS mode.

| 52559974

| The certificate is not supported in FIPS mode.

| 3735626

| Failed to generate signed Certificate.

| 3735558

| Failed to extract information about Common Name from the certificate.

| 3735588

| The common name (CN) extracted from the certificate is not valid.

| 3735632

| Failed to extract Certificate Authority Information from the certificate.

| 3735629

| Failed to sign the certificate because Common Name of signing certificate and Common Name of CA certificate are same.

| 3735630

| Failed to sign the certificate because expiry date of signing certificate exceeds the expiry date of CA certificate.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

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

```
=====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
=====
```

```
[#security_certificate_sign]
```

```
[.api-collapsible-fifth-title]
```

```
security_certificate_sign
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|expiry_time
```

```
|string
```

```
a|Certificate expiration time. The allowed expiration time range is  
between 1 day to 10 years.
```

```
|hash_function
```

```
|string
```

a|Hashing function

|signing_request

|string

a|Certificate signing request to be signed by the given certificate authority. Request should be in X509 PEM format.

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
[[IDcad5fc18f591f56e9fd8529bf1e1c5d5]]
```

```
= Delete security certificates
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-  
block]#`/security/certificates/{uuid}`#
```

```
*Introduced In:* 9.6
```

```
Deletes a security certificate.
```

```
== Related ONTAP commands
```

```
* `security certificate delete`
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```



```

|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|Certificate UUID

|===

== Response

```

Status: 200, Ok

```

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description

| 3735644
| Cannot delete server-chain certificate. Reason: There is a corresponding
server certificate for it.

| 3735679
| Cannot delete pre-installed server_ca certificates through REST. Use CLI
or ZAPI.

| 3735650
| Deleting this client_ca certificate directly is not supported. Delete
the corresponding root-ca certificate using type `root_ca` to delete the
root, client, and server certificates.

| 3735627
| Deleting this server_ca certificate directly is not supported. Delete
the corresponding root-ca certificate using type `root_ca` to delete the
root, client, and server certificates.

| 3735589

```

```
| Cannot delete certificate.

| 3735590
| Cannot delete certificate. Failed to remove SSL configuration for the
certificate.

| 3735683
| Cannot remove this certificate while external key manager is configured.
|===
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|

|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====
```

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
```

```

//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string

```

a|Error message

|target

|string

a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

====

[[ID363ef035bcd6ed6a8eda92ec960c49c]]

= Retrieve security certificates

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/certificates/{uuid}`#

Introduced In: 9.6

Retrieves security certificates.

== Related ONTAP commands

* `security certificate show`

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

|True

a|Certificate UUID

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|authority_key_identifier
|string
a|Provides the key identifier of the issuing CA certificate that signed
the SSL certificate.

|ca
|string
a|Certificate authority

|common_name
|string
a|FQDN or custom common name. Provide on POST when creating a self-signed
certificate.

|expiry_time
|string
a|Certificate expiration time. Can be provided on POST if creating self-
signed certificate. The expiration time range is between 1 day to 10
years.
```

|hash_function

|string

a|Hashing function. Can be provided on POST when creating a self-signed certificate. Hash functions md5 and sha1 are not allowed on POST.

|intermediate_certificates

|array[string]

a|Chain of intermediate Certificates in PEM format. Only valid in POST when installing a certificate.

|key_size

|integer

a|Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate. Key size of 512 is not allowed on POST.

|name

|string

a|Certificate name. If not provided in POST, a unique name specific to the SVM is automatically generated.

|private_key

|string

a|Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.

|public_certificate

|string

a|Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|serial_number

|string

a|Serial number of certificate.

|subject_key_identifier

|string

a|Provides the key identifier used to identify the public key in the SSL certificate.

|svm

|link:#svm[svm]

a|

|type

|string

a|Type of Certificate. The following types are supported:

* client - a certificate and its private key used by an SSL client in ONTAP.

* server - a certificate and its private key used by an SSL server in ONTAP.

* client_ca - a Certificate Authority certificate used by an SSL server in ONTAP to verify an SSL client certificate.

* server_ca - a Certificate Authority certificate used by an SSL client in ONTAP to verify an SSL server certificate.

* root_ca - a self-signed certificate used by ONTAP to sign other certificates by acting as a Certificate Authority.

* enum: ["client", "server", "client_ca", "server_ca", "root_ca"]

* Introduced in: 9.6

|uuid

|string

a|Unique ID that identifies a certificate.

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
```

```

    },
    "authority_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D7",
    "ca": "string",
    "common_name": "test.domain.com",
    "hash_function": "sha1",
    "intermediate_certificates": {
    },
    "name": "cert1",
    "private_key": "-----BEGIN PRIVATE KEY-----
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAu1/a8f3G47cZ6pel
Hd3aONMNkGJ8vSCH5QjicuDm92VtVwkAAACEjIoZSLYlJvPD+odL+lFzVQSmkneW7
VCGqYQIDAQABAKAcfNpg6GCQxoneLOghv1UrRotNZGvqpUOEAvHK3X7AJhz5SU4V
an36qvsAt5ghFMVM2iGvGaXbj0dAd+Jg64pxAiEA32Eh9mPtFSmZhTIUMeGcPmPk
qIYCEuP8a/ZLmI9s4TsCIQDWvLQuvjSVfwPhi0TFab5wqAET8X5LBFqtGX5QlUep
EwIgFnqM02Gc4wtLoqa2d4qPkYu13+uUW9hLd4XSd6i/OS8CIQDT3elU+Rt+qIwW
u0cFrVvNYSV3HNzDfS9N/IoxTagfewIgpVxADe5c2EWbhCUkhN+ZCf38AKewK9TW
lQcDy4L+f14= -----END PRIVATE KEY-----",
    "public_certificate": "-----BEGIN CERTIFICATE-----
MIIBuzCCAWWgAwIBAgIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQAwhDENMASGA1UE
AxMEVEVTVDELMAkGA1UEBhMCVVMwHhcNMTgwNjA4MTgwOTAxWhcNMTkwNjA4MTgw
OTAxWjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDaPvbqUJJFJ6NNTyK3Yb+ytSjJ9aa3yUmYTD9uMiP+6ycjxHWB
e8u9z6yCHsW03ync+dnhE5c5z8wuDAY0fv15AgMBAAGjgYowgYcwDAYDVR0TBAUw
AwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFMJ7Ev/o/3+YNzYh5XNlqqjnw4zm
MEsGA1UdIwREMEKAFMJ7Ev/o/3+YNzYh5XNlqqjnw4zmoSCkhjAcMQ0wCwYDVQQD
EwRURVNUMQswCQYDVQQGEwJVU4IIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQADQQA
vDovYeyGNnknjGI+TVNX6nDbyzf7zUPqnri0KuvObEeybrbPW45sgsnT5dyeE/32U
9Yr6lklkBtVBDBTmLnrc -----END CERTIFICATE-----",
    "scope": "svm",
    "serial_number": "string",
    "subject_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D8",
    "svm": {
        "_links": {
            "self": {
                "href": "/api/resourcelink"
            }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "type": "client",
    "uuid": "string"
}

```



```
====
```

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```
    "arguments": {
```

```
      "code": "string",
```

```
      "message": "string"
```

```
    },
```

```
    "code": "4",
```

```
    "message": "entry doesn't exist",
```

```
    "target": "uuid"
```

```
  }
```

```
}
```

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
====
```

```
[#href]
```

```
[.api-collapsible-fifth-title]
```

```
href
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string

```

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

```

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
:leveloffset: -1
```

```
= Manage Google Cloud KMS
```

```
:leveloffset: +1
```

```
[[ID71fb42244bad8e39bb27de4ad2722ea1]]
= Security gcp-kms endpoint overview
```

```
== Overview
```

Google Cloud Key Management Services is a cloud key management service (KMS) that provides a secure store for encryption keys. This feature allows ONTAP to securely store its encryption keys using Google Cloud KMS. In order to use Google Cloud KMS with ONTAP, a user must first deploy a Google Cloud application with appropriate access to the Google Cloud KMS and then provide ONTAP with the necessary details, such as, project ID, key ring name,

location, key name and application credentials to allow ONTAP to communicate with the deployed Google Cloud application. The properties ``state``, ``google_reachability`` and ``ekmip_reachability`` are considered advanced properties and are populated only when explicitly requested.

== Examples

=== Enabling GCKMS for an SVM

The following example shows how to enable GCKMS at the SVM-scope. Note the `_return_records=true_` query parameter is used to obtain the newly created key manager configuration.

The API:

POST /api/security/gcp-kms

The call:

```
curl -X POST 'https://<mgmt-ip>/api/security/gcp-kms?return_records=true'
-H 'accept: application/hal+json' -d '{"svm":{"uuid":"f36ff553-e713-11ea-
bd56-005056bb4222" }, "project_id": "testProj",
"key_ring_name":"testKeyRing", "key_ring_location": "global", "key_name":
"key1", "application_credentials": "myAppCred"}'
```

The response:

```
{
  "num_records": 1,
  "records": [
    {
      "uuid": "f72098a2-e908-11ea-bd56-005056bb4222",
      "svm": {
        "uuid": "f36ff553-e713-11ea-bd56-005056bb4222",
        "name": "vs0"
      },
      "project_id": "testProj",
      "key_ring_name": "testKeyRing",
      "key_ring_location": "global",
      "key_name": "key1",
      "_links": {
        "self": {
          "href": "/api/security/gcp-kms/f72098a2-e908-11ea-bd56-
005056bb4222"
        }
      }
    }
  ]
}
```

```

    }
  }
]
}
----

'''

=== Retrieving all GCKMS configurations

The following example shows how to retrieve all GCKMS configurations.

----

# The API:
GET /api/security/gcp-kms

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/gcp-kms?fields=*'

# The response:
{
  "records": [
    {
      "uuid": "f72098a2-e908-11ea-bd56-005056bb4222",
      "scope": "svm",
      "svm": {
        "uuid": "f36ff553-e713-11ea-bd56-005056bb4222",
        "name": "vs0"
      },
      "project_id": "testProj",
      "key_ring_name": "testKeyRing",
      "key_ring_location": "global",
      "key_name": "key1",
      "_links": {
        "self": {
          "href": "/api/security/gcp-kms/f72098a2-e908-11ea-bd56-005056bb4222"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/gcp-kms?fields=*"
    }
  }
}

```

```

    }
}
}
----

'''

=== Retrieving a specific GCKMS configuration

The following example shows how to retrieve information for a specific
GCKMS configuration.

----

# The API:
GET /api/security/gcp-kms/{uuid}

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/gcp-kms/f72098a2-e908-11ea-
bd56-005056bb4222?fields=*'

# The response:
{
  "uuid": "f72098a2-e908-11ea-bd56-005056bb4222",
  "scope": "svm",
  "svm": {
    "uuid": "f36ff553-e713-11ea-bd56-005056bb4222",
    "name": "vs0"
  },
  "project_id": "testProj",
  "key_ring_name": "testKeyRing",
  "key_ring_location": "global",
  "key_name": "key1",
  "_links": {
    "self": {
      "href": "/api/security/gcp-kms/f72098a2-e908-11ea-bd56-005056bb4222"
    }
  }
}
}
----

'''

=== Retrieving a specific GCKMS's advanced properties

The following example shows how to retrieve advanced properties for a
specific GCKMS configuration.

```

The API:

GET /api/security/gcp-kms/{uuid}

The call:

curl -X GET 'https://<mgmt-ip>/api/security/gcp-kms/f72098a2-e908-11ea-bd56-005056bb4222?fields=state,google_reachability,ekmip_reachability'

The response:

```
{
  "uuid": "f72098a2-e908-11ea-bd56-005056bb4222",
  "state": {
    "cluster_state": false,
    "message": "The Google Cloud Key Management Service key protection is
    unavailable on the following nodes: cluster1-node1.",
    "code": 65537708
  },
  "google_reachability": {
    "reachable": true,
    "message": "",
    "code": 0
  },
  "ekmip_reachability": [
    {
      "node": {
        "uuid": "d208115f-7721-11eb-bf83-005056bb150e",
        "name": "node1",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/d208115f-7721-11eb-bf83-
005056bb150e"
          }
        }
      },
      "reachable": true,
      "message": "",
      "code": 0
    },
    {
      "node": {
        "uuid": "e208115f-7721-11eb-bf83-005056bb150e",
        "name": "node2",
        "_links": {
          "self": {
```



```

        "href": "/api/cluster/nodes/e208115f-7721-11eb-bf83-
005056bb150e"
      }
    }
  },
  "reachable": true,
  "message": "",
  "code": 0
}
],
"_links": {
  "self": {
    "href": "/api/security/gcp-kms/f72098a2-e908-11ea-bd56-005056bb4222"
  }
}
}
----
'''

```

=== Updating the application credentials of a specific GCKMS configuration

The following example shows how to update the application credentials for a specific GCKMS configuration.

```

----

# The API:
PATCH /api/security/gcp-kms/{uuid}

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/gcp-kms/f72098a2-e908-11ea-
bd56-005056bb4222/' -d '{"application_credentials": "newAppCred"}'
----
'''

```

=== Deleting a specific GCKMS configuration

The following example shows how to delete a specific GCKMS configuration.

```

----

# The API:
DELETE /api/security/gcp-kms/{uuid}

# The call:

```

```

curl -X DELETE 'https://<mgmt-ip>/api/security/gcp-kms/f72098a2-e908-11ea-
bd56-005056bb4222'
----

'''

=== Restoring keys from KMIP server

The following example shows how to restore keys for a GCKMS configuration.

----

# The API:
POST /api/security/gcp-kms/{uuid}/restore

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/gcp-kms/33820b57-ec90-11ea-
875e-005056bbf3f0/restore'
----

'''

[[ID112acc562a4f216aaaae64b17a378c5f]]
= Retrieve Google Cloud KMS configurations for all clusters and SVMs

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/gcp-kms`#

*Introduced In:* 9.9

Retrieves Google Cloud KMS configurations for all clusters and SVMs.

== Related ONTAP commands

* `security key-manager external gcp show`
* `security key-manager external gcp check`

== Parameters

[cols=5*,options=header]
|===

```

```
|Name
|Type
|In
|Required
|Description

|ekmip_reachability.message
|string
|query
|False
a|Filter by ekmip_reachability.message

|ekmip_reachability.code
|integer
|query
|False
a|Filter by ekmip_reachability.code

|ekmip_reachability.reachable
|boolean
|query
|False
a|Filter by ekmip_reachability.reachable

|ekmip_reachability.node.uuid
|string
|query
|False
a|Filter by ekmip_reachability.node.uuid

|ekmip_reachability.node.name
|string
|query
|False
a|Filter by ekmip_reachability.node.name

|key_ring_location
|string
|query
|False
a|Filter by key_ring_location
```

```
|proxy_host  
|string  
|query  
|False  
a|Filter by proxy_host
```

```
|key_ring_name  
|string  
|query  
|False  
a|Filter by key_ring_name
```

```
|proxy_username  
|string  
|query  
|False  
a|Filter by proxy_username
```

```
|uuid  
|string  
|query  
|False  
a|Filter by uuid
```

```
|proxy_type  
|string  
|query  
|False  
a|Filter by proxy_type
```

```
|key_name  
|string  
|query  
|False  
a|Filter by key_name
```

```
|google_reachability.message  
|string  
|query  
|False
```

```
a|Filter by google_reachability.message

|google_reachability.code
|integer
|query
|False
a|Filter by google_reachability.code

|google_reachability.reachable
|boolean
|query
|False
a|Filter by google_reachability.reachable

|state.message
|string
|query
|False
a|Filter by state.message

|state.code
|integer
|query
|False
a|Filter by state.code

|state.cluster_state
|boolean
|query
|False
a|Filter by state.cluster_state

|proxy_port
|integer
|query
|False
a|Filter by proxy_port

|project_id
|string
```

```
|query
|False
a|Filter by project_id
```

```
|svm.uuid
|string
|query
|False
a|Filter by svm.uuid
```

```
|svm.name
|string
|query
|False
a|Filter by svm.name
```

```
|scope
|string
|query
|False
a|Filter by scope
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_timeout
|integer
|query
|False
a|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

|return_records

|boolean

|query

|False

a|The default is true for GET calls. When set to false, only the number of records is returned.

* Default value: 1

|order_by

|array[string]

|query

|False

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|num_records

|integer

a|Number of records

|records

```
|array[link:#gcp_kms[gcp_kms]]
```

```
a|
```

```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "application_credentials": "{ type: service_account, project_id:
project-id, private_key_id: key-id, private_key: -----BEGIN PRIVATE
KEY-----\nprivate-key\n-----END PRIVATE KEY-----\n, client_email: service-
account-email, client_id: client-id, auth_uri:
https://accounts.google.com/o/oauth2/auth, token_uri:
https://accounts.google.com/o/oauth2/token, auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs, client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/service-account-email
}",
    "ekmip_reachability": {
      "code": 346758,
      "message": "embedded KMIP server status unavailable on node.",
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  }
}
```



```

    },
    "google_reachability": {
      "code": 346758,
      "message": "Google Cloud KMS service is not reachable from all nodes
- <reason>."
    },
    "key_name": "cryptokey1",
    "key_ring_location": "global",
    "key_ring_name": "gcpappl-keyring",
    "project_id": "gcpappl",
    "proxy_host": "proxy.eng.com",
    "proxy_password": "proxypassword",
    "proxy_port": 1234,
    "proxy_type": "http",
    "proxy_username": "proxyuser",
    "scope": "svm",
    "state": {
      "code": 346758,
      "message": "Top-level internal key protection key (KEK) is
unavailable on the following nodes with the associated reasons: Node:
node1. Reason: No volumes created yet for the SVM. Wrapped KEK status will
be available after creating encrypted volumes."
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  }
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

```
| 65537551
| Top-level internal key protection key (KEK) unavailable on one or more
nodes.

| 65537552
| Embedded KMIP server status not available.

| 65537730
| The Google Cloud Key Management Service is unreachable from one or more
nodes.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

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

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```

.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]

```

```

|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===

[#ekmip_reachability]
[.api-collapsible-fifth-title]
ekmip_reachability

```

Provides the connectivity status for the given SVM on the given node to all EKMIP servers configured on all nodes of the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|integer
```

a|Code corresponding to the error message. Returns a 0 if a given SVM is able to communicate to the EKMIP servers of all of the nodes in the cluster.

```
|message
```

```
|string
```

a|Error message set when cluster-wide EKMIP server availability from the given SVM and node is false.

```
|node
```

```
|link:#node[node]
```

```
a|
```

```
|reachable
```

```
|boolean
```

a|Set to true if the given SVM on the given node is able to communicate to all EKMIP servers configured on all nodes in the cluster.

```
|===
```

```
[#google_reachability]
```

```
[.api-collapsible-fifth-title]
```

google_reachability

Indicates whether or not the Google Cloud KMS service is reachable from all nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the error message. Returns a 0 if Google Cloud KMS
service is reachable from all nodes in the cluster.

|message
|string
a|Set to the error message when 'reachable' is false.

|reachable
|boolean
a|Set to true if the Google Cloud KMS service is reachable from all nodes
of the cluster.

|===

[#state]
[.api-collapsible-fifth-title]
state

Google Cloud Key Management Services is a cloud key management service
(KMS) that provides a secure store for encryption keys. This object
indicates whether or not the Google Cloud KMS key protection is available
on all nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_state
|boolean

```

a|Set to true when Google Cloud KMS key protection is available on all nodes of the cluster.

|code

|integer

a|Error code corresponding to the status message. Returns 0 if Google Cloud KMS key protection is available in all nodes of the cluster.

|message

|string

a|Error message set when top-level internal key protection key (KEK) availability on cluster is false.

|===

[#svm]

[.api-collapsible-fifth-title]

svm

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|name

|string

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#gcp_kms]

```
[.api-collapsible-fifth-title]
gcp_kms

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|application_credentials
|string
a|Google Cloud application's service account credentials required to
access the specified KMS. It is a JSON file containing an email address
and the private key of the service account holder.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|google_reachability
|link:#google_reachability[google_reachability]
a|Indicates whether or not the Google Cloud KMS service is reachable from
all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|key_name
|string
a|Key Identifier of Google Cloud KMS key encryption key.

|key_ring_location
|string
a|Google Cloud KMS key ring location.

|key_ring_name
|string
a|Google Cloud KMS key ring name of the deployed Google Cloud application.
```


|project_id
|string
a|Google Cloud project (application) ID of the deployed Google Cloud application that has appropriate access to the Google Cloud KMS.

|proxy_host
|string
a|Proxy host name.

|proxy_password
|string
a|Proxy password. Password is not audited.

|proxy_port
|integer
a|Proxy port number.

|proxy_type
|string
a|Type of proxy.

|proxy_username
|string
a|Proxy username.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|state
|link:#state[state]
a|Google Cloud Key Management Services is a cloud key management service (KMS) that provides a secure store for encryption keys. This object indicates whether or not the Google Cloud KMS key protection is available on all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an

instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|A unique identifier for the Google Cloud KMS.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
```

```

|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===

//end collapsible .Definitions block
=====

[[ID58de96f29e723c7998dd4cd4b1b08aa3]]
= Create a Google Cloud KMS configuration for an SVM

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/gcp-kms`#

*Introduced In:* 9.9

Configures the Google Cloud KMS configuration for the specified SVM.

== Required properties

* `svm.uuid` or `svm.name` - Existing SVM in which to create a Google
Cloud KMS.
* `project_id` - Google Cloud project (application) ID of the deployed
Google Cloud application with appropriate access to the Google Cloud KMS.
* `key_ring_name` - Google Cloud KMS key ring name of the deployed Google

```

Cloud application with appropriate access to the specified Google Cloud KMS.

- * ``key_ring_location`` - Google Cloud KMS key ring location.
- * ``key_name`` - Key Identifier of the Google Cloud KMS key encryption key.
- * ``application_credentials`` - Google Cloud application's service account credentials required to access the specified KMS. It is a JSON file containing an email address and the private key of the service account holder.

== Optional properties

- * ``proxy_type`` - Type of proxy (http/https) if proxy configuration is used.
- * ``proxy_host`` - Proxy hostname if proxy configuration is used.
- * ``proxy_port`` - Proxy port number if proxy configuration is used.
- * ``proxy_username`` - Proxy username if proxy configuration is used.
- * ``proxy_password`` - Proxy password if proxy configuration is used.

== Related ONTAP commands

- * ``security key-manager external gcp enable``

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

- * Default value:

|===

== Request Body

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|application_credentials
|string
a|Google Cloud application's service account credentials required to
access the specified KMS. It is a JSON file containing an email address
and the private key of the service account holder.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|google_reachability
|link:#google_reachability[google_reachability]
a|Indicates whether or not the Google Cloud KMS service is reachable from
all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|key_name
|string
a|Key Identifier of Google Cloud KMS key encryption key.

|key_ring_location
|string
a|Google Cloud KMS key ring location.

|key_ring_name
|string
a|Google Cloud KMS key ring name of the deployed Google Cloud application.
```

|project_id
|string
a|Google Cloud project (application) ID of the deployed Google Cloud application that has appropriate access to the Google Cloud KMS.

|proxy_host
|string
a|Proxy host name.

|proxy_password
|string
a|Proxy password. Password is not audited.

|proxy_port
|integer
a|Proxy port number.

|proxy_type
|string
a|Type of proxy.

|proxy_username
|string
a|Proxy username.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|state
|link:#state[state]
a|Google Cloud Key Management Services is a cloud key management service (KMS) that provides a secure store for encryption keys. This object indicates whether or not the Google Cloud KMS key protection is available on all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|svm
|link:#svm[svm]
a|

|uuid
|string
a|A unique identifier for the Google Cloud KMS.
```

```
|===
```

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "application_credentials": "{ type: service_account, project_id:
project-id, private_key_id: key-id, private_key: -----BEGIN PRIVATE
KEY-----\nprivate-key\n-----END PRIVATE KEY-----\n, client_email: service-
account-email, client_id: client-id, auth_uri:
https://accounts.google.com/o/oauth2/auth, token_uri:
https://accounts.google.com/o/oauth2/token, auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs, client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/service-account-email
}",
  "ekmip_reachability": {
    "code": 346758,
    "message": "embedded KMIP server status unavailable on node.",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  },
}
```

```

"google_reachability": {
  "code": 346758,
  "message": "Google Cloud KMS service is not reachable from all nodes -
<reason>."
},
"key_name": "cryptokey1",
"key_ring_location": "global",
"key_ring_name": "gcpappl-keyring",
"project_id": "gcpappl",
"proxy_host": "proxy.eng.com",
"proxy_password": "proxypassword",
"proxy_port": 1234,
"proxy_type": "http",
"proxy_username": "proxyuser",
"scope": "svm",
"state": {
  "code": 346758,
  "message": "Top-level internal key protection key (KEK) is unavailable
on the following nodes with the associated reasons: Node: node1. Reason:
No volumes created yet for the SVM. Wrapped KEK status will be available
after creating encrypted volumes."
},
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```



```

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#gcp_kms[gcp_kms]]
a|

|===

```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```

{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "application_credentials": "{ type: service_account, project_id:
project-id, private_key_id: key-id, private_key: -----BEGIN PRIVATE
KEY-----\nprivate-key\n-----END PRIVATE KEY-----\n, client_email: service-
account-email, client_id: client-id, auth_uri:
https://accounts.google.com/o/oauth2/auth, token_uri:
https://accounts.google.com/o/oauth2/token, auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs, client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/service-account-email
}",
    "ekmip_reachability": {
      "code": 346758,

```

```

    "message": "embedded KMIP server status unavailable on node.",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  },
  "google_reachability": {
    "code": 346758,
    "message": "Google Cloud KMS service is not reachable from all nodes
- <reason>."
  },
  "key_name": "cryptokey1",
  "key_ring_location": "global",
  "key_ring_name": "gcpapp1-keyring",
  "project_id": "gcpapp1",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "svm",
  "state": {
    "code": 346758,
    "message": "Top-level internal key protection key (KEK) is
unavailable on the following nodes with the associated reasons: Node:
node1. Reason: No volumes created yet for the SVM. Wrapped KEK status will
be available after creating encrypted volumes."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
}
=====

```

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 65537703
```

```
| The Google Cloud Key Management Service is not supported for the admin  
Vserver.
```

```
| 65537704
```

```
| The Google Cloud Key Management Service is not supported in MetroCluster  
configurations.
```

```
| 65537706
```

```
| Internal error. Failed to the encrypt the application credentials.
```

```
| 65537713
```

```
| Internal Error. Failed to store the application credentials.
```

```
| 65537719
```

```
| Failed to enable the Google Cloud Key Management Service for SVM  
+++<svm-name>+++because invalid application credentials were  
provided.+++</svm-name>+++
```

```
| 65537720
```

```
| Failed to configure Google Cloud Key Management Service for SVM +++<svm-  
name>+++because a key manager has already been configured for this SVM.  
Use the REST API GET method \"/api/security/key-managers\" to view all of  
the configured key managers.+++</svm-name>+++
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```

a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]

```

```

[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===

[#ekmip_reachability]
[.api-collapsible-fifth-title]
ekmip_reachability

```

Provides the connectivity status for the given SVM on the given node to all EKMIP servers configured on all nodes of the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|integer
```

a|Code corresponding to the error message. Returns a 0 if a given SVM is able to communicate to the EKMIP servers of all of the nodes in the cluster.

```
|message
```

```
|string
```

a|Error message set when cluster-wide EKMIP server availability from the given SVM and node is false.

```
|node
```

```
|link:#node[node]
```

```
a|
```

```
|reachable
```

```
|boolean
```

a|Set to true if the given SVM on the given node is able to communicate to all EKMIP servers configured on all nodes in the cluster.

```
|===
```

```
[#google_reachability]
```

```
[.api-collapsible-fifth-title]
```

```
google_reachability
```

Indicates whether or not the Google Cloud KMS service is reachable from all nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query

parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|integer
```

a|Code corresponding to the error message. Returns a 0 if Google Cloud KMS service is reachable from all nodes in the cluster.

```
|message
```

```
|string
```

a|Set to the error message when 'reachable' is false.

```
|reachable
```

```
|boolean
```

a|Set to true if the Google Cloud KMS service is reachable from all nodes of the cluster.

```
|===
```

```
[#state]
```

```
[.api-collapsible-fifth-title]
```

state

Google Cloud Key Management Services is a cloud key management service (KMS) that provides a secure store for encryption keys. This object indicates whether or not the Google Cloud KMS key protection is available on all nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```

|Description

|cluster_state
|boolean
a|Set to true when Google Cloud KMS key protection is available on all
nodes of the cluster.

|code
|integer
a|Error code corresponding to the status message. Returns 0 if Google
Cloud KMS key protection is available in all nodes of the cluster.

|message
|string
a|Error message set when top-level internal key protection key (KEK)
availability on cluster is false.

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

```



```

|===

[#gcp_kms]
[.api-collapsible-fifth-title]
gcp_kms

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|application_credentials
|string
a|Google Cloud application's service account credentials required to
access the specified KMS. It is a JSON file containing an email address
and the private key of the service account holder.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|google_reachability
|link:#google_reachability[google_reachability]
a|Indicates whether or not the Google Cloud KMS service is reachable from
all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|key_name
|string
a|Key Identifier of Google Cloud KMS key encryption key.

|key_ring_location
|string
a|Google Cloud KMS key ring location.

```

|key_ring_name
|string
a|Google Cloud KMS key ring name of the deployed Google Cloud application.

|project_id
|string
a|Google Cloud project (application) ID of the deployed Google Cloud application that has appropriate access to the Google Cloud KMS.

|proxy_host
|string
a|Proxy host name.

|proxy_password
|string
a|Proxy password. Password is not audited.

|proxy_port
|integer
a|Proxy port number.

|proxy_type
|string
a|Type of proxy.

|proxy_username
|string
a|Proxy username.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|state
|link:#state[state]
a|Google Cloud Key Management Services is a cloud key management service (KMS) that provides a secure store for encryption keys. This object

indicates whether or not the Google Cloud KMS key protection is available on all nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|A unique identifier for the Google Cloud KMS.
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|next
|link:#href[href]
a|
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description

|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```

|===

//end collapsible .Definitions block
=====

[[IDcddf5fa46ab9430589c8ffcc87fb1053]]
= Re-key the external key in the key hierarchy for an SVM

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/gcp-kms/{gcp_kms.uuid}/rekey-external`#

*Introduced In:* 9.11

Rekeys the external key in the key hierarchy for an SVM with a Google
Cloud KMS configuration.

== Related ONTAP commands

* `security key-manager external gcp rekey-external`

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|gcp_kms.uuid
|string
|path
|True
a|UUID of the existing Google Cloud KMS configuration.

|return_timeout
|integer
|query
|False
a|The number of seconds to allow the call to execute before returning.

```

When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

- * Default value: 1
- * Max value: 120
- * Min value: 0

- |return_records
- |boolean
- |query
- |False

a|The default is false. If set to true, the records are returned.

- * Default value:

- |===

== Request Body

- [cols=3*,options=header]
- |===
- |Name
- |Type
- |Description

- |key_name
- |string
- a|Key identifier of the Google Cloud KMS key encryption key.

- |scope
- |string
- a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

- |svm
- |link:#svm[svm]
- a|

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "key_name": "cryptokey1",
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

```
=====
```

```
== Response
```

Status: 202, Accepted

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 65537547
```

| One or more volume encryption keys for encrypted volumes of this data SVM are stored in the key manager configured for the admin SVM. Use the REST API POST method to migrate this data SVM's keys from the admin SVM's key manager to this data SVM's key manager before running the rekey operation.

```
| 65537721
```

| Google Cloud KMS is not configured for the given SVM.

```

| 65537729
| External rekey failed on one or more nodes. Use the REST API POST method
"/api/security/gcp-kms/{uuid}/rekey-external" to try the rekey operation
again.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]

```



```

[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```

```

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#gcp_kms_key]
[.api-collapsible-fifth-title]
gcp_kms_key

[cols=3*,options=header]
|===
|Name
|Type
|Description

|key_name
|string
a|Key identifier of the Google Cloud KMS key encryption key.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|svm
|link:#svm[svm]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===

```

```
|Name
|Type
|Description

|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```

|===

//end collapsible .Definitions block
=====

[[ID0d2cdaa3657cad576b90e14c22c2b113]]
= Delete a Google Cloud KMS configuration

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/gcp-kms/{uuid}`#

*Introduced In:* 9.9

Deletes a Google Cloud KMS configuration.

== Related ONTAP commands

* `security key-manager external gcp disable`

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|Google Cloud KMS UUID

|===

== Response

```

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

Error Code	Description
------------	-------------

65536242	
----------	--

One or more self-encrypting drives are assigned an authentication key.	
--	--

65536243	
----------	--

Cannot determine authentication key presence on one or more self-encrypting drives.	
---	--

65536817	
----------	--

Internal error. Failed to determine if it is safe to disable key manager.	
---	--

65536827	
----------	--

Internal error. Failed to determine if the given SVM has any encrypted volumes.	
---	--

65536834	
----------	--

Internal error. Failed to get existing key-server details for the given SVM.	
--	--

65536867	
----------	--

Volume encryption keys (VEK) for one or more encrypted volumes are stored on the key manager configured for the given SVM.	
--	--

65536883	
----------	--

Internal error. Volume encryption key is missing for a volume.	
--	--

65536884	
----------	--

Internal error. Volume encryption key is invalid for a volume.	
--	--

65536924	
----------	--

Cannot remove key manager that still contains one or more authentication keys for self-encrypting drives.	
---	--

65537721	
----------	--

The Google Cloud Key Management Service is not configured for the SVM.	
--	--

```
| 196608080
| One or more nodes in the cluster have the root volume encrypted using
NVE (NetApp Volume Encryption).

| 196608301
| Internal error. Failed to get encryption type.

| 196608305
| NAE aggregates found in the cluster.
|===
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
```

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

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
```

```

[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message

```

```

|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID441b02ebc1e667c7736f0ba157042654]]
= Retrieve the Google Cloud KMS configuration

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/gcp-kms/{uuid}`#

*Introduced In:* 9.9

Retrieves the Google Cloud KMS configuration for the SVM specified by the
UUID.

== Related ONTAP commands

* `security key-manager external gcp show`
* `security key-manager external gcp check`

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|uuid
|string

```



```

|path
|True
a|Google Cloud KMS UUID

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|application_credentials
|string
a|Google Cloud application's service account credentials required to
access the specified KMS. It is a JSON file containing an email address
and the private key of the service account holder.

|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|google_reachability
|link:#google_reachability[google_reachability]
a|Indicates whether or not the Google Cloud KMS service is reachable from
all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

```

```
|key_name
|string
a|Key Identifier of Google Cloud KMS key encryption key.

|key_ring_location
|string
a|Google Cloud KMS key ring location.

|key_ring_name
|string
a|Google Cloud KMS key ring name of the deployed Google Cloud application.

|project_id
|string
a|Google Cloud project (application) ID of the deployed Google Cloud
application that has appropriate access to the Google Cloud KMS.

|proxy_host
|string
a|Proxy host name.

|proxy_password
|string
a|Proxy password. Password is not audited.

|proxy_port
|integer
a|Proxy port number.

|proxy_type
|string
a|Type of proxy.

|proxy_username
|string
a|Proxy username.
```

```

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|state
|link:#state[state]
a|Google Cloud Key Management Services is a cloud key management service
(KMS) that provides a secure store for encryption keys. This object
indicates whether or not the Google Cloud KMS key protection is available
on all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|A unique identifier for the Google Cloud KMS.

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "application_credentials": "{ type: service_account, project_id:
project-id, private_key_id: key-id, private_key: -----BEGIN PRIVATE
KEY-----\nprivate-key\n-----END PRIVATE KEY-----\n, client_email: service-
account-email, client_id: client-id, auth_uri:
https://accounts.google.com/o/oauth2/auth, token_uri:

```

```

https://accounts.google.com/o/oauth2/token, auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs, client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/service-account-email
}],
  "ekmip_reachability": {
    "code": 346758,
    "message": "embedded KMIP server status unavailable on node.",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  },
  "google_reachability": {
    "code": 346758,
    "message": "Google Cloud KMS service is not reachable from all nodes -
<reason>."
  },
  "key_name": "cryptokey1",
  "key_ring_location": "global",
  "key_ring_name": "gcpappl-keyring",
  "project_id": "gcpappl",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "svm",
  "state": {
    "code": 346758,
    "message": "Top-level internal key protection key (KEK) is unavailable
on the following nodes with the associated reasons: Node: node1. Reason:
No volumes created yet for the SVM. Wrapped KEK status will be available
after creating encrypted volumes."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",

```

```

    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description

| 65537551
| Top-level internal key protection key (KEK) unavailable on one or more
nodes.

| 65537552
| Embedded KMIP server status not available.

| 65537730
| The Google Cloud Key Management Service is unreachable from one or more
nodes.
|===

```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```

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

```

====

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

====

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]

```

|===

```

|Name
|Type
|Description

```

```

|href
|string

```

a|

|===

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]

```

|===

```

|Name
|Type
|Description

```

```

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===

[#ekmip_reachability]
[.api-collapsible-fifth-title]
ekmip_reachability

```

Provides the connectivity status for the given SVM on the given node to all EKMIP servers configured on all nodes of the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```

[cols=3*,options=header]
|===
|Name

```

Type	Description
code	integer
a	Code corresponding to the error message. Returns a 0 if a given SVM is able to communicate to the EKMIP servers of all of the nodes in the cluster.
message	string
a	Error message set when cluster-wide EKMIP server availability from the given SVM and node is false.
node	link:#node[node]
a	
reachable	boolean
a	Set to true if the given SVM on the given node is able to communicate to all EKMIP servers configured on all nodes in the cluster.
===	
[#google_reachability]	[.api-collapsible-fifth-title]
google_reachability	
	Indicates whether or not the Google Cloud KMS service is reachable from all nodes in the cluster.
	This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.
[cols=3*,options=header]	
===	
Name	
Type	
Description	


```

|code
|integer
a|Code corresponding to the error message. Returns a 0 if Google Cloud KMS
service is reachable from all nodes in the cluster.

|message
|string
a|Set to the error message when 'reachable' is false.

|reachable
|boolean
a|Set to true if the Google Cloud KMS service is reachable from all nodes
of the cluster.

|===

[#state]
[.api-collapsible-fifth-title]
state

Google Cloud Key Management Services is a cloud key management service
(KMS) that provides a secure store for encryption keys. This object
indicates whether or not the Google Cloud KMS key protection is available
on all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_state
|boolean
a|Set to true when Google Cloud KMS key protection is available on all
nodes of the cluster.

|code

```

```

|integer
a|Error code corresponding to the status message. Returns 0 if Google
Cloud KMS key protection is available in all nodes of the cluster.


|message
|string
a|Error message set when top-level internal key protection key (KEK)
availability on cluster is false.


|===


[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.


|uuid
|string
a|The unique identifier of the SVM.


|===


[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===

```

```
|Name
|Type
|Description

|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```

|===

//end collapsible .Definitions block
=====

[[ID7025173c386b959dc53a42948f64a0c9]]
= Update the Google Cloud KMS configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/gcp-kms/{uuid}`#

*Introduced In:* 9.9

Updates the Google Cloud KMS configuration.

== Optional properties

* `key_name` - Key Identifier of the Google Cloud KMS key encryption key.
* `application_credentials` - New credentials used to verify the
application's identity to the Google Cloud KMS.
* `proxy_type` - Type of proxy (http/https) if proxy configuration is
used.
* `proxy_host` - Proxy hostname if proxy configuration is used.
* `proxy_port` - Proxy port number if proxy configuration is used.
* `proxy_username` - Proxy username if proxy configuration is used.
* `proxy_password` - Proxy password if proxy configuration is used.
* `project_id` - Google Cloud project (application) ID of the deployed
Google Cloud application with appropriate access to the Google Cloud KMS.
* `key_ring_name` - Google Cloud KMS key ring name of the deployed Google
Cloud application with appropriate access to the specified Google Cloud
KMS.
* `key_ring_location` - Google Cloud KMS key ring location.

== Related ONTAP commands

* `security key-manager external gcp update-credentials`

== Parameters

[cols=5*,options=header]
|===

|Name

```

```

|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|Google Cloud KMS UUID


|return_timeout
|integer
|query
|False
a|The number of seconds to allow the call to execute before returning.
When doing a POST, PATCH, or DELETE operation on a single record, the
default is 0 seconds. This means that if an asynchronous operation is
started, the server immediately returns HTTP code 202 (Accepted) along
with a link to the job. If a non-zero value is specified for POST, PATCH,
or DELETE operations, ONTAP waits that length of time to see if the job
completes so it can return something other than 202.

* Default value: 1
* Max value: 120
* Min value: 0

|===

== Request Body


[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|


|application_credentials
|string
a|Google Cloud application's service account credentials required to

```

access the specified KMS. It is a JSON file containing an email address and the private key of the service account holder.

```
|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|
```

```
|google_reachability
|link:#google_reachability[google_reachability]
a|Indicates whether or not the Google Cloud KMS service is reachable from
all nodes in the cluster.
```

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|key_name
|string
a|Key Identifier of Google Cloud KMS key encryption key.
```

```
|key_ring_location
|string
a|Google Cloud KMS key ring location.
```

```
|key_ring_name
|string
a|Google Cloud KMS key ring name of the deployed Google Cloud application.
```

```
|project_id
|string
a|Google Cloud project (application) ID of the deployed Google Cloud
application that has appropriate access to the Google Cloud KMS.
```

```
|proxy_host
|string
a|Proxy host name.
```

```
|proxy_password
|string
a|Proxy password. Password is not audited.
```

```
|proxy_port
|integer
a|Proxy port number.
```

```
|proxy_type
|string
a|Type of proxy.
```

```
|proxy_username
|string
a|Proxy username.
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|state
|link:#state[state]
a|Google Cloud Key Management Services is a cloud key management service
(KMS) that provides a secure store for encryption keys. This object
indicates whether or not the Google Cloud KMS key protection is available
on all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.
```

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|A unique identifier for the Google Cloud KMS.
```

```
|===
```

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "application_credentials": "{ type: service_account, project_id:
project-id, private_key_id: key-id, private_key: -----BEGIN PRIVATE
KEY-----\nprivate-key\n-----END PRIVATE KEY-----\n, client_email: service-
account-email, client_id: client-id, auth_uri:
https://accounts.google.com/o/oauth2/auth, token_uri:
https://accounts.google.com/o/oauth2/token, auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs, client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/service-account-email
}",
  "ekmip_reachability": {
    "code": 346758,
    "message": "embedded KMIP server status unavailable on node.",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  },
  "google_reachability": {
    "code": 346758,
    "message": "Google Cloud KMS service is not reachable from all nodes -
<reason>."
  },
  "key_name": "cryptokey1",
  "key_ring_location": "global",
  "key_ring_name": "gcpappl-keyring",
  "project_id": "gcpappl",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
```



```

"scope": "svm",
"state": {
  "code": 346758,
  "message": "Top-level internal key protection key (KEK) is unavailable
on the following nodes with the associated reasons: Node: node1. Reason:
No volumes created yet for the SVM. Wrapped KEK status will be available
after creating encrypted volumes."
},
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Response

```

Status: 200, Ok

```

== Response

```

Status: 202, Accepted

```

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 65537541
| No inputs were provided for the patch request.
| 65537547
| One or more volume encryption keys for encrypted volumes of this data
SVM are stored in the key manager configured for the admin SVM. Use the

```

REST API POST method to migrate this data SVM's keys from the admin SVM's key manager to this data SVM's key manager before running the rekey operation.

| 65537713

| Internal Error. Failed to store the application credentials.

| 65537714

| The "application_credentials" field must be specified.

| 65537721

| The Google Cloud Key Management Service is not configured for the SVM.

| 65537724

| Failed to update the Google Cloud Key Management Service because invalid application credentials were provided.

| 65537732

| ONTAP 9.9.1 does not allow modification of the following fields, "project_id", "key_ring_name" and "key_ring_location".

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

=====

[source,json,subs=+macros]

{

 "error": {

 "arguments": {

 "code": "string",

 "message": "string"

 },

```

    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```

```
[#node]
[.api-collapsible-fifth-title]
node
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|
```

```
|uuid
|string
a|
```

```
|===
```

```
[#ekmip_reachability]
[.api-collapsible-fifth-title]
ekmip_reachability
```

Provides the connectivity status for the given SVM on the given node to all EKMIP servers configured on all nodes of the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|integer
```

```
a|Code corresponding to the error message. Returns a 0 if a given SVM is
```

able to communicate to the EKMIP servers of all of the nodes in the cluster.

|message

|string

a|Error message set when cluster-wide EKMIP server availability from the given SVM and node is false.

|node

|link:#node[node]

a|

|reachable

|boolean

a|Set to true if the given SVM on the given node is able to communicate to all EKMIP servers configured on all nodes in the cluster.

|===

[#google_reachability]

[.api-collapsible-fifth-title]

google_reachability

Indicates whether or not the Google Cloud KMS service is reachable from all nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|integer

a|Code corresponding to the error message. Returns a 0 if Google Cloud KMS service is reachable from all nodes in the cluster.

```

|message
|string
a|Set to the error message when 'reachable' is false.

|reachable
|boolean
a|Set to true if the Google Cloud KMS service is reachable from all nodes
of the cluster.

|===

[#state]
[.api-collapsible-fifth-title]
state

Google Cloud Key Management Services is a cloud key management service
(KMS) that provides a secure store for encryption keys. This object
indicates whether or not the Google Cloud KMS key protection is available
on all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_state
|boolean
a|Set to true when Google Cloud KMS key protection is available on all
nodes of the cluster.

|code
|integer
a|Error code corresponding to the status message. Returns 0 if Google
Cloud KMS key protection is available in all nodes of the cluster.

|message

```

```

|string
a|Error message set when top-level internal key protection key (KEK)
availability on cluster is false.

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#gcp_kms]
[.api-collapsible-fifth-title]
gcp_kms

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]

```

a|

|application_credentials

|string

a|Google Cloud application's service account credentials required to access the specified KMS. It is a JSON file containing an email address and the private key of the service account holder.

|ekmip_reachability

|array[link:#ekmip_reachability[ekmip_reachability]]

a|

|google_reachability

|link:#google_reachability[google_reachability]

a|Indicates whether or not the Google Cloud KMS service is reachable from all nodes in the cluster.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

|key_name

|string

a|Key Identifier of Google Cloud KMS key encryption key.

|key_ring_location

|string

a|Google Cloud KMS key ring location.

|key_ring_name

|string

a|Google Cloud KMS key ring name of the deployed Google Cloud application.

|project_id

|string

a|Google Cloud project (application) ID of the deployed Google Cloud application that has appropriate access to the Google Cloud KMS.

|proxy_host

|string

a|Proxy host name.


```
|proxy_password
|string
a|Proxy password. Password is not audited.
```

```
|proxy_port
|integer
a|Proxy port number.
```

```
|proxy_type
|string
a|Type of proxy.
```

```
|proxy_username
|string
a|Proxy username.
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|state
|link:#state[state]
a|Google Cloud Key Management Services is a cloud key management service
(KMS) that provides a secure store for encryption keys. This object
indicates whether or not the Google Cloud KMS key protection is available
on all nodes in the cluster.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.
```

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|A unique identifier for the Google Cloud KMS.
```

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

```
[#error]
```

```
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

```

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDcbcc597868cc16e74a3ccdee40a030ff]]
= Re-key the internal key in the key hierarchy for an SVM

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/gcp-kms/{uuid}/rekey-internal`#

*Introduced In:* 9.10

Rekeys the internal key in the key hierarchy for an SVM with a Google
Cloud KMS configuration.

== Related ONTAP commands

* `security key-manager external gcp rekey-internal`

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|uuid

```

```
|string
|path
|True
a|UUID of the existing Google Cloud KMS configuration.
```

```
|return_timeout
|integer
|query
|False
a|The number of seconds to allow the call to execute before returning.
When doing a POST, PATCH, or DELETE operation on a single record, the
default is 0 seconds. This means that if an asynchronous operation is
started, the server immediately returns HTTP code 202 (Accepted) along
with a link to the job. If a non-zero value is specified for POST, PATCH,
or DELETE operations, ONTAP waits that length of time to see if the job
completes so it can return something other than 202.
```

```
* Default value: 1
* Max value: 120
* Min value: 0
```

```
|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.
```

```
* Default value:
```

```
|===
```

```
== Response
```

Status: 202, Accepted

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description
```

| 65537547
| One or more volume encryption keys for encrypted volumes of this data SVM are stored in the key manager configured for the admin SVM. Use the REST API POST method to migrate this data SVM's keys from the admin SVM's key manager to this data SVM's key manager before running the rekey operation.

| 65537559
| There are no existing internal keys for the SVM. A rekey operation is allowed for an SVM with one or more encryption keys.

| 65537721
| Google Cloud KMS is not configured for the given SVM.
|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

====

[source,json,subs=+macros]

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

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
====
```

```
[#error_arguments]
```

```
[.api-collapsible-fifth-title]
```

```
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```

```
[#error]
```

```
[.api-collapsible-fifth-title]
```

```
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|arguments
```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID8bb1ee9a77811e9882318e1712bb18d5]]
= Restore keys for an SVM from a Google Cloud KMS

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/gcp-kms/{uuid}/restore`#

*Introduced In:* 9.10

Restores the keys for an SVM from a configured Google Cloud KMS.

== Related ONTAP commands

* `security key-manager external gcp restore`

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required

```

|Description

|uuid

|string

|path

|True

a|UUID of the existing Google Cloud KMS configuration.

|return_timeout

|integer

|query

|False

a|The number of seconds to allow the call to execute before returning.

When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

* Default value: 1

* Max value: 120

* Min value: 0

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Response

Status: 202, Accepted

== Error

Status: Default

ONTAP Error Response Codes


```

|===
| Error Code | Description

| 65537721
| The Google Cloud Key Management Service is not configured for the given
SVM.

| 65537722
| Failed to restore keys on the following SVMs.
|===

```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```

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

```

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```

.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```

```

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= View and update IPsec configuration

:leveloffset: +1

[[ID2d222fff02856fbbb9e11d3ee78a59ae]]
= Security IPsec endpoint overview

== Overview

The following operations are supported:

* GET to retrieve the IPsec status: GET security/ipsec
* Patch to update IPsec status: PATCH security/ipsec

[[IDdd03cf5c2182c4a63565233d9028ccdf]]
= Retrieve an IPsec configuration

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/ipsec`#

```

Introduced In: 9.8

Retrieves IPsec configuration via REST APIs.

== Related ONTAP commands

* 'security ipsec config show'

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|==

== Response

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|enabled
|boolean
a|Indicates whether or not IPsec is enabled.

|replay_window
|integer
a|Replay window size in packets, where 0 indicates that the relay window
is disabled.

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "replay_window": 0
}
=====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string

```

```

a|

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]

```

```

error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====

[[IDe597f7ef0865a9e4565cfde7cbf9a256]]
= Update an IPsec configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/ipsec`#

*Introduced In:* 9.8

Updates IPsec configuration via REST APIs.

== Related ONTAP commands

```



```
* 'security ipsec config modify'
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#self_link[self_link]
```

```
a|
```

```
|enabled
```

```
|boolean
```

```
a|Indicates whether or not IPsec is enabled.
```

```
|replay_window
```

```
|integer
```

```
a|Replay window size in packets, where 0 indicates that the relay window is disabled.
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "_links": {
```

```
    "self": {
```

```
      "href": "/api/resourcelink"
```

```
    }
```

```
  },
```

```
  "replay_window": 0
```

```
}
```

```
=====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 66256898
```

```
| Internal error. Failed to enable IPsec.
```

```
| 66256899
```

```
| Internal error. Failed to disable IPsec.
```

```
| 66257199
```

```
| IPsec is not supported in the current cluster version.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```
    "arguments": {
```

```
      "code": "string",
```

```
      "message": "string"
```

```

    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```

```
[#ipsec]
[.api-collapsible-fifth-title]
ipsec
```

Manages IPsec configuration via REST APIs.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#self_link[self_link]
```

```
a|
```

```
|enabled
```

```
|boolean
```

```
a|Indicates whether or not IPsec is enabled.
```

```
|replay_window
```

```
|integer
```

```
a|Replay window size in packets, where 0 indicates that the relay window is disabled.
```

```
|===
```

```
[#error_arguments]
```

```
[.api-collapsible-fifth-title]
```

```
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

:leveloffset: -1

= Manage IPsec security certificates

:leveloffset: +1

[[ID0bb4e416c43d23695d7a3701a5e22d9c]]

= Security IPsec ca-certificates endpoint overview

== Overview

The following APIs can be used to add/remove/retrieve the IPsec CA certificates:

- * Creation Post: POST security/ipsec/ca-certificates
- * Collection Get: GET security/ipsec/ca-certificates
- * Instance Get: GET security/ipsec/ca-certificates/{certificate.uuid}
- * Instance Delete: DELETE security/ipsec/ca-certificates/{certificate.uuid}

[[ID7643bbabe52ac9a6c352fee48724717f]]

= Retrieve IPsec CA certificates configured for the cluster and all SVMs

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/ipsec/ca-certificates`#

Introduced In: 9.10

Retrieves the collection of IPsec CA certificates configured for cluster and all SVMs.

== Related ONTAP commands

* `security ipsec ca-certificate show`

== Parameters

[cols=5*,options=header]

```
|===

|Name
|Type
|In
|Required
|Description

|svm.uuid
|string
|query
|False
a|Filter by svm.uuid

|svm.name
|string
|query
|False
a|Filter by svm.name

|scope
|string
|query
|False
a|Filter by scope

|certificate.uuid
|string
|query
|False
a|Filter by certificate.uuid

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|max_records
|integer
|query
|False
```

a|Limit the number of records returned.

|return_records

|boolean

|query

|False

a|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

a|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

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name

|Type

|Description


```

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#ipsec_ca_certificate[ipsec_ca_certificate]]
a|

|===

```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```

{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "scope": "svm",
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",

```

```

      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

```

====
[ #href]
[ .api-collapsible-fifth-title]
href

[cols=3*,options=header]
|====
|Name
|Type
|Description

|href
|string
a|

|====

[ #_links]
[ .api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|====

[ #_links]
[ .api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name
|Type

```

```

|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

IPsec CA certificate UUID

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#ipsec_ca_certificate]
[.api-collapsible-fifth-title]
ipsec_ca_certificate
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|certificate
|link:#certificate[certificate]
a|IPsec CA certificate UUID
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|svm
|link:#svm[svm]
a|
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block
```

```
=====
```

```
[[ID8e3a0ca13c94533bbede137f2f28b017]]
```

```
= Add a CA certificate to IPsec
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/ipsec/ca-certificates`#
```

```
*Introduced In:* 9.10
```

Add CA certificate to IPsec. The CA certificate should already be installed on the cluster prior to adding them to IPsec. The CA certificate can be installed on the cluster using the `/security/certificates` endpoint. The `svm.uuid` or `svm.name` should not be supplied for certificates that have a scope of cluster.

```
== Related ONTAP commands
```

```
* `security ipsec ca-certificate add`
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|return_records
```

```
|boolean
```

```
|query
```

```
|False
```

```
a|The default is false. If set to true, the records are returned.
```

```
* Default value:
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|certificate
```

```
|link:#certificate[certificate]
```

```
a|IPsec CA certificate UUID
```

```
|scope
```

```
|string
```

```
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to  
"cluster".
```

```
|svm
```

```
|link:#svm[svm]
```

```
a|
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "certificate": {
```

```
    "_links": {
```

```
      "self": {
```

```
        "href": "/api/resourcelink"
```

```
      }
```

```
    },
```

```
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
```

```
  },
```

```
  "scope": "svm",
```

```
  "svm": {
```

```
    "_links": {
```



```

        "self": {
            "href": "/api/resourcelink"
        }
    },
    "name": "svml",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
}
}
====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#ipsec_ca_certificate[ipsec_ca_certificate]]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {

```

```

    "href": "/api/resourcelink"
  }
},
"records": {
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

|===

Error Code	Description
------------	-------------

66257296	
----------	--

	CA certificate is not installed.
--	----------------------------------

|===

[cols=3*,options=header]

|===

Name

Type

Description

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
```

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

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
```

```
[#href]
[.api-collapsible-fifth-title]
href
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|href
|string
a|
```

```

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

IPsec CA certificate UUID

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

|===

[#svm]
[.api-collapsible-fifth-title]

```

svm

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|name

|string

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#ipsec_ca_certificate]

[.api-collapsible-fifth-title]

ipsec_ca_certificate

[cols=3*,options=header]

|===

|Name

|Type

|Description

|certificate

|link:#certificate[certificate]

a|IPsec CA certificate UUID

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|svm

```

|link:#svm[svm]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

```

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID4ca0af7eef25658a05b6113b1455d4db]]
= Delete a CA certificate with the specified UUID from IPsec

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/ipsec/ca-certificates/{certificate.uuid}`#

```

Introduced In: 9.10

Deletes the IPsec CA certificate with the specified UUID from IPsec.

== Related ONTAP commands

* `security ipsec ca-certificate remove`

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|certificate.uuid

|string

|path

|True

a|UUID of the CA certificate to be deleted from IPsec.

|===

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 66257298

| CA certificate is not installed for IPsec.

| 66257303


```
| The CA certificate cannot be removed from IPsec because it is not  
installed.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

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

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
====
```

```
[#error_arguments]
```

```
[.api-collapsible-fifth-title]
```

```
error_arguments
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

|===

//end collapsible .Definitions block

====

[[IDed5b6cfcc1debcf149f52c4424b25050]]

= Retrieve a CA certificate configured for IPsec

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/ipsec/ca-certificates/{certificate.uuid}`#

Introduced In: 9.10

Retrieves a specific CA certificate configured for IPsec.

== Related ONTAP commands

* `security ipsec ca-certificate show`

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|certificate.uuid

|string

|path

|True

a|UUID of the IPsec CA certificate.

|fields

|array[string]

|query

|False

```
a|Specify the fields to return.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|certificate
```

```
|link:#certificate[certificate]
```

```
a|IPsec CA certificate UUID
```

```
|scope
```

```
|string
```

```
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to  
"cluster".
```

```
|svm
```

```
|link:#svm[svm]
```

```
a|
```

```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "certificate": {
```

```
    "_links": {
```

```
      "self": {
```

```
        "href": "/api/resourcelink"
```

```
      }
```

```
    },
```

```
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
```

```
  },
```

```
  "scope": "svm",
```

```

"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
}
====

```

```

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

IPsec CA certificate UUID

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#error_arguments]

```

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message


```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
:leveloffset: -1
```

```
= Manage IPsec policies
```

```
:leveloffset: +1
```

```
[[IDce07d2372fffb15e8c9c4aa5a26e82d75]]
= Security IPsec policies endpoint overview
```

```
== Overview
```

The following operations are supported:

- * Collection Get: GET security/ipsec/policies
- * Creation Post: POST security/ipsec/policies
- * Instance Get: GET security/ipsec/policies/uuid
- * Instance Patch: PATCH security/ipsec/policies/uuid
- * Instance Delete: DELETE security/ipsec/policies/uuid

```
[[ID6faf25dc3a41f6b65af53e89a0d4cd4b]]
= Retrieve IPsec policies
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/ipsec/policies`#
```

```
*Introduced In:* 9.8
```

Retrieves the collection of IPsec policies.

== Related ONTAP commands

* `security ipsec policy show`

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|certificate.name

|string

|query

|False

a|Filter by certificate.name

* Introduced in: 9.10

|certificate.uuid

|string

|query

|False

a|Filter by certificate.uuid

* Introduced in: 9.10

|remote_identity

|string

|query

|False

a|Filter by remote_identity

|svm.uuid

|string

|query

```
|False  
a|Filter by svm.uuid
```

```
|svm.name  
|string  
|query  
|False  
a|Filter by svm.name
```

```
|protocol  
|string  
|query  
|False  
a|Filter by protocol
```

```
|scope  
|string  
|query  
|False  
a|Filter by scope
```

```
|enabled  
|boolean  
|query  
|False  
a|Filter by enabled
```

```
|authentication_method  
|string  
|query  
|False  
a|Filter by authentication_method
```

```
* Introduced in: 9.10
```

```
|ipspace.name  
|string  
|query  
|False  
a|Filter by ipspace.name
```

```
|ipspace.uuid
|string
|query
|False
a|Filter by ipspace.uuid
```

```
|local_identity
|string
|query
|False
a|Filter by local_identity
```

```
|name
|string
|query
|False
a|Filter by name
```

```
|remote_endpoint.address
|string
|query
|False
a|Filter by remote_endpoint.address
```

```
|remote_endpoint.port
|string
|query
|False
a|Filter by remote_endpoint.port
```

```
|remote_endpoint.family
|string
|query
|False
a|Filter by remote_endpoint.family
```

```
|remote_endpoint.netmask
|string
|query
|False
```

```
a|Filter by remote_endpoint.netmask
```

```
|local_endpoint.address
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by local_endpoint.address
```

```
|local_endpoint.port
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by local_endpoint.port
```

```
|local_endpoint.family
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by local_endpoint.family
```

```
|local_endpoint.netmask
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by local_endpoint.netmask
```

```
|uuid
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by uuid
```

```
|fields
```

```
|array[string]
```

```
|query
```

```
|False
```

```
a|Specify the fields to return.
```

```
|max_records
```

```
|integer
```

```

|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|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
a|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
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|_links
|link:#_links[_links]
a|

|error
|link:#error[error]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#records[records]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  },
  "num_records": 1,
  "records": {

```

```

    "action": "bypass",
    "authentication_method": "none",
    "certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "cert1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "ipspace": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "exchange",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "local_endpoint": {
      "address": "10.10.10.7",
      "family": "ipv4",
      "netmask": "24",
      "port": "23"
    },
    "protocol": "17",
    "remote_endpoint": {
      "address": "10.10.10.7",
      "family": "ipv4",
      "netmask": "24",
      "port": "23"
    },
    "scope": "svm",
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  }
}

```



```
====
```

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```
    "arguments": {
```

```
      "code": "string",
```

```
      "message": "string"
```

```
    },
```

```
    "code": "4",
```

```
    "message": "entry doesn't exist",
```

```
    "target": "uuid"
```

```
  }
```

```
}
```

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
====
```

```
[#href]
```

```
[.api-collapsible-fifth-title]
```

```
href
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string

```

```

a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

Certificate for the IPsec policy.
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Certificate name
```

```
|uuid
|string
a|Certificate UUID
```

```
|===
```

```
[#ipspace]
[.api-collapsible-fifth-title]
ipspace
```

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|IPspace name
```

```
|uuid
```

```
|string
```

```
a|IPspace UUID
```

```
|===
```

```
[#local_endpoint]
```

```
[.api-collapsible-fifth-title]
```

```
local_endpoint
```

Local endpoint for the IPsec policy.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|address
```

```
|string
```

```
a|IPv4 or IPv6 address
```

```
|family
```

```

|string
a|IPv4 or IPv6

|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the
default value is 64 with a valid range of 1 to 127. Output is always
netmask length.

|port
|string
a|Application port to be covered by the IPsec policy

|===

[#remote_endpoint]
[.api-collapsible-fifth-title]
remote_endpoint

Remote endpoint for the IPsec policy.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|IPv4 or IPv6 address

|family
|string
a|IPv4 or IPv6

|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the
default value is 64 with a valid range of 1 to 127. Output is always
netmask length.

```

```
|port
|string
a|Application port to be covered by the IPsec policy
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#records]
[.api-collapsible-fifth-title]
records
```

IPsec policy object.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```

|Type
|Description

|action
|string
a|Action for the IPsec policy.

|authentication_method
|string
a|Authentication method for the IPsec policy.

|certificate
|link:#certificate[certificate]
a|Certificate for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|ipspace
|link:#ipspace[ipspace]
a|Applies to both SVM and cluster-scoped objects. Either the UUID or name
may be supplied on input.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|local_identity
|string
a|Local Identity

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

```



```
|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.
```

```
|remote_identity
|string
a|Remote Identity
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|secret_key
|string
a|Pre-shared key for IKE negotiation.
```

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|Unique identifier of the IPsec policy.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[IDf2f0ad0452921381c6cf051f27f9633c]]
= Create an IPsec policy
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/ipsec/policies`#
```

```
*Introduced In:* 9.8
```

Creates an IPsec policy.

== Related ONTAP commands

* `security ipsec policy create`

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|action

|string

a|Action for the IPsec policy.

|authentication_method

|string

a|Authentication method for the IPsec policy.

|certificate
|link:#certificate[certificate]
a|Certificate for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|ipSPACE
|link:#ipSPACE[ipSPACE]
a|Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|local_identity
|string
a|Local Identity

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|remote_identity
|string
a|Remote Identity

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|secret_key
|string
a|Pre-shared key for IKE negotiation.
```

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|Unique identifier of the IPsec policy.
```

```
|===
```

.Example request

[%collapsible%closed]

=====

[source,json,subs=+macros]

```
{
  "action": "bypass",
  "authentication_method": "none",
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "cert1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
}
```

```

    "name": "exchange",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|error

```

```
|link:#error[error]
```

```
a|
```

```
|num_records
```

```
|integer
```

```
a|Number of records
```

```
|records
```

```
|array[link:#records[records]]
```

```
a|
```

```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  },
  "num_records": 1,
  "records": {
    "action": "bypass",
    "authentication_method": "none",
    "certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    }
  }
}
```

```

    },
    "name": "cert1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "exchange",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 66257099

| Only one protocol can be specified.

| 66257100

| Only one local port can be specified.

| 66257101

| Only one remote port can be specified.

| 66257104

| IPsec policy with same name already exists in this SVM.

| 66257107

| The specified pre-shared key is not a valid hexadecimal string.

| 66257109

| The specified pre-shared key is not a valid Base64 encoded binary string.

| 66257110

| Failed to a create policy sequencing value.

| 66257111

| The IPsec policy with action ESP TRANSPORT provides packet protection and requires a secret key or certificate for authentication.

| 66257112

| The IPsec policy with the action specified does not provide packet protection and the authentication method provided for the policy will be ignored.

| 66257113

| Only one local IP subnet can be specified.

| 66257114

| Only one remote IP subnet can be specified.

| 66257115

| Port ranges containing more than one port are not supported.

| 66257117

| IPsec is not supported on the SVM specified in the policy, IPsec is

supported on data SVMs only.

```
| 66257120
| The subnet selector must be a host address (An IPv4 address with a 32-
bit netmask or an IPv6 address with a 128-bit netmask).

| 66257121
| The maximum limit of IPsec Policies has reached for the specified SVM.

| 66257125
| The local_endpoint.address must be specified with
local_endpoint.netmask.

| 66257126
| The remote_endpoint.address must be specified with
remote_endpoint.netmask.

| 66257132
| Invalid value for port field. Value should be in range <1-65535>.

| 66257133
| A pre-shared key is needed for the PSK authentication method. Use the
secret_key option to specify a key.

| 66257134
| An end-entity certificate is needed for the PKI authentication method.
Use the certificate.uuid option to specify an end-entity certificate.

| 66257137
| A pre-shared key is not needed for the PKI authentication method.

| 66257139
| Certificate with the specified UUID was not found.

| 66257140
| Only certificates with a client or server type are supported.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```

|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

Certificate for the IPsec policy.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Certificate name

|uuid
|string
a|Certificate UUID

|===

```

```
[#ipspace]
[.api-collapsible-fifth-title]
ipspace
```

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|IPspace name
```

```
|uuid
|string
a|IPspace UUID
```

```
|===
```

```
[#local_endpoint]
[.api-collapsible-fifth-title]
local_endpoint
```

Local endpoint for the IPsec policy.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|address
|string
a|IPv4 or IPv6 address
```

```
|family
|string
a|IPv4 or IPv6
```

```
|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the
default value is 64 with a valid range of 1 to 127. Output is always
netmask length.
```

```
|port
|string
a|Application port to be covered by the IPsec policy
```

```
|===
```

```
[#remote_endpoint]
[.api-collapsible-fifth-title]
remote_endpoint
```

Remote endpoint for the IPsec policy.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|address
|string
a|IPv4 or IPv6 address
```

```
|family
|string
a|IPv4 or IPv6
```

```
|netmask
|string
```

a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always netmask length.

|port

|string

a|Application port to be covered by the IPsec policy

|===

[#svm]

[.api-collapsible-fifth-title]

svm

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|name

|string

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#ipsec_policy]

[.api-collapsible-fifth-title]

ipsec_policy

IPsec policy object.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|action
|string
a|Action for the IPsec policy.

|authentication_method
|string
a|Authentication method for the IPsec policy.

|certificate
|link:#certificate[certificate]
a|Certificate for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|ipspace
|link:#ipspace[ipspace]
a|Applies to both SVM and cluster-scoped objects. Either the UUID or name
may be supplied on input.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|local_identity
|string
a|Local Identity

|name
|string
a|IPsec policy name.

```

```

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|remote_identity
|string
a|Remote Identity

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|secret_key
|string
a|Pre-shared key for IKE negotiation.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|Unique identifier of the IPsec policy.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

```



```

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]

```

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

|string

a|The target parameter that caused the error.

|===

[#records]

[.api-collapsible-fifth-title]

records

IPsec policy object.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|action

|string

a|Action for the IPsec policy.

|authentication_method

|string

a|Authentication method for the IPsec policy.

|certificate

|link:#certificate[certificate]

a|Certificate for the IPsec policy.

```

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|ipspace
|link:#ipspace[ipspace]
a|Applies to both SVM and cluster-scoped objects. Either the UUID or name
may be supplied on input.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|local_identity
|string
a|Local Identity

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|remote_identity
|string
a|Remote Identity

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

```

```

|secret_key
|string
a|Pre-shared key for IKE negotiation.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|Unique identifier of the IPsec policy.

```

```

|===

```

```

//end collapsible .Definitions block
====

```

```

[[ID9ae2e9c675702ba120a8705a8d2ad639]]
= Delete an IPsec policy

```

```

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/ipsec/policies/{uuid}`#

```

```

*Introduced In:* 9.8

```

```

Deletes a specific IPsec policy.

```

```

== Related ONTAP commands

```

```

* `security ipsec policy delete`

```

```

== Parameters

```

```

[cols=5*,options=header]
|===

```

```

|Name
|Type
|In

```

```
|Required
|Description

|uuid
|string
|path
|True
a|IPsec policy UUID

|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description

| 66257096
| Internal error. Failed to purge connections associated with the IPsec
policy.

| 66257116
| IPsec policy with the specified UUID was not found.

|===
```

```
[cols=3*,options=header]
```

```
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====
```

== Definitions

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID33afb7a7fe21e760b0c32092f5cfcdb7]]
= Retrieve an IPsec policy

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/ipsec/policies/{uuid}`#

```

***Introduced In:** 9.8

Retrieves a specific IPsec policy.

== Related ONTAP commands

* ``security ipsec policy show``

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

|True

a|IPsec policy UUID

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|==

== Response

Status: 200, Ok

[cols=3*,options=header]

|==

|Name

|Type

|Description

|action


```

|string
a|Action for the IPsec policy.

|authentication_method
|string
a|Authentication method for the IPsec policy.

|certificate
|link:#certificate[certificate]
a|Certificate for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|ipspace
|link:#ipspace[ipspace]
a|Applies to both SVM and cluster-scoped objects. Either the UUID or name
may be supplied on input.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|local_identity
|string
a|Local Identity

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]

```

a|Remote endpoint for the IPsec policy.

|remote_identity

|string

a|Remote Identity

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|secret_key

|string

a|Pre-shared key for IKE negotiation.

|svm

|link:#svm[svm]

a|

|uuid

|string

a|Unique identifier of the IPsec policy.

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "action": "bypass",
  "authentication_method": "none",
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "cert1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
}
```

```

"ipspace": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "exchange",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"local_endpoint": {
  "address": "10.10.10.7",
  "family": "ipv4",
  "netmask": "24",
  "port": "23"
},
"protocol": "17",
"remote_endpoint": {
  "address": "10.10.10.7",
  "family": "ipv4",
  "netmask": "24",
  "port": "23"
},
"scope": "svm",
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

```

| 66257116
| IPsec policy with the specified UUID was not found.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

Certificate for the IPsec policy.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```

```
|name
|string
a|Certificate name
```

```
|uuid
|string
a|Certificate UUID
```

```
|===
```

```
[#ipspace]
[.api-collapsible-fifth-title]
ipspace
```

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|IPspace name
```

```
|uuid
|string
a|IPspace UUID
```

```
|===
```

```
[#local_endpoint]
[.api-collapsible-fifth-title]
local_endpoint
```

Local endpoint for the IPsec policy.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|address
```

```
|string
```

```
a|IPv4 or IPv6 address
```

```
|family
```

```
|string
```

```
a|IPv4 or IPv6
```

```
|netmask
```

```
|string
```

```
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the  
default value is 64 with a valid range of 1 to 127. Output is always  
netmask length.
```

```
|port
```

```
|string
```

```
a|Application port to be covered by the IPsec policy
```

```
|===
```

```
[#remote_endpoint]
```

```
[.api-collapsible-fifth-title]
```

```
remote_endpoint
```

Remote endpoint for the IPsec policy.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```

|address
|string
a|IPv4 or IPv6 address

|family
|string
a|IPv4 or IPv6

|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the
default value is 64 with a valid range of 1 to 127. Output is always
netmask length.

|port
|string
a|Application port to be covered by the IPsec policy

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string

```


a|The unique identifier of the SVM.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

|===

|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[ID2a18be4b61140c943e36958dc5412ab8]]
= Update an IPsec policy
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/ipsec/policies/{uuid}`#
```

```
*Introduced In:* 9.8
```

Updates a specific IPsec policy.

```
== Related ONTAP commands
```

```
* `security ipsec policy modify`
```

```
== Parameters
```

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```

```
|uuid
```

```
|string
|path
|True
a|IPsec policy UUID
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|action
```

```
|string
```

```
a|Action for the IPsec policy.
```

```
|authentication_method
```

```
|string
```

```
a|Authentication method for the IPsec policy.
```

```
|certificate
```

```
|link:#certificate[certificate]
```

```
a|Certificate for the IPsec policy.
```

```
|enabled
```

```
|boolean
```

```
a|Indicates whether or not the policy is enabled.
```

```
|ipspace
```

```
|link:#ipspace[ipspace]
```

```
a|Applies to both SVM and cluster-scoped objects. Either the UUID or name  
may be supplied on input.
```

```
|local_endpoint
```

```
|link:#local_endpoint[local_endpoint]
```

```
a|Local endpoint for the IPsec policy.
```

```

|local_identity
|string
a|Local Identity

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|remote_identity
|string
a|Remote Identity

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|secret_key
|string
a|Pre-shared key for IKE negotiation.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|Unique identifier of the IPsec policy.

|===

```

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "action": "bypass",
  "authentication_method": "none",
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "cert1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "exchange",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  }
}
```

```
    },  
    "name": "svm1",  
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"  
  },  
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"  
}  
====
```

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|====

Error Code	Description
------------	-------------

66257097	
----------	--

Internal error. Failed to update the IPsec policy.	
--	--

66257099	
----------	--

Only one protocol can be specified.	
-------------------------------------	--

66257100	
----------	--

Only one local port can be specified.	
---------------------------------------	--

66257101	
----------	--

Only one remote port can be specified.	
--	--

66257110	
----------	--

Failed to create a policy sequencing value.	
---	--

66257113	
----------	--

Only one local IP subnet can be specified.	
--	--

66257114	
----------	--

Only one remote IP subnet can be specified.	
---	--

66257115	
----------	--

Port ranges containing more than one port are not supported.	
--	--

```
| 66257116
| IPsec policy with the specified UUID was not found.

| 66257120
| The subnet selector must be a host address (An IPv4 address with a 32-
bit netmask or an IPv6 address with a 128-bit netmask).

| 66257139
| Certificate with the specified UUID was not found.

| 66257140
| Only certificates with a client or server type are supported.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

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

```
=====
```

```
== Definitions
```

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

Certificate for the IPsec policy.

```



```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|Certificate name
```

```
|uuid
```

```
|string
```

```
a|Certificate UUID
```

```
|===
```

```
[#ipspace]
```

```
[.api-collapsible-fifth-title]
```

```
ipspace
```

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|IPspace name
```

```
|uuid
```

```
|string
a|IPspace UUID
```

```
|===
```

```
[#local_endpoint]
[.api-collapsible-fifth-title]
local_endpoint
```

Local endpoint for the IPsec policy.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|address
|string
a|IPv4 or IPv6 address
```

```
|family
|string
a|IPv4 or IPv6
```

```
|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the
default value is 64 with a valid range of 1 to 127. Output is always
netmask length.
```

```
|port
|string
a|Application port to be covered by the IPsec policy
```

```
|===
```

```
[#remote_endpoint]
[.api-collapsible-fifth-title]
```

remote_endpoint

Remote endpoint for the IPsec policy.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|address

|string

a|IPv4 or IPv6 address

|family

|string

a|IPv4 or IPv6

|netmask

|string

a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always netmask length.

|port

|string

a|Application port to be covered by the IPsec policy

|===

[#svm]

[.api-collapsible-fifth-title]

svm

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

```

|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#ipsec_policy]
[.api-collapsible-fifth-title]
ipsec_policy

IPsec policy object.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|action
|string
a|Action for the IPsec policy.

|authentication_method
|string
a|Authentication method for the IPsec policy.

|certificate
|link:#certificate[certificate]
a|Certificate for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

```

|ipSPACE
|link:#ipSPACE[ipSPACE]
a|Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|local_identity
|string
a|Local Identity

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|remote_identity
|string
a|Remote Identity

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|secret_key
|string
a|Pre-shared key for IKE negotiation.

```
|svm
|link:#svm[svm]
a|

|uuid
|string
a|Unique identifier of the IPsec policy.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= View IPsec security associations

:leveloffset: +1

[[IDd2caa00e04f4b54624a7a397fd925741]]
= Security IPsec security-associations endpoint overview

== Overview

* Collection Get: GET security/ipsec/security-associations
* Instance Get: GET security/ipsec/security-associations/uuid

```

```
[[ID88931f1e529e8a070d3d2065754a0cdb]]
```

= Retrieve IPsec and IKE security associations

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/ipsec/security-associations`#
```

Introduced In: 9.8

Retrieves the IPsec and IKE (Internet Key Exchange) security associations.

== Related ONTAP commands

* `security ipsec show-ipseca`

* `security ipsec show-ikesa`

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|remote_address
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by remote_address
```

```
|policy_name
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by policy_name
```

```
|cipher_suite
```

```
|string
```

```
|query
```



```
|False  
a|Filter by cipher_suite
```

```
|local_address  
|string  
|query  
|False  
a|Filter by local_address
```

```
|node.uuid  
|string  
|query  
|False  
a|Filter by node.uuid
```

```
|node.name  
|string  
|query  
|False  
a|Filter by node.name
```

```
|lifetime  
|integer  
|query  
|False  
a|Filter by lifetime
```

```
|svm.uuid  
|string  
|query  
|False  
a|Filter by svm.uuid
```

```
|svm.name  
|string  
|query  
|False  
a|Filter by svm.name
```

```
|scope
```

```
|string  
|query  
|False  
a|Filter by scope
```

```
|ike.authentication  
|string  
|query  
|False  
a|Filter by ike.authentication
```

```
|ike.is_initiator  
|boolean  
|query  
|False  
a|Filter by ike.is_initiator
```

```
|ike.version  
|integer  
|query  
|False  
a|Filter by ike.version
```

```
|ike.responder_security_parameter_index  
|string  
|query  
|False  
a|Filter by ike.responder_security_parameter_index
```

```
|ike.initiator_security_parameter_index  
|string  
|query  
|False  
a|Filter by ike.initiator_security_parameter_index
```

```
|ike.state  
|string  
|query  
|False  
a|Filter by ike.state
```

```
|type
|string
|query
|False
a|Filter by type
```

```
|uuid
|string
|query
|False
a|Filter by uuid
```

```
|ipsec.action
|string
|query
|False
a|Filter by ipsec.action
```

```
|ipsec.inbound.packets
|integer
|query
|False
a|Filter by ipsec.inbound.packets
```

```
|ipsec.inbound.security_parameter_index
|string
|query
|False
a|Filter by ipsec.inbound.security_parameter_index
```

```
|ipsec.inbound.bytes
|integer
|query
|False
a|Filter by ipsec.inbound.bytes
```

```
|ipsec.state
|string
|query
|False
```

a|Filter by ipsec.state

|ipsec.outbound.packets

|integer

|query

|False

a|Filter by ipsec.outbound.packets

|ipsec.outbound.security_parameter_index

|string

|query

|False

a|Filter by ipsec.outbound.security_parameter_index

|ipsec.outbound.bytes

|integer

|query

|False

a|Filter by ipsec.outbound.bytes

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|max_records

|integer

|query

|False

a|Limit the number of records returned.

|return_records

|boolean

|query

|False

a|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
a|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
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|num_records
```

```
|integer
```

```
a|Number of records
```

```

|records
|array[link:#records[records]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  },
  "num_records": 1,
  "records": {
    "cipher_suite": "suite_aescbc",
    "ike": {
      "authentication": "none",
      "state": "none"
    },
    "ipsec": {
      "action": "bypass"
    },
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    }
  },

```

```

    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "ipsec"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },

```

```

    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|next
|link:#href[href]
a|

```

```

|self
|link:#href[href]

```



```

a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
[#ike]
[.api-collapsible-fifth-title]
ike
```

Objects containing parameters specific to IKE (Internet Key Exchange) security association.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|authentication
|string
a|Authentication method for internet key exchange protocol.
```

```
|initiator_security_parameter_index
|string
a|Initiator's security parameter index for the IKE security association.
```

```
|is_initiator
|boolean
a|Indicates whether or not IKE has been initiated by this node.
```

```
|responder_security_parameter_index
|string
a|Responder's security parameter index for the IKE security association.
```

```
|state
|string
a|State of the IKE connection.
```

```
|version
|integer
a|Internet key exchange protocol version.
```

```
|===
```

```
[#inbound]
[.api-collapsible-fifth-title]
inbound
```

Status for inbound parameters for the IPsec security association.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|bytes
|integer
a|Number of inbound bytes for the IPsec security association.
```

```
|packets
|integer
a|Number of inbound packets for the IPsec security association.
```

```
|security_parameter_index
|string
a|Inbound security parameter index for the IPSec security association.
```

```
|===
```

```
[#outbound]
[.api-collapsible-fifth-title]
```

outbound

Status for outbound parameters for the IPsec security association.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|bytes

|integer

a|Number of outbound bytes for the IPsec security association.

|packets

|integer

a|Number of outbound packets for the IPsec security association.

|security_parameter_index

|string

a|Outbound security parameter index for the IPsec security association.

|===

[#ipsec]

[.api-collapsible-fifth-title]

ipsec

Objects containing parameters specific to IPsec security association.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|action

|string

a|Action for the IPsec security association.

```

|inbound
|link:#inbound[inbound]
a|Status for inbound parameters for the IPsec security association.

|outbound
|link:#outbound[outbound]
a|Status for outbound parameters for the IPsec security association.

|state
|string
a|State of the IPsec security association.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

Node with the security association.

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#records]
[.api-collapsible-fifth-title]
records

```

Security association object for IPsec security association and IKE (Internet Key Exchange) security association.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|cipher_suite
```

```
|string
```

```
a|Cipher suite for the security association.
```

```
|ike
```

```
|link:#ike[ike]
```

```
a|Objects containing parameters specific to IKE (Internet Key Exchange) security association.
```

```
|ipsec
```

```
|link:#ipsec[ipsec]
```

```
a|Objects containing parameters specific to IPsec security association.
```

```
|lifetime
```

```
|integer
```

```
a|Lifetime for the security association in seconds.
```

```
|local_address
```

```
|string
```

```
a|Local address of the security association.
```

```
|node
```

```
|link:#node[node]
```

```
a|Node with the security association.
```

```
|policy_name
```

```
|string
```

```
a|Policy name for the security association.
```

```
|remote_address
```

```

|string
a|Remote address of the security association.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|svm
|link:#svm[svm]
a|

|type
|string
a|Type of security association, it can be IPsec or IKE (Internet Key
Exchange).

|uuid
|string
a|Unique identifier of the security association.

|===

//end collapsible .Definitions block
====

[[ID293390d627e273dba9f82905859cd61e]]
= Retrieve an IPsec or IKE security association

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/ipsec/security-associations/{uuid}`#

*Introduced In:* 9.8

Retrieves a specific IPsec or IKE (Internet Key Exchange) security
association.

== Related ONTAP commands

* `security ipsec show-ipsecsa`

```



```
* `security ipsec show-ikesa`
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|UUID of IPsec or IKE security association.
```

```
|fields
```

```
|array[string]
```

```
|query
```

```
|False
```

```
a|Specify the fields to return.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|cipher_suite
```

```
|string
```

```
a|Cipher suite for the security association.
```

```
|ike
```

```
|link:#ike[ike]
```

a|Objects containing parameters specific to IKE (Internet Key Exchange) security association.

|ipsec

|link:#ipsec[ipsec]

a|Objects containing parameters specific to IPsec security association.

|lifetime

|integer

a|Lifetime for the security association in seconds.

|local_address

|string

a|Local address of the security association.

|node

|link:#node[node]

a|Node with the security association.

|policy_name

|string

a|Policy name for the security association.

|remote_address

|string

a|Remote address of the security association.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|svm

|link:#svm[svm]

a|

|type

|string

a|Type of security association, it can be IPsec or IKE (Internet Key

Exchange).

```
|uuid
|string
a|Unique identifier of the security association.
```

```
|===
```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "cipher_suite": "suite_aescbc",
  "ike": {
    "authentication": "none",
    "state": "none"
  },
  "ipsec": {
    "action": "bypass"
  },
  "node": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "ipsec"
}
=====
```

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 66257118
```

```
| IPsec SA with the specified UUID was not found.
```

```
| 66257119
```

```
| IPsec SA with the specified UUID was not found.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```
    "arguments": {
```

```
      "code": "string",
```

```
      "message": "string"
```

```
    },
```

```
    "code": "4",
```

```
    "message": "entry doesn't exist",
```

```
    "target": "uuid"
```

```
  }
```

```
}
```

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
====
```

```
[#ike]
```

```
[.api-collapsible-fifth-title]
```

```
ike
```

Objects containing parameters specific to IKE (Internet Key Exchange) security association.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|authentication
```

```
|string
```

```
a|Authentication method for internet key exchange protocol.
```

```
|initiator_security_parameter_index
```

```
|string
```

```
a|Initiator's security parameter index for the IKE security association.
```

```
|is_initiator
```

```
|boolean
```

```
a|Indicates whether or not IKE has been initiated by this node.
```

```
|responder_security_parameter_index
```

```
|string
```

```
a|Responder's security parameter index for the IKE security association.
```

```
|state
```

```
|string
```

```
a|State of the IKE connection.
```

```
|version
|integer
a|Internet key exchange protocol version.
```

```
|===
```

```
[#inbound]
[.api-collapsible-fifth-title]
inbound
```

Status for inbound parameters for the IPsec security association.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|bytes
|integer
a|Number of inbound bytes for the IPsec security association.
```

```
|packets
|integer
a|Number of inbound packets for the IPsec security association.
```

```
|security_parameter_index
|string
a|Inbound security parameter index for the IPSec security association.
```

```
|===
```

```
[#outbound]
[.api-collapsible-fifth-title]
outbound
```

Status for outbound parameters for the IPsec security association.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|bytes
|integer
a|Number of outbound bytes for the IPsec security association.

|packets
|integer
a|Number of outbound packets for the IPsec security association.

|security_parameter_index
|string
a|Outbound security parameter index for the IPSec security association.

|===

[#ipsec]
[.api-collapsible-fifth-title]
ipsec

Objects containing parameters specific to IPsec security association.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|action
|string
a|Action for the IPsec security association.

|inbound
|link:#inbound[inbound]
a|Status for inbound parameters for the IPsec security association.

```

```
|outbound
|link:#outbound[outbound]
a|Status for outbound parameters for the IPsec security association.
```

```
|state
|string
a|State of the IPsec security association.
```

```
|===
```

```
[#href]
[.api-collapsible-fifth-title]
href
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|href
```

```
|string
```

```
a|
```

```
|===
```

```
[#_links]
```

```
[.api-collapsible-fifth-title]
```

```
_links
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|self
```

```
|link:#href[href]
```

```
a|
```

```
|===
```



```
[#node]
[.api-collapsible-fifth-title]
node

Node with the security association.
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|
```

```
|uuid
|string
a|
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
```

```

|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= View and update key manager configurations

:leveloffset: +1

[[IDe71d00cc7c2972e570afef30706c2989]]
= Security key-manager-configs endpoint overview

== Overview

Retrieves or modifies the key management configuration options. The
following operations are supported:

* GET
* PATCH

== Examples

=== Retrieving cluster-level key manager configurations

```

The following example shows how to retrieve cluster-level manager configurations.

The API:

GET /api/security/key-manager-configs

The call:

curl -X GET 'https://<mgmt-ip>/api/security/key-manager-configs' -H
'accept: application/hal+json'

The response:

```
{
  "cc_mode_enabled": false,
  "health_monitor_polling_interval": 15,
  "cloud_kms_retry_count": 3,
  "_links": {
    "self": {
      "href": "/api/security/key-manager-configs"
    }
  }
}
```

'''

=== Updating the cluster-level key manager configurations

The following example shows how to modify the
"health_monitor_polling_interval" and "cloud_kms_retry_count" fields.

The API:

PATCH /api/security/key-manager-configs

The call:

curl -X PATCH 'https://<mgmt-ip>/api/security/key-manager-configs' -H
'accept: application/hal+json' -d '{"health_monitor_polling_interval":
"20", "cloud_kms_retry_count": "5"}'

'''

=== Updating the cluster-level key manager configurations

The following example shows how to modify the "cc_mode".

The API:

PATCH /api/security/key-manager-configs

The call:

```
curl -X PATCH 'https://<mgmt-ip>/api/security/key-manager-configs' -H
'accept: application/hal+json' -d "{ \"cc_mode_enabled\" : \"true\",
\"passphrase\": \"current_passphrase\" }"
```

'''

[[IDd4e41c11577e6eae5fb75aee24a5e6ae]]
= Retrieve key manager configurations

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/key-manager-configs`#

Introduced In: 9.10

Retrieves key manager configurations.

== Related ONTAP commands

* `security key-manager config show`

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|fields
|array[string]

```
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|cc_mode_enabled
|boolean
a|Indicates whether the Common Criteria Mode configuration is enabled.

|cloud_kms_retry_count
|integer
a|Cloud key manager connection retry count. Supported value range of 0-10.

|health_monitor_polling_interval
|integer
a|Health Monitor Polling Period, in minutes. Supported value range of 15-30 minutes.

|passphrase
|string
a|Current cluster-wide passphrase. This is a required field when setting the cc_mode_enabled field value to true. This is not audited.

|===

.Example response
```

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "cloud_kms_retry_count": 3,
  "health_monitor_polling_interval": 20,
  "passphrase": "The cluster passphrase of length 64-256 ASCII
characters."
}
====

== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
```

```

    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]

```


[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

```

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID19f99d739aaf5ed2cdf0a5babefa9714]]
= Update key manager configurations

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/key-manager-configs`#

*Introduced In:* 9.10

Updates key manager configurations.

== Related ONTAP commands

* `security key-manager config modify`

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|cc_mode_enabled
|boolean
a|Indicates whether the Common Criteria Mode configuration is enabled.

```

```
|cloud_kms_retry_count
|integer
a|Cloud key manager connection retry count. Supported value range of 0-10.

|health_monitor_polling_interval
|integer
a|Health Monitor Polling Period, in minutes. Supported value range of 15-30 minutes.

|passphrase
|string
a|Current cluster-wide passphrase. This is a required field when setting the cc_mode_enabled field value to true. This is not audited.
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "cloud_kms_retry_count": 3,
  "health_monitor_polling_interval": 20,
  "passphrase": "The cluster passphrase of length 64-256 ASCII
characters."
}
```

```
=====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

|===

Error Code	Description
------------	-------------

65536139	
----------	--

	Cluster-wide passphrase is incorrect.
--	---------------------------------------

65536805	
----------	--

	Common Criteria Mode requires an effective cluster version of ONTAP 9.4 or later.
--	---

65536806	
----------	--

	Passphrase length error.
--	--------------------------

65536807	
----------	--

	MetroCluster cannot be configured while in Common Criteria mode.
--	--

65536809	
----------	--

	Common Criteria mode is disabled on the cluster. Contact technical support for assistance in enabling Common Criteria mode.
--	---

65537302	
----------	--

	The passphrase field is required when changing cc_mode_enabled to true.
--	---

65537303	
----------	--

	Modifying polling period requires an effective cluster version of ONTAP 9.10 or later.
--	--

65537304	
----------	--

	Unable to modify polling period because no external key management is configured on the cluster.
--	--

65538404	
----------	--

	Modifying cloud keymanager retry count requires an effective cluster version of ONTAP 9.11 or later.
--	--

|===

[cols=3*,options=header]

|===

Name

Type

Description

|error

```

|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```
[#self_link]
[.api-collapsible-fifth-title]
self_link
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#key_manager_config]
[.api-collapsible-fifth-title]
key_manager_config
```

Manages the various key manager configuration options.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#self_link[self_link]
a|
```

```
|cc_mode_enabled
|boolean
a|Indicates whether the Common Criteria Mode configuration is enabled.
```

```
|cloud_kms_retry_count
|integer
a|Cloud key manager connection retry count. Supported value range of 0-10.
```

```
|health_monitor_polling_interval
|integer
a|Health Monitor Polling Period, in minutes. Supported value range of 15-
```

30 minutes.

```
|passphrase
|string
a|Current cluster-wide passphrase. This is a required field when setting
the cc_mode_enabled field value to true. This is not audited.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= Manage key managers
```

```
:leveloffset: +1
```

```
[[IDb3794eb544035b07851a0f00181531d7]]
```

```
= Security key-managers endpoint overview
```

```
== Overview
```

A key manager is a key management solution (software or dedicated hardware) that enables other ONTAP client modules to securely and persistently store keys for various uses. For example, WAFL uses the key management framework to store and retrieve the volume encryption keys that it uses to encrypt/decrypt data on NVE volumes. A key manager can be configured at both cluster scope and SVM, with one key manager allowed per

SVM. The key management framework in ONTAP supports two mutually exclusive modes for persisting keys: external and onboard.

When an SVM is configured with external key management, the keys are stored on up to four primary key servers that are external to the system.

Once external key management is enabled for an SVM, primary key servers can be added or removed using the `_/api/security/key-managers/{uuid}/key-servers_` endpoint. See [``POST /security/key-managers/{uuid}/key-servers+``] and [``DELETE /security/key-managers/{uuid}/key-servers/{server}+``] for more details.

Setting up external key management dictates that the required certificates for securely communicating with the key server are installed prior to configuring the key manager. To install the required client and server_ca certificates, use the `_/api/security/certificates/_` endpoint.

See [``POST /security/certificates``], [``GET /security/certificates/uuid``] and [``+DELETE /security/certificates/{uuid}+``] for more details.

When an SVM is configured with the Onboard Key Manager, the keys are stored in ONTAP in wrapped format using a key hierarchy created using the salted hash of the passphrase entered when configuring the Onboard Key Manager. This model fits well for customers who use ONTAP to store their own data.

== Examples

=== Creating an external key manager with 1 primary key server for a cluster

The example key manager is configured at the cluster-scope with one primary key server. Note that the UUIDs of the certificates are those that are already installed at the cluster-scope. Note the `_return_records=true` query parameter is used to obtain the newly created key manager configuration.

The API:

`POST /api/security/key-managers`

The call:

```
curl -X POST 'https://<mgmt-ip>/api/security/key-
managers?return_records=true' -H 'accept: application/hal+json' -d "{
  \"external\": { \"client_certificate\": { \"uuid\": \"5fb1701a-d922-11e8-
bfe8-005056bb017d\" }, \"server_ca_certificates\": [ { \"uuid\":
```

```
\\"827d7d31-d6c8-11e8-b5bf-005056bb017d\\" }],\\"servers\\": [ { \\"server\\":  
\\"10.225.89.33:5696\\" } ] } }"
```

The response:

```
{  
  "num_records": 1,  
  "records": [  
    {  
      "uuid": "815e9462-dc57-11e8-9b2c-005056bb017d",  
      "external": {  
        "client_certificate": {  
          "uuid": "5fb1701a-d922-11e8-bfe8-005056bb017d"  
        },  
        "server_ca_certificates": [  
          {  
            "uuid": "827d7d31-d6c8-11e8-b5bf-005056bb017d"  
          }  
        ],  
        "servers": [  
          {  
            "server": "10.225.89.33:5696"  
          }  
        ]  
      },  
      "_links": {  
        "self": {  
          "href": "/api/security/key-managers/815e9462-dc57-11e8-9b2c-  
005056bb017d"  
        }  
      }  
    }  
  ],  
}
```

'''

=== Creating an external key manager with two primary key servers

The example key manager is configured at the cluster-scope with two primary key servers. Note that the UUIDs of the certificates are those that are already installed at the cluster-scope. Note the `_return_records=true_query` parameter is used to obtain the newly created key manager configuration.

```

# The API:
POST /api/security/key-managers

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-
managers?return_records=true' -H 'accept: application/hal+json' -d "{
\"external\": { \"client_certificate\": { \"uuid\": \"5fb1701a-d922-11e8-
bfe8-005056bb017d\" }, \"server_ca_certificates\": [ { \"uuid\":
\"827d7d31-d6c8-11e8-b5bf-005056bb017d\" } ], \"servers\": [ { \"server\":
\"104.224.89.33:5696\" }, { \"server\": \"104.224.89.34:5696\" } ] } }"

# The response:
{
  "num_records": 1,
  "records": [
    {
      "uuid": "815e9462-dc57-11e8-9b2c-005056bb017d",
      "external": {
        "client_certificate": {
          "uuid": "5fb1701a-d922-11e8-bfe8-005056bb017d"
        },
        "server_ca_certificates": [
          {
            "uuid": "827d7d31-d6c8-11e8-b5bf-005056bb017d"
          }
        ],
        "servers": [
          {
            "server": "10.225.89.33:5696"
          }
        ]
      },
      "_links": {
        "self": {
          "href": "/api/security/key-managers/815e9462-dc57-11e8-9b2c-
005056bb017d"
        }
      }
    }
  ]
}
-----

'''

=== Creating an external key manager with 1 primary key server for an SVM

```

The example key manager is configured at the SVM-scope with one primary key server. Note that the UUIDs of the certificates are those that are already installed in that SVM. Note the `_return_records=true_query` parameter is used to obtain the newly created key manager configuration.

The API:

POST /api/security/key-managers

The call:

```
curl -X POST 'https://<mgmt-ip>/api/security/key-  
managers?return_records=true' -H 'accept: application/hal+json' -d "{  
  \"svm\": { \"uuid\": \"216e6c26-d6c6-11e8-b5bf-005056bb017d\" },  
  \"external\": { \"client_certificate\": { \"uuid\": \"91dcaf7c-dbbd-11e8-  
9b2c-005056bb017d\" }, \"server_ca_certificates\": [ { \"uuid\":  
  \"a4d4b8ba-dbbd-11e8-9b2c-005056bb017d\" } ], \"servers\": [ { \"server\":  
  \"10.225.89.34:5696\" } ] } }"
```

The response:

```
{  
  "num_records": 1,  
  "records": [  
    {  
      "uuid": "80af63f2-dbbf-11e8-9b2c-005056bb017d",  
      "svm": {  
        "uuid": "216e6c26-d6c6-11e8-b5bf-005056bb017d"  
      },  
      "external": {  
        "client_certificate": {  
          "uuid": "91dcaf7c-dbbd-11e8-9b2c-005056bb017d"  
        },  
        "server_ca_certificates": [  
          {  
            "uuid": "a4d4b8ba-dbbd-11e8-9b2c-005056bb017d"  
          }  
        ],  
        "servers": [  
          {  
            "server": "10.225.89.34:5696"  
          }  
        ]  
      },  
      "_links": {  
        "self": {
```

```

        "href": "/api/security/key-managers/80af63f2-dbbf-11e8-9b2c-
005056bb017d"
    }
}
]
}
-----
'''

```

=== Creating an onboard key manager for a cluster

The following example shows how to create an onboard key manager for a cluster with the onboard key manager configured at the cluster-scope.

```

-----

# The API:
POST /api/security/key-managers

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-managers' -H 'accept:
application/hal+json' -d '{ "onboard": { "passphrase": "passphrase" } }'
-----

'''

```

=== Retrieving the key manager configurations for all clusters and SVMs

The following example shows how to retrieve all configured key managers along with their configurations.

```

-----

# The API:
GET /api/security/key-managers

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers?fields=*' -H
'accept: application/hal+json'

# The response:
{
  "records": [
    {
      "uuid": "2345f09c-d6c9-11e8-b5bf-005056bb017d",

```

```

"scope": "svm",
"svm": {
  "uuid": "0f22f8f3-d6c6-11e8-b5bf-005056bb017d",
  "name": "vs0"
},
"external": {
  "client_certificate": {
    "uuid": "4cb15482-d6c8-11e8-b5bf-005056bb017d",
    "_links": {
      "self": {
        "href": "/api/security/certificates/4cb15482-d6c8-11e8-b5bf-005056bb017d/"
      }
    }
  },
  "server_ca_certificates": [
    {
      "uuid": "8a17c858-d6c8-11e8-b5bf-005056bb017d",
      "_links": {
        "self": {
          "href": "/api/security/certificates/8a17c858-d6c8-11e8-b5bf-005056bb017d/"
        }
      }
    }
  ],
  "servers": [
    {
      "server": "10.2.30.4:5696",
      "timeout": 25,
      "username": "",
      "_links": {
        "self": {
          "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-005056bb017d/key-servers/10.2.30.4:5696/"
        }
      }
    },
    {
      "server": "vs0.local1:3678",
      "timeout": 25,
      "username": "",
      "secondary_key_servers": "1.1.1.1, secondarykeyserver.com",
      "_links": {
        "self": {
          "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-

```



```

        }
    }
}
],
{
    "_links": {
        "self": {
            "href": "/api/security/key-managers/815e9462-dc57-11e8-9b2c-
005056bb017d"
        }
    }
}
],
"num_records": 2,
"_links": {
    "self": {
        "href": "/api/security/key-managers?fields=*"
    }
}
}
}
----

'''

```

=== Retrieving the key manager configurations for all clusters and SVMs (showing Onboard Key Manager)

The following example shows how to retrieve all configured key managers along with their configurations.

```

----

# The API:
GET /api/security/key-managers

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers?fields=*' -H
'accept: application/hal+json'

# The response:
{
    "records": [
        {
            "uuid": "8ba52e0f-ae22-11e9-b747-005056bb7636",
            "scope": "cluster",
            "onboard": {

```



```

        "enabled": true,
        "key_backup": "-----BEGIN
BACKUP-----\n <Backup Data>
\n-----END BACKUP-----\n"
    },
    "volume_encryption": {
        "supported": false,
        "message": "The following nodes do not support volume granular
encryption: ntap-vsim2.",
        "code": 65536935
    },
    "is_default_data_at_rest_encryption_disabled": false
}
],
"num_records": 1
}
----
'''

```

=== Retrieving expensive fields such as, status.code and status.message, associated with a key manager.

These values are not retrieved by default with the 'fields=*' option. The following example shows how to retrieve the expensive objects associated with a key manager.

```

----

# The API:
GET /api/security/key-managers

# The call:
curl -X GET "https://<mgmt-ip>/api/security/key-
managers?fields=status.message,status.code" -H 'acct:
application/hal+json'

# The response:
{
  "records": [
    {
      "uuid": "ac305d46-aef4-11e9-ad3c-005056bb7636",
      "status": {
        "message": "No action needed at this time.",
        "code": 65537200
      },
    },
  ],
}

```

```

    "_links": {
      "self": {
        "href": "/api/security/key-managers/ac305d46-aef4-11e9-ad3c-
005056bb7636"
      }
    }
  },
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/key-managers?fields=status.message,status.code"
    }
  }
}
----

'''

```

=== Retrieving a specific key manager configuration

The following example shows how to retrieve a specific key manager configuration.

The API:

GET /api/security/key-managers/{uuid}

The call:

```

curl -X GET 'https://<mgmt-ip>/api/security/key-managers/<uuid>?fields=*'
-H 'accept: application/hal+json'

```

The response:

```

{
  "uuid": "2345f09c-d6c9-11e8-b5bf-005056bb017d",
  "scope": "svm",
  "svm": {
    "uuid": "0f22f8f3-d6c6-11e8-b5bf-005056bb017d",
    "name": "vs0"
  },
  "external": {
    "client_certificate": {
      "uuid": "4cb15482-d6c8-11e8-b5bf-005056bb017d",
      "_links": {
        "self": {

```

```

    "href": "/api/security/certificates/4cb15482-d6c8-11e8-b5bf-005056bb017d/"
  }
},
"server_ca_certificates": [
  {
    "uuid": "8a17c858-d6c8-11e8-b5bf-005056bb017d",
    "_links": {
      "self": {
        "href": "/api/security/certificates/8a17c858-d6c8-11e8-b5bf-005056bb017d/"
      }
    }
  }
],
"servers": [
  {
    "server": "10.2.30.4:5696",
    "timeout": 25,
    "username": "",
    "_links": {
      "self": {
        "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-005056bb017d/key-servers/10.2.30.4:5696/"
      }
    }
  },
  {
    "server": "vs0.local11:3678",
    "timeout": 25,
    "username": "",
    "_links": {
      "self": {
        "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-005056bb017d/key-servers/vs0.local11:3678/"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-005056bb017d"
  }
}

```

```
}  
}
```

```
'''
```

=== Updating the configuration of an external key manager

The following example shows how to update the `server_ca` configuration of an external key manager.

```
----
```

The API:

```
PATCH /api/security/key-managers/{uuid}
```

The call:

```
curl -X PATCH 'https://<mgmt-ip>/api/security/key-managers/<uuid>?' -H  
'accept: application/hal+json' -d "{ \"external\": {  
  \"server_ca_certificates\": [ { \"uuid\": \"23b05c58-d790-11e8-b5bf-  
005056bb017d\" } ] } }"
```

```
----
```

```
'''
```

=== Updating the passphrase of an Onboard Key Manager

The following example shows how to update the passphrase of a given key manager.

```
----
```

The API:

```
PATCH /api/security/key-managers/{uuid}
```

The call:

```
curl -X PATCH 'https://<mgmt-ip>/api/security/key-managers/<uuid>?' -H  
'accept: application/hal+json' -d "{ \"onboard\": {  
  \"existing_passphrase\": \"existing_passphrase\", \"passphrase\":  
  \"new_passphrase\" } }"
```

```
----
```

```
'''
```

=== Synchronizing the passphrase of the Onboard Key Manager on a cluster

The following example shows how to synchronize the passphrase on a cluster

where the Onboard Key Manager is already configured.

The API:

PATCH /api/security/key-managers/{uuid}

The call:

```
curl -X PATCH 'https://<mgmt-ip>/api/security/key-managers/<uuid>?' -H
'accept: application/hal+json' -d "{  \"onboard\": {
\"existing_passphrase\": \"existing_passphrase\",    \"synchronize\": true
}}"
```

'''

=== Configuring the Onboard Key Manager on a cluster

The following example shows how to configure the Onboard Key Manager on a cluster where the Onboard Key Manager is not configured, but is configured on an MetroCluster partner cluster.

The API:

POST /api/security/key-managers

The call:

```
curl -X POST 'https://<mgmt-ip>/api/security/key-
managers?return_records=false' -H 'accept: application/hal+json' -H
"Content-Type: application/json" -d "{  \"onboard\": {    \"passphrase\":
\"passphrase\",    \"synchronize\": true  }}"
```

'''

=== Deleting a configured key manager

The following example shows how to delete a key manager given its UUID.

The API:

DELETE /api/security/key-managers/{uuid}

The call:

```
curl -X DELETE 'https://<mgmt-ip>/api/security/key-managers/<uuid>?' -H
```

```
'accept: application/hal+json'
```

```
----
```

```
'''
```

```
=== Adding a primary key server to an external key manager
```

The following example shows how to add a primary key server to an external key manager.

```
----
```

```
# The API:
```

```
POST /api/security/key-managers/{uuid}/key-servers
```

```
# The call:
```

```
curl -X POST 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-  
servers?return_records=true' -H 'accept: application/hal+json' -d "{  
  \"server\": \"10.225.89.34:5696\" }"
```

```
# The response:
```

```
{  
  "num_records": 1,  
  "records": [  
    {  
      "server": "10.225.89.34:5696",  
      "_links": {  
        "self": {  
          "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-  
005056bb017d/key-servers/10.225.89.34%3A5696"  
        }  
      }  
    }  
  ]  
}
```

```
----
```

```
'''
```

```
=== Adding 2 primary key servers to an external key manager
```

The following example shows how to add 2 primary key servers to an external key manager. Note that the `_records_` property is used to add multiple primary key servers to the key manager in a single API call.

```
----
```

```
# The API:
POST /api/security/key-managers/{uuid}/key-servers

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers?return_records=true' -H 'accept: application/hal+json' -d '{"records": [ { "server": "10.225.89.34:5696" }, { "server": "10.225.89.33:5696" } ] }'

# The response:
{
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-005056bb017d/key-servers/"
        }
      }
    }
  ]
}
-----

'''
```

=== Retrieving all the key servers configured in an external key manager

The following example shows how to retrieve all key servers configured in an external key manager.

```
-----

# The API:
GET /api/security/key-managers/{uuid}/key-servers

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers?fields=*' -H 'accept: application/hal+json'

# The response:
{
  "records": [
    {
      "uuid": "43e0c191-dc5c-11e8-9b2c-005056bb017d",
```

```

    "server": "10.225.89.33:5696",
    "timeout": 25,
    "username": "",
    "secondary_key_servers": [
        "1.1.1.1",
        "secondarykeyserver.com"
    ],
    "_links": {
        "self": {
            "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-005056bb017d/key-servers/10.225.89.33%3A5696"
        }
    }
},
{
    "uuid": "43e0c191-dc5c-11e8-9b2c-005056bb017d",
    "server": "10.225.89.34:5696",
    "timeout": 25,
    "username": "",
    "_links": {
        "self": {
            "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-005056bb017d/key-servers/10.225.89.34%3A5696"
        }
    }
}
],
"num_records": 2,
"_links": {
    "self": {
        "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-005056bb017d/key-servers?fields=*"
    }
}
}
}
----

'''

```

=== Retrieving a specific primary key server (and any associated secondary key servers) configured in an external key manager

The following example shows how to retrieve a specific primary key server (and any associated secondary key servers) configured in an external key manager.


```

-----

# The API:
GET /api/security/key-managers/{uuid}/key-servers/{server}

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-
servers/{server}?fields=*' -H 'accept: application/hal+json'

# The response:
{
  "uuid": "43e0c191-dc5c-11e8-9b2c-005056bb017d",
  "server": "10.225.89.34:5696",
  "timeout": 25,
  "username": "",
  "secondary_key_servers": [
    "1.1.1.1",
    "secondarykeyserver.com"
  ],
  "_links": {
    "self": {
      "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-
005056bb017d/key-servers/10.225.89.34:5696"
    }
  }
}
-----

```

```
'''
```

=== Updating a specific primary key server configuration configured in an external key manager

The following example shows how to update a specific primary key server configured in an external key manager.

```

-----

# The API:
PATCH /api/security/key-managers/{uuid}/key-servers/{server}

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-
servers/{server}' -H 'accept: application/hal+json' -d '{"timeout": 45
}'
-----

```

'''

=== When the 'secondary_key_servers' field is populated in the PATCH API, the list of secondary key servers

=== associated with the primary key servers is replaced by the list of secondary key servers specified in the

=== 'secondary_key_servers' field.

The following example shows how to update the set of secondary key servers associated with a primary key server.

The API:

PATCH /api/security/key-managers/{uuid}/key-servers/{server}

The call:

```
curl -X PATCH 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers/{server}' -H 'accept: application/hal+json' -d '{"secondary_key_servers": [ \"1.1.1.1\", \"secondarykeyserver.com\" ] }'
```

'''

=== Deleting a primary key server from an external key manager

The following example shows how to delete a primary key server from an external key manager.

The API:

DELETE /api/security/key-managers/{uuid}/key-servers/{server}

The call:

```
curl -X DELETE 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers/{server}' -H 'accept: application/hal+json'
```

'''

=== Bypass the out of quorum checks when deleting a primary key server from an external key manager

The following example shows how to bypass the out of quorum checks when

deleting a primary key server from an external key manager.

The API:

DELETE /api/security/key-managers/{uuid}/key-servers/{server}

The call:

curl -X DELETE 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers/{server}?force=true' -H 'accept: application/hal+json'

'''

[[IDbcd07ecf8f628518141f53637ed1de95]]

= Retrieve key managers

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/key-managers`#

Introduced In: 9.6

Retrieves key managers.

== Expensive properties

There is an added cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter. See [xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Requesting_specific_fields\[Requesting specific fields\]](#) to learn more.

* `status.message`

* `status.code`

== Related ONTAP commands

* `security key-manager show-key-store`

* `security key-manager external show`

* `security key-manager external show-status`

* `security key-manager onboard show-backup`

```
== Parameters
```

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|svm.uuid  
|string  
|query  
|False  
a|Filter by svm.uuid
```

```
|svm.name  
|string  
|query  
|False  
a|Filter by svm.name
```

```
|scope  
|string  
|query  
|False  
a|Filter by scope
```

```
|onboard.key_backup  
|string  
|query  
|False  
a|Filter by onboard.key_backup
```

```
* Introduced in: 9.7
```

```
|onboard.enabled  
|boolean  
|query  
|False  
a|Filter by onboard.enabled
```

```
|volume_encryption.code
|integer
|query
|False
a|Filter by volume_encryption.code
```

* Introduced in: 9.7

```
|volume_encryption.message
|string
|query
|False
a|Filter by volume_encryption.message
```

* Introduced in: 9.7

```
|volume_encryption.supported
|boolean
|query
|False
a|Filter by volume_encryption.supported
```

* Introduced in: 9.7

```
|uuid
|string
|query
|False
a|Filter by uuid
```

```
|is_default_data_at_rest_encryption_disabled
|boolean
|query
|False
a|Filter by is_default_data_at_rest_encryption_disabled
```

* Introduced in: 9.7

```
|policy
|string
|query
```

```

|False
a|Filter by policy

* Introduced in: 9.9

|external.servers.timeout
|integer
|query
|False
a|Filter by external.servers.timeout

* Max value: 60
* Min value: 1

|external.servers.secondary_key_servers
|string
|query
|False
a|Filter by external.servers.secondary_key_servers

* Introduced in: 9.8

|external.servers.username
|string
|query
|False
a|Filter by external.servers.username

|external.servers.server
|string
|query
|False
a|Filter by external.servers.server

|external.client_certificate.name
|string
|query
|False
a|Filter by external.client_certificate.name

* Introduced in: 9.8

```

```
|external.client_certificate.uuid  
|string  
|query  
|False  
a|Filter by external.client_certificate.uuid
```

```
|external.server_ca_certificates.name  
|string  
|query  
|False  
a|Filter by external.server_ca_certificates.name
```

* Introduced in: 9.8

```
|external.server_ca_certificates.uuid  
|string  
|query  
|False  
a|Filter by external.server_ca_certificates.uuid
```

```
|status.code  
|integer  
|query  
|False  
a|Filter by status.code
```

* Introduced in: 9.7

```
|status.message  
|string  
|query  
|False  
a|Filter by status.message
```

* Introduced in: 9.7

```
|fields  
|array[string]  
|query  
|False  
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_timeout
|integer
|query
|False
a|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.
```

```
* Max value: 120
* Min value: 0
* Default value: 1
```

```
|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.
```

```
* Default value: 1
```

```
|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.
```

```
|===
```

```
== Response
```

Status: 200, Ok


```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#security_key_manager[security_key_manager]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    },
  "external": {
    "client_certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    }
  }
}

```



```

AQAAAAAMAAAYAQAAAAAALgePkcAAAAAIgAAAAAaAAAAAAAEOTcR0AAAA
AAAAAAAAAACAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAACIAAAAAAA
KAAAAAAACILCHZAAAAAAAAAAAAAAAAAgAAAAAAQCafcabsxRXMM7gxhLRrzh
AAAAAAAAAAkAAAAAAAAAIAAAAAAAAAA2JjQBQAAACt4IqXcNpVggahl0axLsN4
yQjnNVKWY7mANB29042hI7b70DTGCTaVAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAA
7sbaoQAAAAAiAAAAAAACgAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAka
ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAIgAAAAAaAAAAAAALOHfWkAAAAA
AAAAAAAAAACAAAAAABAMoI9UxrHOGthQm/CB+EHdAAAAAAAAAACQAAAAAA
gAAAAAAACnMmUtAAAAAGV8AtPzENFgsGdsFvmucmYrlQCsFew0HDSFKaZqK6
W8IEVzBAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----'",
    "passphrase": "The cluster password of length 32-256 ASCII
characters."
  },
  "scope": "svm",
  "status": {
    "code": 346758,
    "message": "This cluster is part of a MetroCluster configuration.
Use the REST API POST method security/key_managers/ with the synchronize
option and the same passphrase on the partner cluster before proceeding
with any key manager operations. Failure to do so could lead to
switchover or switchback failure."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "string",
  "volume_encryption": {
    "code": 346758,
    "message": "No platform support for volume encryption in following
nodes - node1, node2."
  }
}
}
====

== Error

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

```

```
[#client_certificate]
[.api-collapsible-fifth-title]
client_certificate
```

Client certificate

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|Certificate name
```

```
|uuid
|string
a|Certificate UUID
```

```
|===
```

```
[#server_ca_certificates]
[.api-collapsible-fifth-title]
server_ca_certificates
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
```

```

a|Certificate name

|uuid
|string
a|Certificate UUID

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#key_server_readcreate]
[.api-collapsible-fifth-title]
key_server_readcreate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|secondary_key_servers
|string
a|A comma delimited string of the secondary key servers associated with
the primary key server.

```

```
|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used.
```

```
|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.
```

```
|username
|string
a|Username credentials for connecting with the key server.
```

```
|===
```

```
[#external]
[.api-collapsible-fifth-title]
external
```

Configures external key management

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|client_certificate
|link:#client_certificate[client_certificate]
a|Client certificate
```

```
|server_ca_certificates
|array[link:#server_ca_certificates[server_ca_certificates]]
a|The UUIDs of the server CA certificates already installed in the cluster
or SVM. The array of certificates are common for all the keyservers per
SVM.
```

```
|servers
|array[link:#key_server_readcreate[key_server_readcreate]]
```


a|The set of external key servers.

|===

[#onboard]
[.api-collapsible-fifth-title]
onboard

Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

[cols=3*,options=header]

|===

|Name
|Type
|Description

|enabled
|boolean

a|Is the onboard key manager enabled?

|existing_passphrase
|string

a|The cluster-wide passphrase. This is not audited.

|key_backup
|string

a|Backup of the onboard key manager's key hierarchy. It is required to save this backup after configuring the onboard key manager to help in the recovery of the cluster in case of catastrophic failures.

|passphrase
|string

a|The cluster-wide passphrase. This is not audited.

|synchronize
|boolean

a|Synchronizes missing onboard keys on any node in the cluster. If a node is added to a cluster that has onboard key management configured, the

synchronize operation needs to be performed in a PATCH operation. In a MetroCluster configuration, if onboard key management is enabled on one site, then the synchronize operation needs to be run as a POST operation on the remote site providing the same passphrase.

|===

```
[#status]
[.api-collapsible-fifth-title]
status
```

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|code
```

```
|integer
```

a|Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|message
```

```
|string
```

a|Current state of the key manager indicating any additional steps to perform to finish the setup. This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

|===

```
[#svm]
```

[.api-collapsible-fifth-title]

svm

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|name

|string

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#volume_encryption]

[.api-collapsible-fifth-title]

volume_encryption

Indicates whether volume encryption is supported in the cluster.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|integer

a|Code corresponding to the status message. Returns a 0 if volume encryption is supported in all nodes of the cluster.

|message

|string

a|Reason for not supporting volume encryption.

|supported

|boolean

a|Set to true when volume encryption support is available on all nodes of the cluster.

|===

[#security_key_manager]

[.api-collapsible-fifth-title]

security_key_manager

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|external

|link:#external[external]

a|Configures external key management

|is_default_data_at_rest_encryption_disabled

|boolean

a|Indicates whether default data-at-rest encryption is disabled in the cluster. This field is deprecated in ONTAP 9.8 and later. Use the "software_data_encryption.disabled_by_default" of /api/security endpoint.

* Default value:

* Introduced in: 9.7

* x-ntap-readModify: true

|onboard

|link:#onboard[onboard]

a|Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

```

|policy
|string
a|Security policy associated with the key manager. This value is currently
ignored if specified for the onboard key manager.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code

```

```

|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
[[IDb0eeb903463c82e277be11cc6e5f27d8]]
```

= Create a key manager

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/key-managers`#
```

Introduced In: 9.6

Creates a key manager.

== Required properties

* `svm.uuid` or `svm.name` - Existing SVM in which to create a key manager.

* `external.client_certificate` - Client certificate. Required only when creating an external key manager.

* `external.server_ca_certificates` - Server CA certificates. Required only when creating an external key manager.

* `external.servers.server` - Primary Key servers. Required only when creating an external key manager.

* `onboard.passphrase` - Cluster-wide passphrase. Required only when creating an Onboard Key Manager.

* `synchronize` - Synchronizes missing onboard keys on any node in the cluster. Required only when creating an Onboard Key Manager at the partner site of a MetroCluster configuration.

== Related ONTAP commands

* `security key-manager external enable`

* `security key-manager onboard enable`

* `security key-manager onboard sync`

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster. This field is deprecated in ONTAP 9.8 and later. Use the
"software_data_encryption.disabled_by_default" of /api/security endpoint.

* Default value: 1
* Introduced in: 9.7
* x-ntap-readModify: true

|onboard
|link:#onboard[onboard]
a|Configures onboard key management. After configuring onboard key
management, save the encrypted configuration data in a safe location so
that you can use it if you need to perform a manual recovery operation.

```



```

|policy
|string
a|Security policy associated with the key manager. This value is currently
ignored if specified for the onboard key manager.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "external": {
    "client_certificate": {
      "_links": {

```



```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
AQAAAMAAAYAQAAAAAALgePkcAAAAAIgAAAAAAAAoAAAAAAAEOTcR0AAAAA
AAAAAAAAAACAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAACIAAAAAAAAA
KAAAAAAAAACi1CHZAAAAAAAAAAAAAAAAAAGAAAAAAAAQCafcabsxRXMM7gxhLRrzh
AAAAAAAAAAkAAAAAAAAIAAAAAAAAAA2JjQBQAAACt4IqXcNpVggah10axLsN4
yQjnNVKWY7mANB29042hI7b70DTGCTaVAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
7sbaoQAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAIAAAAAAAAAAAAAAAAAAka
ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAIgAAAAAAAAoAAAAAAALOHfWkAAAAA
AAAAAAAAAACAAAAAABAMoI9UxrHOGthQm/CB+EHdAAAAAAAAAACQAAAAAAAA
gAAAAAAAAACnMmUtAAAAAGV8AtPzENFGsGdsFvmucmYrlQCsFew0HDSFKaZqK6
W8IEVzBAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----",
  "passphrase": "The cluster password of length 32-256 ASCII
characters."
},
"scope": "svm",
"status": {
  "code": 346758,
  "message": "This cluster is part of a MetroCluster configuration. Use
the REST API POST method security/key_managers/ with the synchronize
option and the same passphrase on the partner cluster before proceeding
with any key manager operations. Failure to do so could lead to
switchover or switchback failure."
},
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svml",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "string",
"volume_encryption": {
  "code": 346758,
  "message": "No platform support for volume encryption in following
nodes - node1, node2."
}
}
===

```

Status: 201, Created

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#security_key_manager[security_key_manager]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "external": {
```

```

"client_certificate": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "cert1",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"server_ca_certificates": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "cert1",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"servers": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "secondary_key_servers": "secondary1.com, 10.2.3.4",
  "server": "keyserver1.com:5698",
  "timeout": 60,
  "username": "admin"
}
},
"onboard": {
  "existing_passphrase": "The cluster password of length 32-256 ASCII
characters.",
  "key_backup": "'-----BEGIN
BACKUP-----
TmV0QXBwIetleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAAAAxBFWWAAAAACEAAAAAAAAA
QAAAAAAAAABzDyyVAAAAALI5Jsjvy6gUxnT78KoDKXHYb6sSeraM00quOULY6BeV
n6dMFxuErCD1lbERaOQZSuaYy1p8oQHtTEfGMLZM4TYiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAGAZJEIWvdeHr5RCavHGclo+wAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAAGAAAAAAAAADV1Vd/AAAAAMFM9Q229Bhp
mDaTSdqku5DCd8wG+fOZSr4bx4JT5WHvV/r5gJnXDQQAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

```

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
AQAAAMAAAYAQAAAAAALgePkcAAAAAIgAAAAAAAOAAAAAAAAAEOTcR0AAAAA
AAAAAAAAAACAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAACIAAAAAAAAA
KAAAAAAAAACIlCHZAAAAAAAAAAAAAAAAAgAAAAAAQCafcabSxRXMM7gxhLRzxxh
AAAAAAAAAAkAAAAAAAAAIAAAAAAAAAA2JjQBQAAACt4IqXcNpVggah10axLsN4
yQjnNVKWY7mANB29042hI7b70DTGCTaVAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAA
7sbaoQAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAka
ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAIgAAAAAAAOAAAAAAAAALOHfWkAAAAA
AAAAAAAAAACAAAAAABAMoI9UxrHOGthQm/CB+EHdAAAAAAAAAACQAAAAAAAA
gAAAAAAAAACnMmUtAAAAAGV8AtPzENFgsGdsFvmucmYrlQCsfew0HDSFKaZqK6
W8IEVzBAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----",
    "passphrase": "The cluster password of length 32-256 ASCII
characters."
  },
  "scope": "svm",
  "status": {
    "code": 346758,
    "message": "This cluster is part of a MetroCluster configuration.
Use the REST API POST method security/key_managers/ with the synchronize
option and the same passphrase on the partner cluster before proceeding
with any key manager operations. Failure to do so could lead to
switchover or switchback failure."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "string",
  "volume_encryption": {
    "code": 346758,
    "message": "No platform support for volume encryption in following
nodes - node1, node2."
  }
}

```

```
}  
====  
  
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 65536038  
| A maximum of 4 active primary key servers are allowed.  
  
| 65536214  
| Failed to generate cluster key encryption key.  
  
| 65536216  
| Failed to add cluster key encryption key.  
  
| 65536310  
| Failed to setup the Onboard Key Manager because the MetroCluster peer is  
unhealthy.  
  
| 65536341  
| Failed to setup the Onboard Key Manager because the MetroCluster peer is  
unhealthy.  
  
| 65536508  
| The platform does not support data at rest encryption.  
  
| 65536821  
| The certificate is not installed.  
  
| 65536822  
| Multitenant key management is not supported in the current cluster  
version.  
  
| 65536823  
| The SVM has key manager already configured.  
  
| 65536824  
| Multitenant key management is not supported in MetroCluster  
configurations.
```

| 65536834
| Failed to get existing key-server details for the SVM.

| 65536852
| Failed to query supported KMIP protocol versions.

| 65536870
| Key management servers already configured.

| 65536871
| Duplicate key management servers exist.

| 65536876
| External key management requires client and server CA certificates installed and with one or more key servers provided.

| 65536878
| External key management cannot be configured as one or more volume encryption keys of the SVM are stored in cluster key management server.

| 65536895
| External key manager cannot be configured since this cluster is part of a MetroCluster configuration and the partner site of this MetroCluster configuration has Onboard Key Manager configured.

| 65536900
| The Onboard Key Manager cannot be configured because this cluster is part of a MetroCluster configuration and the partner site has the external key manager configured.

| 65536903
| The Onboard Key Manager has failed to configure on some nodes in the cluster. Use the CLI to sync the Onboard Key Manager configuration on failed nodes.

| 65536906
| The Onboard Key Manager has already been configured at the partner site. Use the CLI to sync the Onboard Key Manager with the same passphrase.

| 65536907
| The Onboard Key Manager is already configured. Use the CLI to sync any nodes with the Onboard Key Manager configuration.

| 65536916
| The Onboard Key Manager is only supported for an admin SVM.

| 65536920


```

| The Onboard Key Manager passphrase length is incorrect.

| 65537240
| The Onboard Key Manager passphrase must be provided when performing a
POST/synchronize operation.

| 65537241
| The Onboard Key Manager existing_passphrase must not be provided when
performing a POST/synchronize operation.

| 65537244
| Unable to sync/create Onboard Key Manager on the local cluster; Onboard
Key Manager is already configured on the cluster.

| 65537245
| Unable to sync/create Onboard Key Manager on the local cluster; Onboard
Key Manager is not configured on the partner cluster.

| 65537246
| Unable to sync/create Onboard Key Manager on local cluster. This cluster
is not part of a MetroCluster configuration.

| 66060338
| Failed to establish secure connection for a key management server due to
incorrect server_ca certificates.

| 66060339
| Failed to establish secure connection for a key management server due to
incorrect client certificates.

| 66060340
| Failed to establish secure connection for a key management server due to
Cryptsoft error.
|===

```

```

[cols=3*,options=header]

```

```

|===

```

```

|Name

```

```

|Type

```

```

|Description

```

```

|error

```

```

|link:#error[error]

```

```

a|

```

```

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]

```

```

_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#client_certificate]
[.api-collapsible-fifth-title]
client_certificate

Client certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Certificate name

|uuid
|string
a|Certificate UUID

|===

[#server_ca_certificates]
[.api-collapsible-fifth-title]

```

server_ca_certificates

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|name

|string

a|Certificate name

|uuid

|string

a|Certificate UUID

|===

[#self_link]

[.api-collapsible-fifth-title]

self_link

[cols=3*,options=header]

|===

|Name

|Type

|Description

|self

|link:#href[href]

a|

|===

[#key_server_readcreate]

[.api-collapsible-fifth-title]

key_server_readcreate

[cols=3*,options=header]

```

|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|secondary_key_servers
|string
a|A comma delimited string of the secondary key servers associated with
the primary key server.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|Username credentials for connecting with the key server.

|===

[#external]
[.api-collapsible-fifth-title]
external

Configures external key management

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|client_certificate
|link:#client_certificate[client_certificate]
a|Client certificate

|server_ca_certificates
|array[link:#server_ca_certificates[server_ca_certificates]]
a|The UUIDs of the server CA certificates already installed in the cluster
or SVM. The array of certificates are common for all the keyservers per
SVM.

|servers
|array[link:#key_server_readcreate[key_server_readcreate]]
a|The set of external key servers.

|===

[#onboard]
[.api-collapsible-fifth-title]
onboard

Configures onboard key management. After configuring onboard key
management, save the encrypted configuration data in a safe location so
that you can use it if you need to perform a manual recovery operation.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|enabled
|boolean
a|Is the onboard key manager enabled?

|existing_passphrase
|string
a|The cluster-wide passphrase. This is not audited.

|key_backup
|string

```

a|Backup of the onboard key manager's key hierarchy. It is required to save this backup after configuring the onboard key manager to help in the recovery of the cluster in case of catastrophic failures.

|passphrase

|string

a|The cluster-wide passphrase. This is not audited.

|synchronize

|boolean

a|Synchronizes missing onboard keys on any node in the cluster. If a node is added to a cluster that has onboard key management configured, the synchronize operation needs to be performed in a PATCH operation. In a MetroCluster configuration, if onboard key management is enabled on one site, then the synchronize operation needs to be run as a POST operation on the remote site providing the same passphrase.

|===

[#status]

[.api-collapsible-fifth-title]

status

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|integer

a|Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|message
|string
a|Current state of the key manager indicating any additional steps to
perform to finish the setup. This is an advanced property; there is an
added cost to retrieving its value. The property is not populated for
either a collection GET or an instance GET unless it is explicitly
requested using the `fields` query parameter or GET for all advanced
properties is enabled.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#volume_encryption]
[.api-collapsible-fifth-title]
volume_encryption
```

Indicates whether volume encryption is supported in the cluster.


```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message. Returns a 0 if volume
encryption is supported in all nodes of the cluster.

|message
|string
a|Reason for not supporting volume encryption.

|supported
|boolean
a|Set to true when volume encryption support is available on all nodes of
the cluster.

|===

[#security_key_manager]
[.api-collapsible-fifth-title]
security_key_manager

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled
|boolean

```

a|Indicates whether default data-at-rest encryption is disabled in the cluster. This field is deprecated in ONTAP 9.8 and later. Use the "software_data_encryption.disabled_by_default" of /api/security endpoint.

* Default value: 1

* Introduced in: 9.7

* x-ntap-readModify: true

|onboard

|link:#onboard[onboard]

a|Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

|policy

|string

a|Security policy associated with the key manager. This value is currently ignored if specified for the onboard key manager.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|status

|link:#status[status]

a|Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

|svm

|link:#svm[svm]

a|

|uuid

|string

a|

|volume_encryption

|link:#volume_encryption[volume_encryption]

a|Indicates whether volume encryption is supported in the cluster.

```

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

```

```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID74d34827b2aa5aff173b33a5e21e5411]]
= Delete key managers

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/key-managers/{uuid}`#

*Introduced In:* 9.6

Deletes a key manager.

```

== Related ONTAP commands

```
* `security key-manager external disable`  
* `security key-manager onboard disable`
```

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

|True

a|Key manager UUID

|===

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 65536208

| Failed to delete the SVM Key ID.

| 65536233

| Internal error. Deletion of km_wrapped_kdb key database has failed for the Onboard Key Manager.

```
| 65536234
| Internal error. Deletion of cluster_kdb key database has failed for the
Onboard Key Manager.

| 65536239
| Encrypted volumes are found for the SVM.

| 65536242
| One or more self-encrypting drives are assigned an authentication key.

| 65536243
| Cannot determine authentication key presence on one or more self-
encrypting drives.

| 65536800
| Failed to lookup onboard keys.

| 65536813
| Encrypted kernel core files found.

| 65536817
| Failed to determine if key manager is safe to disable.

| 65536822
| Multitenant key management is not supported in the current cluster
version.

| 65536827
| Failed to determine if the SVM has any encrypted volumes.

| 65536828
| External key management is not enabled for the SVM.

| 65536867
| Encrypted volumes are found for the SVM.

| 196608301
| Failed to determine the type of encryption.

| 196608305
| NAE aggregates are found in the cluster.
|===
```

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

```


====

[[IDe0641002a747ed4d30c5107b1d81129a]]

= Retrieve key managers

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/key-managers/{uuid}`#

Introduced In: 9.6

Retrieves key managers.

== Expensive properties

There is an added cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter. See [xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Requesting_specific_fields\[Requesting specific fields\]](#) to learn more.

* `status.message`

* `status.code`

== Related ONTAP commands

* `security key-manager show-key-store`

* `security key-manager external show`

* `security key-manager external show-status`

* `security key-manager onboard show-backup`

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

```

|True
a|Key manager UUID

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster. This field is deprecated in ONTAP 9.8 and later. Use the
"software_data_encryption.disabled_by_default" of /api/security endpoint.

* Default value: 1
* Introduced in: 9.7
* x-ntap-readModify: true

|onboard
|link:#onboard[onboard]
a|Configures onboard key management. After configuring onboard key
management, save the encrypted configuration data in a safe location so

```

that you can use it if you need to perform a manual recovery operation.

|policy
|string
a|Security policy associated with the key manager. This value is currently ignored if specified for the onboard key manager.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
 "_links": {
 "self": {
 "href": "/api/resourcelink"
 }
 },
}

```

"external": {
  "client_certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "cert1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "server_ca_certificates": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "cert1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "servers": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "secondary_key_servers": "secondary1.com, 10.2.3.4",
    "server": "keyserver1.com:5698",
    "timeout": 60,
    "username": "admin"
  }
},
"onboard": {
  "existing_passphrase": "The cluster password of length 32-256 ASCII
characters.",
  "key_backup": "'-----BEGIN
BACKUP-----
TmV0QXBwIEtleSBGbG9iAAEAAAAEAAAAcAEAAAAAAAAAxBFWWAAAAACEAAAAAAAAA
QAAAAAAAAABzDyyVAAAAALi5JsJvy6gUxnT78KoDKXHYb6sSeraM00quOULY6BeV
n6dMFxuErCD1lbERaOQZSuaYy1p8oQHtTEfGMLZM4TYiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAAgAZJEIWvdeHr5RCavHGclo+wAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAAgAAAAAAAAADV1Vd/AAAAAMFM9Q229Bhp
mDaTSdqku5DCd8wG+fOZSr4bx4JT5WHvV/r5gJnXDQQAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

```

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
AQAAAAMAAAYYAQAAAAAALgePkcAAAAAIgAAAAAAAoAAAAAAAEOtCR0AAAAA
AAAAAAAAAAAAACAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAACIAAAAAAAA
KAAAAAAAAAACILCHZAAAAAAAAAAAAAAAAAagAAAAAAQCafcabsxRXMM7gxhLRrzxh
AAAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAA2JjQBQAAACt4IqXcNpVggahl0axLsN4
yQjnNVKWY7mANB29O42hI7b70DTGCTaVAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
7sbaoQAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAAIAAAAAAkA
ave0kd8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAoAAAAAAAALOHfWkAAAAA
AAAAAAAAAAAAACAAAAAABAMoi9UxrHOGthQm/CB+EhdAAAAAAAAAACQAAAAAAAA
gAAAAAAAAACnMmUtAAAAAGVk8AtPzENFgsGdsFvmucmYrlQCsfew0HDSFKaZqK6
W8IEVzbAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----"',
    "passphrase": "The cluster password of length 32-256 ASCII
characters."
},
    "scope": "svm",
    "status": {
        "code": 346758,
        "message": "This cluster is part of a MetroCluster configuration. Use
the REST API POST method security/key_managers/ with the synchronize
option and the same passphrase on the partner cluster before proceeding
with any key manager operations. Failure to do so could lead to
switchover or switchback failure."
    },
    "svm": {
        "_links": {
            "self": {
                "href": "/api/resourceLink"
            }
        },
        "name": "svml",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "volume_encryption": {
        "code": 346758,
        "message": "No platform support for volume encryption in following
nodes - node1, node2."
    }
}

```

```

}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]

```

```

href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#client_certificate]
[.api-collapsible-fifth-title]
client_certificate

Client certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]

```

```

a|

|name
|string
a|Certificate name

|uuid
|string
a|Certificate UUID

|===

[#server_ca_certificates]
[.api-collapsible-fifth-title]
server_ca_certificates

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Certificate name

|uuid
|string
a|Certificate UUID

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]

```



```

|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#key_server_readcreate]
[.api-collapsible-fifth-title]
key_server_readcreate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|secondary_key_servers
|string
a|A comma delimited string of the secondary key servers associated with
the primary key server.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|Username credentials for connecting with the key server.

```

```
|===
```

```
[#external]  
[.api-collapsible-fifth-title]  
external
```

Configures external key management

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|client_certificate  
|link:#client_certificate[client_certificate]  
a|Client certificate
```

```
|server_ca_certificates  
|array[link:#server_ca_certificates[server_ca_certificates]]  
a|The UUIDs of the server CA certificates already installed in the cluster  
or SVM. The array of certificates are common for all the keyservers per  
SVM.
```

```
|servers  
|array[link:#key_server_readcreate[key_server_readcreate]]  
a|The set of external key servers.
```

```
|===
```

```
[#onboard]  
[.api-collapsible-fifth-title]  
onboard
```

Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|enabled
|boolean
a|Is the onboard key manager enabled?

|existing_passphrase
|string
a|The cluster-wide passphrase. This is not audited.

|key_backup
|string
a|Backup of the onboard key manager's key hierarchy. It is required to
save this backup after configuring the onboard key manager to help in the
recovery of the cluster in case of catastrophic failures.

|passphrase
|string
a|The cluster-wide passphrase. This is not audited.

|synchronize
|boolean
a|Synchronizes missing onboard keys on any node in the cluster. If a node
is added to a cluster that has onboard key management configured, the
synchronize operation needs to be performed in a PATCH operation. In a
MetroCluster configuration, if onboard key management is enabled on one
site, then the synchronize operation needs to be run as a POST operation
on the remote site providing the same passphrase.

|===

[#status]
[.api-collapsible-fifth-title]
status

Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message. Returns 0 if the setup is
complete. This is an advanced property; there is an added cost to
retrieving its value. The property is not populated for either a
collection GET or an instance GET unless it is explicitly requested using
the `fields` query parameter or GET for all advanced properties is
enabled.

|message
|string
a|Current state of the key manager indicating any additional steps to
perform to finish the setup. This is an advanced property; there is an
added cost to retrieving its value. The property is not populated for
either a collection GET or an instance GET unless it is explicitly
requested using the `fields` query parameter or GET for all advanced
properties is enabled.

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#volume_encryption]
[.api-collapsible-fifth-title]
volume_encryption
```

Indicates whether volume encryption is supported in the cluster.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|integer
```

a|Code corresponding to the status message. Returns a 0 if volume encryption is supported in all nodes of the cluster.

```
|message
|string
```

a|Reason for not supporting volume encryption.

```
|supported
|boolean
```

a|Set to true when volume encryption support is available on all nodes of the cluster.

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
[[ID39744332292f785f49e7811650c665fe]]
```

```
= Update key managers
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-  
block]#`/security/key-managers/{uuid}`#
```

```
*Introduced In:* 9.6
```

```
Updates a key manager.
```

```
== Required properties
```

```
* `onboard.existing_passphrase` - Cluster-wide passphrase. Required only  
when synchronizing the passphrase of the Onboard Key Manager.
```

```
* `synchronize` - Synchronizes missing Onboard Key Manager keys on any  
node in the cluster. Required only when synchronizing the Onboard Key  
Manager keys in a local cluster.
```

```
== Related ONTAP commands
```

```
* `security key-manager external modify`
```

```
* `security key-manager onboard sync`
```

```
* `security key-manager onboard update-passphrase`
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|uuid
```

```

|string
|path
|True
a|Key manager UUID

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster. This field is deprecated in ONTAP 9.8 and later. Use the
"software_data_encryption.disabled_by_default" of /api/security endpoint.

* Default value: 1
* Introduced in: 9.7
* x-ntap-readModify: true

|onboard
|link:#onboard[onboard]
a|Configures onboard key management. After configuring onboard key
management, save the encrypted configuration data in a safe location so
that you can use it if you need to perform a manual recovery operation.

|policy
|string
a|Security policy associated with the key manager. This value is currently

```


ignored if specified for the onboard key manager.

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.
```

|===

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "external": {
    "client_certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    }
  }
}
```



```

AAAAAAAAAAAAACAAAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAAACIAAAAAAAAA
KAAAAAAAAAACIlCHZAAAAAAAAAAAAAAAAAAGAAAAAAAAQCaFcabsxRXMM7gxhLRrzh
AAAAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAA2JjQBQAAACt4IqXcNpVggah10axLsN4
yQjnNVKWY7mANB29O42hI7b70DTGCTaVAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
7sbaoQAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAka
ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAAAoAAAAAAAAALOHfWkAAAAA
AAAAAAAAAAAAACAAAAAABAMoI9UxrHOGthQm/CB+EHdAAAAAAAAAACQAAAAAAAA
gAAAAAAAAACnMmUtAAAAAGVk8AtPzENFgsGdsFvmucmYrlQCsFew0HDSFKaZqK6
W8IEVzBAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----"',
  "passphrase": "The cluster password of length 32-256 ASCII
characters."
},
"scope": "svm",
"status": {
  "code": 346758,
  "message": "This cluster is part of a MetroCluster configuration. Use
the REST API POST method security/key_managers/ with the synchronize
option and the same passphrase on the partner cluster before proceeding
with any key manager operations. Failure to do so could lead to
switchover or switchback failure."
},
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "string",
"volume_encryption": {
  "code": 346758,
  "message": "No platform support for volume encryption in following
nodes - node1, node2."
}
}
====

== Response

```

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 65536139  
| The existing passphrase value provided does not match the configured  
| passphrase.  
  
| 65536150  
| The new passphrase is same as old passphrase.  
  
| 65536404  
| The passphrase does not match the accepted length.  
  
| 65536406  
| The change of passphrase failed.  
  
| 65536407  
| The passphrase update failed on some nodes.  
  
| 65536802  
| The passphrase does not match the accepted length in common criteria  
| mode.  
  
| 65536821  
| The certificate is not installed.  
  
| 65536822  
| Multitenant key management is not supported in the current cluster  
| version.  
  
| 65536828  
| External key management is not enabled for the SVM.  
  
| 65536850  
| New client certificate public or private keys are different from the  
| existing client certificate.  
  
| 65536852  
| Failed to query supported KMIP protocol versions.
```

```

| 65536917
| Updating an onboard passphrase requires both new and existing cluster
passphrase.

| 65537242
| The Onboard Key Manager existing_passphrase must be provided when
performing a PATCH/synchronize operation.

| 65537243
| The Onboard Key Manager passphrase must not be provided when performing
a PATCH/synchronize operation.

| 66060338
| Failed to establish secure connection for a key management server due to
incorrect server_ca certificates.

| 66060339
| Failed to establish secure connection for a key management server due to
incorrect client certificates.

| 66060340
| Failed to establish secure connection for a key management server due to
Cryptsoft error.
|===

```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```

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

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self

```

```

|link:#href[href]
a|

|===

[#client_certificate]
[.api-collapsible-fifth-title]
client_certificate

Client certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Certificate name

|uuid
|string
a|Certificate UUID

|===

[#server_ca_certificates]
[.api-collapsible-fifth-title]
server_ca_certificates

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links

```

```

|link:#_links[_links]
a|

|name
|string
a|Certificate name

|uuid
|string
a|Certificate UUID

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#key_server_readcreate]
[.api-collapsible-fifth-title]
key_server_readcreate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

```



```
|secondary_key_servers
|string
a|A comma delimited string of the secondary key servers associated with
the primary key server.
```

```
|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used.
```

```
|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.
```

```
|username
|string
a|Username credentials for connecting with the key server.
```

```
|===
```

```
[#external]
[.api-collapsible-fifth-title]
external
```

Configures external key management

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|client_certificate
|link:#client_certificate[client_certificate]
a|Client certificate
```

```
|server_ca_certificates
|array[link:#server_ca_certificates[server_ca_certificates]]
a|The UUIDs of the server CA certificates already installed in the cluster
or SVM. The array of certificates are common for all the keyservers per
```

SVM.

```
|servers
|array[link:#key_server_readcreate[key_server_readcreate]]
a|The set of external key servers.
```

```
|===
```

```
[#onboard]
[.api-collapsible-fifth-title]
onboard
```

Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|enabled
|boolean
```

```
a|Is the onboard key manager enabled?
```

```
|existing_passphrase
|string
```

```
a|The cluster-wide passphrase. This is not audited.
```

```
|key_backup
|string
```

```
a|Backup of the onboard key manager's key hierarchy. It is required to save this backup after configuring the onboard key manager to help in the recovery of the cluster in case of catastrophic failures.
```

```
|passphrase
|string
```

```
a|The cluster-wide passphrase. This is not audited.
```

|synchronize

|boolean

a|Synchronizes missing onboard keys on any node in the cluster. If a node is added to a cluster that has onboard key management configured, the synchronize operation needs to be performed in a PATCH operation. In a MetroCluster configuration, if onboard key management is enabled on one site, then the synchronize operation needs to be run as a POST operation on the remote site providing the same passphrase.

|===

[#status]

[.api-collapsible-fifth-title]

status

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|integer

a|Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

|message

|string

a|Current state of the key manager indicating any additional steps to perform to finish the setup. This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|===
```

```
[#svm]
```

```
[.api-collapsible-fifth-title]
```

```
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#volume_encryption]
```

```
[.api-collapsible-fifth-title]
```

```
volume_encryption
```

Indicates whether volume encryption is supported in the cluster.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|integer
```

```
a|Code corresponding to the status message. Returns a 0 if volume
```

encryption is supported in all nodes of the cluster.

```
|message
|string
a|Reason for not supporting volume encryption.
```

```
|supported
|boolean
a|Set to true when volume encryption support is available on all nodes of
the cluster.
```

```
|===
```

```
[#security_key_manager]
[.api-collapsible-fifth-title]
security_key_manager
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|external
|link:#external[external]
a|Configures external key management
```

```
|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster. This field is deprecated in ONTAP 9.8 and later. Use the
"software_data_encryption.disabled_by_default" of /api/security endpoint.
```

```
* Default value: 1
* Introduced in: 9.7
* x-ntap-readModify: true
```

```

|onboard
|link:#onboard[onboard]
a|Configures onboard key management. After configuring onboard key
management, save the encrypted configuration data in a safe location so
that you can use it if you need to perform a manual recovery operation.

|policy
|string
a|Security policy associated with the key manager. This value is currently
ignored if specified for the onboard key manager.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===

```

```
|Name
|Type
|Description

|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= View security key managers

:leveloffset: +1

[[ID0203fb55a2157a58fd02ad0235ee9739]]
= Security key-managers security_key_manager.uuid keys node.uuid key-ids
endpoint overview


:doctype: book

== Overview

Retrieves the key manager keys on the give node. The following operations
are supported:

* GET

== Examples

=== Retrieving key manager key-id information for a node

The following example shows how to retrieve key-ids present on a node for
a key manager.

```

The API:

GET /api/security/key-manager/{security_key_manager.uuid}/keys/{node.uuid}/key-ids

The call:

```

curl -X GET 'https://<mgmt-ip>/api/f4f98a48-8a5c-c548-cd03-c6335f5803a8/keys/00000000-0000-0000-0000-000000000000/key-ids/0000000000000000000000000000000020000000000005009ad4da8fea2cafe2bed803078b780ebe00000000000000c01' -H

```


'accept: application/hal+json'</mgmt-ip>

The response:

```
{ "security_key_manager": { "uuid": "f4f98a48-8a5c-c548-cd03-c6335f5803a8" }, "node": { "uuid": "00000000-0000-0000-0000-000000000000" }, "key_id": "000000000000000000002000000000005009ad4da8fea2cafe2bed803078b780ebe0000000000000c01", "svm": { "name": "cluster-1" }, "key_tag": "4d82cc07-f9e0-114e-55dc-82a224bea631", "key_type": "vek", "restored": false, "key_store": "onboard", "key_user": "datavs", "key_manager": "onboard", "key_store_type": "okm", "encryption_algorithm": "XTS-AES-256", "_links": { "self": { "href": "/api/security/key-managers/f4f98a48-8a5c-c548-cd03-c6335f5803a8/keys/00000000-0000-0000-0000-000000000000/key-ids/000000000000000000002000000000005009ad4da8fea2cafe2bed803078b780ebe0000000000000c01" } } }
```

Retrieve key manager configurations

GET /security/key-managers/{security_key_manager.uuid}/keys/{node.uuid}/key-ids

Introduced In: 9.11

Retrieves key manager configurations.

Required properties

- security_key_manager.uuid - Key manager UUID.
- node.uuid - Node UUID.

Related ONTAP commands

- security key-manager key query

Parameters

Name	Type	In	Required	Description
security_key_manager.uuid	string	path	True	Key manager UUID.
node.uuid	string	path	True	Node UUID.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. <ul style="list-style-type: none">• Default value: 1

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

Response

Status: 200, Ok

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

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "crn": "CRN=vl:bluemix:public:containers-kubernetes",
    "encryption_algorithm": "XTS-AES-256",
    "key_id":
"000000000000000000000000000000001000000000000123456789asdfghjklqwertyuio12345678000000
00000000090",
    "key_manager": "keyserver1.local:5696",
    "key_server": "keyserver1.com:5698",
    "key_store": "onboard",
    "key_store_type": "okm",
    "key_tag": "key#",
    "key_type": "nse_ak",
    "key_user": "vs1",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "policy": "IBM_Key_Lore",
    "restored": 1
  }
}
```

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	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

key_manager_keys

Displays the keys stored in a key manager.

Name	Type	Description
_links	self_link	
crn	string	Cloud resource name.
encryption_algorithm	string	Encryption algorithm for the key
key_id	string	Key identifier.

Name	Type	Description
key_manager	string	Key manager key server managing the key. Indicates the external key server when external key manager is configured.
key_server	string	External key server for key management.
key_store	string	Security key manager configured for the given key manager UUID. Key manager keystore value can be onboard or external.
key_store_type	string	Security key manager keystore type. Keystore type can be onboard, external, or supported cloud key manager.
key_tag	string	Additional information associated with the key.
key_type	string	Encryption Key type.
key_user	string	SVM associated with the key.
node	node	
policy	string	Key store policy.
restored	boolean	Indicates whether the key is present locally on the node.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

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

Retrieve key management key information for specified keys

GET /security/key-managers/{security_key_manager.uuid}/keys/{node.uuid}/key-ids/{key_id}

Introduced In: 9.11

Retrieves the key management keys information for the specified key_id.

Related ONTAP commands

- `security key-manager key query -key-id <key_id>`

Parameters

Name	Type	In	Required	Description
security_key_manager.uuid	string	path	True	Key manager UUID.
node.uuid	string	path	True	Node UUID.
key_id	string	path	True	Key identifier.
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
_links	self_link	
crn	string	Cloud resource name.
encryption_algorithm	string	Encryption algorithm for the key

Name	Type	Description
key_id	string	Key identifier.
key_manager	string	Key manager key server managing the key. Indicates the external key server when external key manager is configured.
key_server	string	External key server for key management.
key_store	string	Security key manager configured for the given key manager UUID. Key manager keystore value can be onboard or external.
key_store_type	string	Security key manager keystore type. Keystore type can be onboard, external, or supported cloud key manager.
key_tag	string	Additional information associated with the key.
key_type	string	Encryption Key type.
key_user	string	SVM associated with the key.
node	node	
policy	string	Key store policy.
restored	boolean	Indicates whether the key is present locally on the node.

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "crn": "CRN=vl:bluemix:public:containers-kubernetes",
  "encryption_algorithm": "XTS-AES-256",
  "key_id":
  "000000000000000000100000000000123456789asdfghjklqwertyuio12345678000000
  0000000090",
  "key_manager": "keyserver1.local:5696",
  "key_server": "keyserver1.com:5698",
  "key_store": "onboard",
  "key_store_type": "okm",
  "key_tag": "key#",
  "key_type": "nse_ak",
  "key_user": "vs1",
  "node": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "policy": "IBM_Key_Lore",
  "restored": 1
}
```

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	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

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.

Migrate SVM keys between security key managers

POST /security/key-managers/{source.uuid}/migrate

Introduced In: 9.7

Migrates the keys belonging to an SVM between the cluster's key manager and the SVM's key manager. This operation can run for several minutes.

Required properties

- `source.uuid` - UUID of the source key manager.
- `uuid` - UUID of the destination key manager. The UUID of onboard and external KMIP key manager can be fetched using [GET /api/security/key-managers]. The UUID of Azure Key Vault key manager can be fetched using [GET /api/security/azure-key-vaults]. The UUID of Google Cloud key manager can be fetched using [GET /api/security/gcp-kms].

Related ONTAP commands

- `security key-manager migrate`

Parameters

Name	Type	In	Required	Description
source.uuid	string	path	True	Migration source key manager UUID

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value:

Request Body

Name	Type	Description
_links	_links	
uuid	string	Key manager UUID

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
}
```

Response

Status: 202, Accepted

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
```

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
65536886	The specified migration option is not supported in this release.
65536959	The source-uuid and UUID must be different values.
65536968	Check that all nodes of the cluster are healthy and retry the operation.
65537117	The migrate operation cannot be started because a UUID cannot be converted to an SVM name.
65537117	Cannot start migration because a key manager referenced by a provided UUID does not exist.
65537551	Top-level internal key protection key (KEK) is unavailable on one or more nodes.
65537552	Embedded KMIP server status is not available.
65537564	Check that the Azure Key Vault Service is healthy and retry the operation.
65537720	Failed to configure the Google Cloud Key Management Service for an SVM because a key manager is already configured.
65537736	Check that the Google Cloud Key Management Service is healthy and retry the operation.
65538107	Key migration to an IBM Key Lore key manager is not supported.

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	

info

Migration destination key manager UUID

Name	Type	Description
_links	_links	
uuid	string	Key manager UUID

job_link

Name	Type	Description
_links	_links	
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

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

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

List key servers configured in an external key manager

GET /security/key-managers/{uuid}/key-servers

Introduced In: 9.6

Retrieves the list of key servers configured in an external key manager.

Related ONTAP commands

- `security key-manager external show`
- `security key-manager external show-status`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	External key manager UUID
server	string	query	False	Filter by server
secondary_key_servers	string	query	False	Filter by secondary_key_servers <ul style="list-style-type: none"> • Introduced in: 9.8
timeout	integer	query	False	Filter by timeout <ul style="list-style-type: none"> • Max value: 60 • Min value: 1
username	string	query	False	Filter by username
fields	array[string]	query	False	Specify the fields to return.

Name	Type	In	Required	Description
max_records	integer	query	False	Limit the number of records returned.
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Max value: 120 • Min value: 0 • Default value: 1
return_records	boolean	query	False	<p>The default is true for GET calls. When set to false, only the number of records is returned.</p> <ul style="list-style-type: none"> • Default value: 1
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[key_server]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "password": "password",
    "records": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "password": "password",
      "server": "bulkkeyserver.com:5698",
      "timeout": 60,
      "username": "username"
    },
    "secondary_key_servers": [
      "secondary1.com",
      "10.1.2.3"
    ],
    "server": "keyserver1.com:5698",
    "timeout": 60,
    "username": "username"
  }
}
```

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	

records

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

key_server

Name	Type	Description
_links	_links	

Name	Type	Description
password	string	Password credentials for connecting with the key server. This is not audited.
records	array[records]	An array of key servers specified to add multiple key servers to a key manager in a single API call. Valid in POST only and not valid if <code>server</code> is provided.
secondary_key_servers	array[string]	A list of the secondary key servers associated with the primary key server.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

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

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

Add primary key servers to an external key manager

POST /security/key-managers/{uuid}/key-servers

Introduced In: 9.6

Adds primary key servers to a configured external key manager.

Required properties

- `uuid` - UUID of the external key manager.
- `server` - Primary Key server name.

Related ONTAP commands

- `security key-manager external add-servers`

Parameters

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

Request Body

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.

Name	Type	Description
records	array[records]	An array of key servers specified to add multiple key servers to a key manager in a single API call. Valid in POST only and not valid if <code>server</code> is provided.
secondary_key_servers	array[string]	A list of the secondary key servers associated with the primary key server.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "password": "password",
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "password": "password",
    "server": "bulkkeyserver.com:5698",
    "timeout": 60,
    "username": "username"
  },
  "secondary_key_servers": [
    "secondary1.com",
    "10.1.2.3"
  ],
  "server": "keyserver1.com:5698",
  "timeout": 60,
  "username": "username"
}
```

Response

Status: 201, Created

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

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "password": "password",
    "records": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "password": "password",
      "server": "bulkkeyserver.com:5698",
      "timeout": 60,
      "username": "username"
    },
    "secondary_key_servers": [
      "secondary1.com",
      "10.1.2.3"
    ],
    "server": "keyserver1.com:5698",
    "timeout": 60,
    "username": "username"
  }
}
```

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
65536038	A maximum of 4 active primary key servers are allowed.
65536042	Cannot add key server because it is already a secondary key server.
65536600	Cannot add a key server while a node is out quorum.
65536821	The certificate is not installed.
65536822	Multitenant key management is not supported in the current cluster version.
65536824	Multitenant key management is not supported in MetroCluster configurations.
65536828	External key management is not enabled for the SVM.
65536834	Failed to get existing key-server details for the SVM.
65536852	Failed to query supported KMIP protocol versions.
65536870	Key management servers are already configured.
65536871	Duplicate key management servers exist.
65536921	The following issues were found. Unable to execute command on KMIP server.
66060338	Unable to establish secure connection to KMIP server due to incorrect server_ca certificates.
66060339	Unable to establish secure connection to KMIP server due to incorrect client certificates.
66060340	Unable to establish secure connection to KMIP server due to Cryptsoft 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	

records

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

key_server

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.

Name	Type	Description
records	array[records]	An array of key servers specified to add multiple key servers to a key manager in a single API call. Valid in POST only and not valid if <code>server</code> is provided.
secondary_key_servers	array[string]	A list of the secondary key servers associated with the primary key server.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

`_links`

Name	Type	Description
next	href	
self	href	

`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

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

Delete a primary key server

DELETE /security/key-managers/{uuid}/key-servers/{server}

Introduced In: 9.6

Deletes a primary key server.

Optional parameters:

- **force** - Bypass Out of Quorum checks wehn deleting a primary key server. This flag is set to "false" by default.

Related ONTAP commands

- `security key-manager external remove-servers`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	External key manager UUID
server	string	path	True	Primary key server configured in the external key manager.
force	boolean	query	False	Set the force flag to "true" to bypass out of quorum checks when removing a primary key server. <ul style="list-style-type: none"> • Introduced in: 9.11 • Default value:

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
65536600	Cannot remove a key server while a node is out quorum.
65536700	The key server contains keys that are currently in use and not available from any other configured key server in the SVM.
65536822	Multitenant key management is not supported in the current cluster version.
65536824	Multitenant key management is not supported in MetroCluster configurations.
65536828	External key management is not enabled for the SVM.
65536843	The key management server is not configured for the SVM.

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 key servers configured in an external key manager

GET /security/key-managers/{uuid}/key-servers/{server}

Introduced In: 9.6

Retrieves key servers configured in an external key manager.

Related ONTAP commands

- `security key-manager external show`
- `security key-manager external show-status`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	External key manager UUID

Name	Type	In	Required	Description
server	string	path	True	Primary Key server configured in the key manager.
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.
records	array[records]	An array of key servers specified to add multiple key servers to a key manager in a single API call. Valid in POST only and not valid if <code>server</code> is provided.
secondary_key_servers	array[string]	A list of the secondary key servers associated with the primary key server.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "password": "password",
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "password": "password",
    "server": "bulkkeyserver.com:5698",
    "timeout": 60,
    "username": "username"
  },
  "secondary_key_servers": [
    "secondary1.com",
    "10.1.2.3"
  ],
  "server": "keyserver1.com:5698",
  "timeout": 60,
  "username": "username"
}
```

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	

records

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

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

Update a primary key server

PATCH /security/key-managers/{uuid}/key-servers/{server}

Introduced In: 9.6

Updates a primary key server.

Related ONTAP commands

- `security key-manager external modify-server`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	External key manager UUID
server	string	path	True	Primary key server configured in the external key manager.

Request Body

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.
records	array[records]	An array of key servers specified to add multiple key servers to a key manager in a single API call. Valid in POST only and not valid if <code>server</code> is provided.

Name	Type	Description
secondary_key_servers	array[string]	A list of the secondary key servers associated with the primary key server.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "password": "password",
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "password": "password",
    "server": "bulkkeyserver.com:5698",
    "timeout": 60,
    "username": "username"
  },
  "secondary_key_servers": [
    "secondary1.com",
    "10.1.2.3"
  ],
  "server": "keyserver1.com:5698",
  "timeout": 60,
  "username": "username"
}
```

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
65536600	Cannot modify a key server while a node is out quorum.

Error Code	Description
65536822	Multitenant key management is not supported in the current cluster version.
65536824	Multitenant key management is not supported in MetroCluster configurations.
65536828	External key management is not enabled for the SVM.
65536843	The key management server is not configured for the SVM.
65536845	Missing username.
65536846	Missing password.
65537400	Exceeded maximum number of secondary key servers.
65538407	A secondary key server is a duplicate of the associated primary key server.
65538408	The list of secondary key servers contains duplicates.
65538413	A secondary key server address is not formatted correctly.
65538502	A secondary key server is also a primary key server.
65538503	Support for adding secondary key servers requires an ECV of ONTAP 9.11.1 or later.

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	

records

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

key_server

Name	Type	Description
_links	_links	
password	string	Password credentials for connecting with the key server. This is not audited.

Name	Type	Description
records	array[records]	An array of key servers specified to add multiple key servers to a key manager in a single API call. Valid in POST only and not valid if <code>server</code> is provided.
secondary_key_servers	array[string]	A list of the secondary key servers associated with the primary key server.
server	string	External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if <code>records</code> is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	KMIP username credentials for connecting with the key server.

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.

View key stores

Security key-stores endpoint overview

Overview

A keystore describes a key-manager, specifically the type of key-manager.

Examples

Retrieving information for all configured key managers

The following example shows how to retrieve information about all configured key managers.

= The API:

```
GET /api/security/key-stores
```

= The call:

```
curl -X GET 'https://+++<mgmt-ip>+++/api/security/key-stores?fields=*' -H  
'accept: application/hal+json'+++</mgmt-ip>+++
```

= The response:

```
{  
  "records": [  
    {  
      "uuid": "33421d82-0a8d-11ec-ae88-005056bb5955",  
      "keystore": {  
        "type": "akv"  
      },  
      "_links": {  
        "self": {  
          "href": "/api/security/key-stores/33421d82-0a8d-11ec-ae88-  
005056bb5955/akv"  
        }  
      }  
    },  
    {  
      "uuid": "46a0b20a-0a8d-11ec-ae88-005056bb5955",  
      "keystore": {  
        "type": "okm"  
      },  
      "_links": {  
        "self": {  
          "href": "/api/security/key-stores/46a0b20a-0a8d-11ec-ae88-  

```

```
005056bb5955/okm"
    }
  }
},
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/security/key-stores"
  }
}
}
```

```
[[IDb4f463ef2c424f02dbe6c3e94f268917]]
= Retrieve keystores
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/key-stores`#
```

Introduced In: 9.10

Retrieves keystores.

== Expensive properties

There is an added cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter. See [xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Requesting_specific_fields\[Requesting specific fields\]](#) to learn more.

```
* `keystore.location`
* `svm.name`
* `svm.uuid`
```

== Related ONTAP commands

```
* `security key-manager show-key-store`
```

== Parameters

```
[cols=5*,options=header]
```

```

|===

|Name
|Type
|In
|Required
|Description

|svm.uuid
|string
|query
|False
a|Filter by svm.uuid


|svm.name
|string
|query
|False
a|Filter by svm.name


|location
|string
|query
|False
a|Filter by location


|type
|string
|query
|False
a|Filter by type


|uuid
|string
|query
|False
a|Filter by uuid


|fields
|array[string]
|query
|False

```


a|Specify the fields to return.

|max_records
|integer
|query
|False

a|Limit the number of records returned.

|return_timeout
|integer
|query
|False

a|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

|return_records
|boolean
|query
|False

a|The default is true for GET calls. When set to false, only the number of records is returned.

* Default value: 1

|order_by
|array[string]
|query
|False

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records.

|records
|array[link:#security_keystore[security_keystore]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "type": "okm",

```

```

    "uuid": "string"
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#security_keystore]
[.api-collapsible-fifth-title]
security_keystore

[cols=3*,options=header]
|===
|Name
|Type
|Description

|location
|string

```

```

a|Indicates whether the keystore is onboard or external.

|svm
|link:#svm[svm]
a|

|type
|string
a|Type of keystore that is configured: * 'okm' - Onboard Key Manager *
'kmip' - External Key Manager * 'akv' - Azure Key Vault Key Management
Service * 'gcp' - Google Cloud Platform Key Management Service * 'aws' -
Amazon Web Service Key Management Service

|uuid
|string
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]

```

```

error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====

:leveloffset: -1

= View and update login message configuration

:leveloffset: +1


[[ID6e6ecbb3a55cac17a146a5e0b7414a1d]]
= Security login messages endpoint overview

```

== Overview

You can use this API to display and manage the login messages configuration. The GET request retrieves all of the login messages in the cluster. GET operations on /security/login/messages/{uuid} retrieve the login messages configuration by UUID. PATCH operations on /security/login/messages/{uuid} update the login messages configuration by UUID.

+

'''

== Examples

=== Retrieving all of the login messages in the cluster

'''

The API:

/api/security/login/messages

The call:

```
curl -X GET "https://<mgmt-ip>/api/security/login/messages?fields=*" -H
"accept: application/hal+json"
```

The response:

```
{
  "records": [
    {
      "uuid": "2581e5aa-9fe3-11e8-b309-005056bbef18",
      "scope": "cluster",
      "banner": "*** WARNING: DO NOT PROCEED IF YOU ARE NOT AUTHORIZED!
****\n",
      "message": "#### Welcome to Cluster X ####\n",
      "show_cluster_message": true,
      "_links": {
        "self": {
          "href": "/api/security/login/messages/2581e5aa-9fe3-11e8-b309-
005056bbef18"
        }
      }
    },
  ],
}
```



```

    "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
    "scope": "svm",
    "svm": {
      "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
      "name": "svm1"
    },
    "message": "#### Welcome to SVM1 ####\n",
    "show_cluster_message": true,
    "_links": {
      "self": {
        "href": "/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-005056bbef18"
      }
    }
  },
  {
    "uuid": "8ddee11e-a58c-11e8-85e0-005056bbef18",
    "scope": "svm",
    "svm": {
      "uuid": "8ddee11e-a58c-11e8-85e0-005056bbef18",
      "name": "svm3"
    },
    "banner": "*** WARNING: This system is for the use of authorized users only. ***\n",
    "_links": {
      "self": {
        "href": "/api/security/login/messages/8ddee11e-a58c-11e8-85e0-005056bbef18"
      }
    }
  },
  {
    "uuid": "f7e41c99-9ffa-11e8-a5dd-005056bbef18",
    "scope": "svm",
    "svm": {
      "uuid": "f7e41c99-9ffa-11e8-a5dd-005056bbef18",
      "name": "svm2"
    },
    "_links": {
      "self": {
        "href": "/api/security/login/messages/f7e41c99-9ffa-11e8-a5dd-005056bbef18"
      }
    }
  }
],

```

```

"num_records": 4,
"_links": {
  "self": {
    "href": "/api/security/login/messages?fields=*"
  }
}
}
}
----

'''

=== Retrieving the login messages configuration at the cluster scope

'''

----

# The API:
/api/security/login/messages

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/login/messages?scope=cluster&fields=*" -H "accept:
application/hal+json"

# The response:
{
"records": [
  {
    "uuid": "2581e5aa-9fe3-11e8-b309-005056bbef18",
    "scope": "cluster",
    "banner": "*** WARNING: DO NOT PROCEED IF YOU ARE NOT AUTHORIZED!
****\n",
    "message": "#### Welcome to Cluster X ####\n",
    "show_cluster_message": true,
    "_links": {
      "self": {
        "href": "/api/security/login/messages/2581e5aa-9fe3-11e8-b309-
005056bbef18"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {

```

```

    "href": "/api/security/login/messages?scope=cluster&fields=*"
  }
}
}
----

'''

=== Retrieving the login banner configured at the cluster scope

'''

----

# The API:
/api/security/login/messages

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/login/messages?scope=cluster&fields=banner" -H "accept:
application/hal+json"

# The response:
{
  "records": [
    {
      "uuid": "2581e5aa-9fe3-11e8-b309-005056bbef18",
      "scope": "cluster",
      "banner": "*** WARNING: DO NOT PROCEED IF YOU ARE NOT AUTHORIZED!
***\n",
      "_links": {
        "self": {
          "href": "/api/security/login/messages/2581e5aa-9fe3-11e8-b309-
005056bbef18"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?scope=cluster&fields=banner"
    }
  }
}
----

```

```
'''

=== Retrieving the login messages configuration of a specific SVM

'''

----

# The API:
/api/security/login/messages

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/login/messages?svm.name=svm1&fields=*" -H "accept:
application/hal+json"

# The response:
{
"records": [
  {
    "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
    "scope": "svm",
    "svm": {
      "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
      "name": "svm1"
    },
    "message": "#### Welcome to SVM1 ####\n",
    "show_cluster_message": true,
    "_links": {
      "self": {
        "href": "/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-
005056bbef18"
      }
    }
  },
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?svm.name=svm1&fields=*"
    }
  }
}

----

'''
```

```
=== Retrieving the login messages configuration by UUID, including all fields
```

```
'''
```

```
----
```

```
# The API:
```

```
/api/security/login/messages/{uuid}
```

```
# The call:
```

```
curl -X GET "https://<mgmt-ip>/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-005056bbef18?fields=*" -H "accept: application/hal+json"
```

```
# The response:
```

```
{
"uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
"scope": "svm",
"svm": {
  "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
  "name": "svm1"
},
"message": "#### Welcome to SVM1 ####\n",
"show_cluster_message": true,
"_links": {
  "self": {
    "href": "/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-005056bbef18"
  }
}
}
```

```
----
```

```
'''
```

```
=== Configuring the login banner in a cluster
```

```
'''
```

```
----
```

```
# The API:
```

```
/api/security/login/messages
```

```
# The call:
```

```
curl -X PATCH "https://<mgmt-ip>/api/security/login/messages?scope=cluster" -H "accept:
```

```

application/hal+json" -H "Content-Type: appplication/json" -d "{
  \"banner\": \"You are entering secure area.\" }"

# The response:
{
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?scope=cluster"
    }
  }
}
}
-----

'''

=== Configuring the message of the day (MOTD) in a cluster

'''

-----

# The API:
/api/security/login/messages

# The call:
curl -X PATCH "https://<mgmt-
ip>/api/security/login/messages?scope=cluster" -H "accept:
application/hal+json" -H "Content-Type: appplication/json" -d "{
  \"message\": \"Welcome to Cluster X\",  \"show_cluster_message\": true }"

# The response:
{
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?scope=cluster"
    }
  }
}
}
-----

'''

=== Clearing the login banner and message of the day (MOTD) in a cluster

'''

```

The API:

/api/security/login/messages

The call:

```
curl -X PATCH "https://<mgmt-  
ip>/api/security/login/messages?scope=cluster" -H "accept:  
application/hal+json" -H "Content-Type: application/json" -d "{  
  \"banner\": \"\", \"message\": \"\" }"
```

The response:

```
{  
  "num_records": 1,  
  "_links": {  
    "self": {  
      "href": "/api/security/login/messages?scope=cluster"  
    }  
  }  
}
```

'''

=== Configuring the login messages for a specific SVM

'''

The API:

/api/security/login/messages

The call:

```
curl -X PATCH "https://<mgmt-  
ip>/api/security/login/messages?svm.name=svm1" -H "accept:  
application/hal+json" -H "Content-Type: application/json" -d "{  
  \"banner\" : \"AUTHORIZED ACCESS ONLY\", \"message\": \"WELCOME!\" }"
```

The response:

```
{  
  "num_records": 1,  
  "_links": {  
    "self": {  
      "href": "/api/security/login/messages?svm.name=svm1"  
    }  
  }  
}
```

```

}
}
----

'''

=== Configuring the login messages by UUID

'''

----

# The API:
/api/security/login/messages/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/login/messages/7b1b3715-
9ffa-11e8-a5dd-005056bbef18" -H "accept: application/hal+json" -H
"Content-Type: application/json" -d "{ \"banner\" : \"AUTHORIZED ACCESS
ONLY\", \"message\": \"WELCOME!\" }"
----

'''

=== Clearing the login messages configuration by UUID

'''

----

# The API:
/api/security/login/messages/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/login/messages/7b1b3715-
9ffa-11e8-a5dd-005056bbef18" -H "accept: application/hal+json" -H
"Content-Type: appplication/json" -d "{ \"banner\": \"\", \"message\":
\"\" }"
----

'''

[[ID240e364008c0799f71fb9254e069a4a2]]

```


= Retrieve login banner and messages of the day

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/login/messages`#
```

Introduced In: 9.6

Retrieves the login banner and messages of the day (MOTD) configured in the cluster and in specific SVMs.

== Parameters

```
[cols=5*,options=header]  
|==
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|uuid  
|string  
|query  
|False  
a|Filter by uuid
```

```
|message  
|string  
|query  
|False  
a|Filter by message
```

```
* maxLength: 2048  
* minLength: 0
```

```
|scope  
|string  
|query  
|False  
a|Filter by scope
```

```
|svm.uuid  
|string  
|query  
|False  
a|Filter by svm.uuid
```

```
|svm.name  
|string  
|query  
|False  
a|Filter by svm.name
```

```
|show_cluster_message  
|boolean  
|query  
|False  
a|Filter by show_cluster_message
```

```
|banner  
|string  
|query  
|False  
a|Filter by banner
```

```
* maxLength: 2048  
* minLength: 0
```

```
|fields  
|array[string]  
|query  
|False  
a|Specify the fields to return.
```

```
|max_records  
|integer  
|query  
|False  
a|Limit the number of records returned.
```

```
|return_timeout  
|integer
```

```
|query
|False
a|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

|return_records
|boolean
|query
|False
a|The default is true for GET calls.  When set to false, only the number
of records is returned.

* Default value: 1

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
```

```

|integer
a|Number of records

|records
|array[link:#login_messages[login_messages]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "scope": "svm",
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "string"
  }
}
=====

== Error

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

```

```

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#login_messages]
[.api-collapsible-fifth-title]
login_messages

The login banner and message of the day (MOTD) configuration.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|banner
|string

```

a|The login banner text. This message is displayed during SSH and console device login just before the password prompt displays. When configured, a cluster-level login banner is used for every incoming connection. Each data SVM can override the cluster-level banner to instead display when you log into the SVM. To restore the default setting for a data SVM, set the banner to an empty string. New lines are supplied as either LF or CRLF but are always returned as LF. Optional in the PATCH body.

|message
|string

a|The message of the day (MOTD). This message appears just before the clustershell prompt after a successful login. When configured, the cluster message displays first. If you log in as a data SVM administrator, the SVM message is then printed. The cluster-level MOTD can be disabled for a given data SVM using the "show_cluster_message" property. New lines are supplied as either LF or CRLF but are always returned as LF. Optional in the PATCH body.

|scope
|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|show_cluster_message
|boolean

a|Specifies whether to show a cluster-level message before the SVM message when logging in as an SVM administrator. This setting can only be modified by the cluster administrator. Optional in the PATCH body.

|svm
|link:#svm[svm]
a|

|uuid
|string

a|The unique identifier (ID) of the login messages configuration.

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

|===

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDf01ba01e47b4c75be5f16265cb958724]]
= Retrieve login message configuration by UUID

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/login/messages/{uuid}`#

*Introduced In:* 9.6

Retrieves the login messages configuration by UUID.

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|Login messages configuration UUID

```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|banner
|string
a|The login banner text. This message is displayed during SSH and console
device
login just before the password prompt displays. When configured, a
cluster-level
login banner is used for every incoming connection. Each data SVM can
override
the cluster-level banner to instead display when you log into the SVM. To
restore
the default setting for a data SVM, set the banner to an empty string.
New lines are supplied as either LF or CRLF but are always returned as LF.
Optional in the PATCH body.

|message
|string
a|The message of the day (MOTD). This message appears just before the
clustershell
prompt after a successful login. When configured, the cluster message
displays first. If you log in as a data SVM administrator, the
SVM message is then printed. The cluster-level MOTD can be disabled
for a given data SVM using the "show_cluster_message" property.
New lines are supplied as either LF or CRLF but are always returned as LF.
```

Optional in the PATCH body.

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|show_cluster_message
|boolean
a|Specifies whether to show a cluster-level message before the SVM message
when logging in as an SVM administrator.
This setting can only be modified by the cluster administrator.
Optional in the PATCH body.
```

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|The unique identifier (ID) of the login messages configuration.
```

```
|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
```

```

    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "string"
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

```

====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]

```

```

a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[IDa36d83f1fbfad5b76fe77be9671942e4]]
= Update a login message configuration
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/login/messages/{uuid}`#
```

***Introduced In:* 9.6**

Updates the login messages configuration.
There are no required fields. An empty body makes no modifications.

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
```



```

|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|Login messages configuration UUID

```

```

|===

```

```

== Request Body

```

```

[cols=3*,options=header]

```

```

|===

```

```

|Name
|Type
|Description

```

```

|_links
|link:#_links[_links]
a|

```

```

|banner
|string
a|The login banner text. This message is displayed during SSH and console
device
login just before the password prompt displays. When configured, a
cluster-level
login banner is used for every incoming connection. Each data SVM can
override
the cluster-level banner to instead display when you log into the SVM. To
restore
the default setting for a data SVM, set the banner to an empty string.
New lines are supplied as either LF or CRLF but are always returned as LF.
Optional in the PATCH body.

```

```

|message
|string
a|The message of the day (MOTD). This message appears just before the
clustershell
prompt after a successful login. When configured, the cluster message

```

displays first. If you log in as a data SVM administrator, the SVM message is then printed. The cluster-level MOTD can be disabled for a given data SVM using the "show_cluster_message" property. New lines are supplied as either LF or CRLF but are always returned as LF. Optional in the PATCH body.

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|show_cluster_message
|boolean
a|Specifies whether to show a cluster-level message before the SVM message
when logging in as an SVM administrator.
This setting can only be modified by the cluster administrator.
Optional in the PATCH body.
```

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|The unique identifier (ID) of the login messages configuration.
```

```
|===
```

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
```

```

        "href": "/api/resourcelink"
    },
    {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    {
        "uuid": "string"
    }
}
====

== Response

```

Status: 200, Ok

```

== Error

```

Status: Default

ONTAP Error Response codes

```

|===

```

Error codes	Description
-------------	-------------

10225636	
----------	--

Only a cluster administrator can modify the `show_cluster_message` property.
--

```

|===

```

```

[cols=3*,options=header]

```

```

|===

```

Name

Type

Description

error

link:#error[error]

a

```

|===

```

.Example error

[%collapsible%closed]

```

=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#login_messages]
[.api-collapsible-fifth-title]
login_messages

The login banner and message of the day (MOTD) configuration.

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|_links
|link:#_links[_links]
a|

|banner
|string
a|The login banner text. This message is displayed during SSH and console
device
login just before the password prompt displays. When configured, a
cluster-level
login banner is used for every incoming connection. Each data SVM can
override
the cluster-level banner to instead display when you log into the SVM. To
restore
the default setting for a data SVM, set the banner to an empty string.
New lines are supplied as either LF or CRLF but are always returned as LF.
Optional in the PATCH body.

|message
|string
a|The message of the day (MOTD). This message appears just before the
clustershell
prompt after a successful login. When configured, the cluster message
displays first. If you log in as a data SVM administrator, the
SVM message is then printed. The cluster-level MOTD can be disabled
for a given data SVM using the "show_cluster_message" property.
New lines are supplied as either LF or CRLF but are always returned as LF.
Optional in the PATCH body.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|show_cluster_message
|boolean
a|Specifies whether to show a cluster-level message before the SVM message
when logging in as an SVM administrator.
This setting can only be modified by the cluster administrator.
Optional in the PATCH body.

```

```

|svm
|link:#svm[svm]
a|

|uuid
|string
a|The unique identifier (ID) of the login messages configuration.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments

```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= Manage the multi-admin-verify global setting
```

```
:leveloffset: +1
```

```
[[ID56d0711e6039ffb47f9478b454a8d100]]
```

```
= Security multi-admin-verify endpoint overview
```

```
== Overview
```

These APIs provide information on the multi-admin verification global setting.

The GET API retrieves the object store that contains the global setting values of the multi-admin-verify feature.

The PATCH request is used to modify the multi-admin-verify global setting.

All fields are optional for the PATCH request.

+

'''

== Examples

=== Retrieving the multi-admin-verify global setting

Retrieves the current multi-admin-verify global setting. If the global setting is not set, default values are returned.

+

'''

The API:

/api/security/multi-admin-verify

The call:

curl -X GET "https://<cluster-ip>/api/security/multi-admin-verify"

The response:

```
{
  "approval_groups": [
  ],
  "required_approvers": 1,
  "enabled": false,
  "execution_expiry": "PT1H",
  "approval_expiry": "PT1H",
  "_links": {
    "self": {
      "href": "/api/security/multi-admin-verify"
    }
  }
}
```

'''

=== Updating the multi-admin-verify global setting

The following example updates the multi-admin-verify global settings. Note that the approval_groups needs to be available in /security/multi-admin-verify/approval-groups before it is set in the global setting.

+

```

'''

----

# The API:
/api/security/multi-admin-verify

# The call:
curl -X PATCH "https://<cluster-ip>/api/security/multi-admin-verify" -d
'{"required_approvers": "1", "enabled": "true", "execution_expiry": "2h",
"approval_expiry": "3h"}'
----

'''

[[ID6f33ca2e8a366d56ccb1751bbff34804]]
= Retrieve the multi-admin-verify configuration

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/multi-admin-verify`#

*Introduced In:* 9.11

Retrieves the multi-admin-verify configuration.

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|fields
|array[string]
|query
|False
|a|Specify the fields to return.

```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|approval_expiry
```

```
|string
```

```
a|Default time for requests to be approved, in ISO-8601 duration format.
```

```
|approval_groups
```

```
|array[string]
```

```
a|List of approval groups that are allowed to approve requests for rules  
that don't have approval groups.
```

```
|enabled
```

```
|boolean
```

```
a|
```

```
|execution_expiry
```

```
|string
```

```
a|Default time for requests to be executed once approved, in ISO-8601  
duration format.
```

```
|required_approvers
```

```
|integer
```

```
a|The number of required approvers, excluding the user that made the  
request.
```

```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
{
  "approval_groups": {
  }
}
====

== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
```

```

//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string

```

a|Error message

|target

|string

a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

====

[[IDfb853d16c8a033aabf18ac5c6f7b26ba]]

= Modify the multi-admin-verify configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-block]#`/security/multi-admin-verify`#

Introduced In: 9.11

Modifies the multi-admin-verify configuration.

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|approval_expiry

|string

a|Default time for requests to be approved, in ISO-8601 duration format.

|approval_groups

|array[string]

a|List of approval groups that are allowed to approve requests for rules that don't have approval groups.

```

|enabled
|boolean
a|

|execution_expiry
|string
a|Default time for requests to be executed once approved, in ISO-8601
duration format.

|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "approval_groups": {
  }
}
====

== Response

```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 262309
| The feature must be enabled first.

```

```

| 262311
| Value must be greater than zero.

| 262312
| Number of required approvers must be less than the total number of
unique approvers in the approval-groups.

| 262313
| Number of unique approvers in the approval-groups must be greater than
the number of required approvers.

| 262315
| Approval-groups must be specified when enabling this feature.

| 262316
| Value must be in the range one second to two weeks.

| 262318
| multi-admin-verify requires an effective cluster version of ONTAP 9.11.1
or later.
|===

```

```

[cols=3*,options=header]

```

```

|===

```

```

|Name

```

```

|Type

```

```

|Description

```

```

|error

```

```

|link:#error[error]

```

```

a|

```

```

|===

```

```

.Example error

```

```

[%collapsible%closed]

```

```

====

```

```

[source,json,subs=+macros]

```

```

{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    }
  }
}

```



```

    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#multi_admin_verify_config]
[.api-collapsible-fifth-title]
multi_admin_verify_config

[cols=3*,options=header]
|===
|Name
|Type
|Description

|approval_expiry
|string
a|Default time for requests to be approved, in ISO-8601 duration format.

|approval_groups
|array[string]
a|List of approval groups that are allowed to approve requests for rules
that don't have approval groups.

|enabled
|boolean
a|

|execution_expiry
|string
a|Default time for requests to be executed once approved, in ISO-8601
duration format.

|required_approvers

```

```

|integer
a|The number of required approvers, excluding the user that made the
request.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code

```

```

|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage multi-admin approval groups

:leveloffset: +1

[[ID05919e75f3ae4fdf2287ef9c9feaa7aa]]
= Security multi-admin-verify approval-groups endpoint overview

== Overview

A group of users can be defined in a cluster server context.
Approval groups can be associated with a rule or global setting from which
the associated request can retrieve approvals.
+
'''

== Examples

=== Creating a multi-admin-verify approval group

```

Creates an approval group for a specified SVM for a specified list of ONTAP users.

+

'''

The API:

/api/security/multi-admin-verify/approval-groups

The call:

```
curl -X POST "https://<mgmt-ip>/api/security/multi-admin-verify/approval-  
groups?return_records=true" -H "accept: application/hal+json" -d  
'{"owner.uuid": "c109634f-7011-11ec-a23d-005056a78fd5", "name": "group1",  
"approvers": ["admin"], "email": ["group1.approvers@email.com"]}'
```

The response:

```
{  
  "num_records": 1,  
  "records": [  
    {  
      "owner": {  
        "uuid": "c109634f-7011-11ec-a23d-005056a78fd5",  
        "_links": {  
          "self": {  
            "href": "/api/svm/svms/c109634f-7011-11ec-a23d-005056a78fd5"  
          }  
        }  
      },  
      "name": "group1",  
      "approvers": [  
        "admin"  
      ],  
      "email": [  
        "group1.approvers@email.com"  
      ],  
      "_links": {  
        "self": {  
          "href": "/api/security/multi-admin-verify/approval-  
groups/c109634f-7011-11ec-a23d-005056a78fd5/group1"  
        }  
      }  
    }  
  ]  
}
```

```

}
----

'''

=== Retrieving multi-admin-verify approval groups

Displays information about approval groups and the users that are
registered with each group.
+

'''

----

# The API:
/api/security/multi-admin-verify/approval-groups

# The call:
curl -X GET "https://<cluster-ip>/api/security/multi-admin-
verify/approval-groups"

# The response:
{
"records": [
  {
    "owner": {
      "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
        }
      }
    },
    "name": "group1",
    "_links": {
      "self": {
        "href": "/api/security/multi-admin-verify/approval-
groups/52b75787-7011-11ec-a23d-005056a78fd5/group1"
      }
    }
  }
],
"num_records": 1,
"_links": {

```

```

    "self": {
      "href": "/api/security/multi-admin-verify/approval-groups"
    }
  }
}
----

'''

[[IDf2d5721698cf9b6dd0193f85226f11ff]]
= Retrieve multi-admin-verify approval groups

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/multi-admin-verify/approval-groups`#

*Introduced In:* 9.11

Retrieves multi-admin-verify approval groups.

== Parameters

[cols=5*,options=header]
|==
|Name
|Type
|In
|Required
|Description

|approvers
|string
|query
|False
a|Filter by approvers

|owner.uuid
|string
|query
|False
a|Filter by owner.uuid

```

```
|owner.name
|string
|query
|False
a|Filter by owner.name
```

```
|email
|string
|query
|False
a|Filter by email
```

```
|name
|string
|query
|False
a|Filter by name
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|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
a|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
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#multi_admin_verify_approval_group[multi_admin_verify_approval_group]]
a|
```



```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "approvers": {
    },
    "email": {
    },
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}
```

```
====
```

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|next
|link:#href[href]
a|
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

The owner of the approval group. The only valid owner is currently the cluster.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#multi_admin_verify_approval_group]
[.api-collapsible-fifth-title]
multi_admin_verify_approval_group

[cols=3*,options=header]
|===
|Name
|Type
|Description

|approvers
|array[string]
a|List of users that can approve a request.

|email
|array[string]
a|Email addresses that are notified when a request is created, approved,
vetoed, or executed.

|name
|string
a|Name of the approval group.

```

```
|owner
|link:#owner[owner]
a|The owner of the approval group. The only valid owner is currently the
cluster.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID4dd93e6f70f89ed590ef956e7cdaf914]]
= Create a multi-admin-verify approval group

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/multi-admin-verify/approval-groups`#

*Introduced In:* 9.11

Creates a multi-admin-verify approval group.

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

```

```

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|approvers
|array[string]
a|List of users that can approve a request.

|email
|array[string]
a|Email addresses that are notified when a request is created, approved,
vetoed, or executed.

|name
|string
a|Name of the approval group.

|owner
|link:#owner[owner]
a|The owner of the approval group. The only valid owner is currently the
cluster.

|===

.Example request
[%collapsible%closed]

```

```

=====
[source,json,subs=+macros]
{
  "approvers": {
  },
  "email": {
  },
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
=====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#multi_admin_verify_approval_group[multi_admin_verify_approval_group]]
a|

|===

```



```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "approvers": {
    },
    "email": {
    },
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}
====

== Error
```

Status: Default

ONTAP Error Response Codes

```
|====
| Error Code | Description
|
| 262309
| The feature must be enabled first.
|====
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

The owner of the approval group. The only valid owner is currently the cluster.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```

|uuid
|string
a|The unique identifier of the SVM.

|===

[#multi_admin_verify_approval_group]
[.api-collapsible-fifth-title]
multi_admin_verify_approval_group

[cols=3*,options=header]
|===
|Name
|Type
|Description

|approvers
|array[string]
a|List of users that can approve a request.

|email
|array[string]
a|Email addresses that are notified when a request is created, approved,
vetoed, or executed.

|name
|string
a|Name of the approval group.

|owner
|link:#owner[owner]
a|The owner of the approval group. The only valid owner is currently the
cluster.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage multi-admin-verify approval groups

:leveloffset: +1

[[ID9c3781920e5331a99cb9ae954b7b1ab4]]
= Security multi-admin-verify approval-groups owner.uuid name endpoint
overview

== Overview

```

These APIs provide information about a specific multi-admin verification approval-group.

A group of users can be defined in a cluster server context.

Approval groups can be associated with a rule or global setting from which the associated request can retrieve approvals.

+

'''

== Examples

=== Retrieving a multi-admin-verify approval group

Displays information about a specific approval group and the users that are registered within that group.

+

'''

The API:

/api/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}

The call:

curl -X GET "https://<cluster-ip>/api/security/multi-admin-verify/approval-groups/52b75787-7011-11ec-a23d-005056a78fd5/group1"

The response:

```
{
  "owner": {
    "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
      }
    }
  },
  "name": "group1",
  "approvers": [
    "admin"
  ],
  "email": [
    "group1.approvers@email.com"
  ],
  "_links": {
```

```

    "self": {
        "href": "/api/security/multi-admin-verify/approval-groups/52b75787-
7011-11ec-a23d-005056a78fd5/group1"
    }
}
}
}
----

'''

=== Updating a multi-admin-verify approval group

Modifies attributes of an approval group.
+

'''

----

# The API:
/api/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}

# The call:
curl -X PATCH "https://<cluster-ip>/api/security/multi-admin-
verify/approval-groups/52b75787-7011-11ec-a23d-005056a78fd5/group1" -d
'{"approvers": ["admin1"], "email": ["group1.approvers.new@email.com"]}'
----

'''

=== Deleting a multi-admin-verify approval group

Deletes the specified approval group.
+

'''

----

# The API:
/api/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}

# The call:
curl -X DELETE "https://<cluster-ip>/api/security/multi-admin-
verify/approval-groups/52b75787-7011-11ec-a23d-005056a78fd5/group1"
----

```



```

[[ID60a3f8b44131cec60fd45d9ccb28351c]]
= Delete a multi-admin-verify approval group

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}`#

*Introduced In:* 9.11

Deletes a multi-admin-verify approval group.

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|owner.uuid
|string
|path
|True
a|

|name
|string
|path
|True
a|
|===

== Response

```

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```

|===

//end collapsible .Definitions block
=====

[[IDa9d0c22f71df9f860e62b3f310d0a1d7]]
= Retrieve a multi-admin-verify approval group

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}`#

*Introduced In:* 9.11

Retrieves a multi-admin-verify approval group.

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|owner.uuid
|string
|path
|True
a|

|name
|string
|path
|True
a|

|fields
|array[string]
|query

```

```
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|approvers
|array[string]
a|List of users that can approve a request.

|email
|array[string]
a|Email addresses that are notified when a request is created, approved,
vetoed, or executed.

|name
|string
a|Name of the approval group.

|owner
|link:#owner[owner]
a|The owner of the approval group. The only valid owner is currently the
cluster.

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "approvers": {
```

```

    },
    "email": {
    },
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

```

    }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#owner]
[.api-collapsible-fifth-title]

```

owner

The owner of the approval group. The only valid owner is currently the cluster.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#error_arguments]
```

```
[.api-collapsible-fifth-title]
```

```
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```



```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID086e36a9d6bf526de3f0944c74955a4b]]
= Update a multi-admin-verify approval group

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
```

```
block]#`/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}`#
```

Introduced In: 9.11

Updates a multi-admin-verify approval group.

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|owner.uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|
```

```
|name
```

```
|string
```

```
|path
```

```
|True
```

```
a|
```

```
|===
```

== Request Body

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|approvers
```

```
|array[string]
```

```
a|List of users that can approve a request.
```

```
|email
```

```
|array[string]
a|Email addresses that are notified when a request is created, approved,
vetoed, or executed.
```

```
|name
|string
a|Name of the approval group.
```

```
|owner
|link:#owner[owner]
a|The owner of the approval group. The only valid owner is currently the
cluster.
```

```
|===
```

```
.Example request
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
{
  "approvers": {
  },
  "email": {
  },
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

```
====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

ONTAP Error Response Codes

|===

| Error Code | Description

| 262331

| At least one approver is required.

| 262332

| An add or remove list is required.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

=====

[source,json,subs=+macros]

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

=====

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
====
```

```
[#href]
```

```
[.api-collapsible-fifth-title]
```

```
href
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|href
```

```
|string
```

```
a|
```

```
|===
```

```
[#_links]
```

```
[.api-collapsible-fifth-title]
```

```
_links
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|self
```

```
|link:#href[href]
```

```
a|
```

```
|===
```

```
[#owner]
```

```
[.api-collapsible-fifth-title]
```

```
owner
```

The owner of the approval group. The only valid owner is currently the cluster.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#multi_admin_verify_approval_group]
```

```
[.api-collapsible-fifth-title]
```

```
multi_admin_verify_approval_group
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|approvers
```

```
|array[string]
```

```
a|List of users that can approve a request.
```

```
|email
```

```
|array[string]
```

```
a|Email addresses that are notified when a request is created, approved,  
vetoed, or executed.
```

```
|name
```

```

|string
a|Name of the approval group.

|owner
|link:#owner[owner]
a|The owner of the approval group. The only valid owner is currently the
cluster.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments

```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= Manage multi-admin-verify approval requests
```

```
:leveloffset: +1
```

```
[[ID8075f94bc0bdd387ef47e1235863f8e0]]
```

```
= Security multi-admin-verify requests endpoint overview
```

```
== Overview
```

These APIs provide information about multi-admin verification requests.

If you need to execute a command that is protected by a multi-admin rule, you must first submit a request to be allowed to execute the command.

The request must then be approved by the designated approvers according to the rule associated with the command.


```

+

'''

== Examples

=== Creating a multi-admin-verify request

Creates a request for the specified ONTAP operation.
+

'''

----

# The API:
/api/security/multi-admin-verify/requests

# The call:
curl -X POST "https://<mgmt-ip>/api/security/multi-admin-
verify/requests?return_records=true" -H "accept: application/hal+json" -d
'{"operation": "volume delete", "query": "-vserver vs0 -volume v1",
"permitted_users": ["user1","user2"]}'

# The response:
{
  "num_records": 1,
  "records": [
    {
      "index": 10,
      "operation": "volume delete",
      "query": "-vserver vs0 -volume v1",
      "state": "pending",
      "required_approvers": 2,
      "pending_approvers": 2,
      "permitted_users": [
        "user1",
        "user2"
      ],
      "user_requested": "admin",
      "owner": {
        "uuid": "c1483186-6e73-11ec-bc92-005056a7ad04",
        "name": "cluster1",
        "_links": {
          "self": {
            "href": "/api/svm/svms/c1483186-6e73-11ec-bc92-005056a7ad04"

```

```

        }
    }
},
"create_time": "2022-01-06T16:59:49-05:00",
"approve_expiry_time": "2022-01-06T19:59:49-05:00",
"_links": {
    "self": {
        "href": "/api/security/multi-admin-verify/requests/10"
    }
}
}
]
}
----

'''

=== Retrieving multi-admin-verify requests

Retrieves information about multi-admin verification requests.
+

'''

----

# The API:
/api/security/multi-admin-verify/requests

# The call:
curl -X GET "https://<cluster-ip>/api/security/multi-admin-verify/requests"

# The response:
{
"records": [
    {
        "index": 1,
        "_links": {
            "self": {
                "href": "/api/security/multi-admin-verify/requests/1"
            }
        }
    },
    {
        "index": 2,

```

```

    "_links": {
      "self": {
        "href": "/api/security/multi-admin-verify/requests/2"
      }
    }
  },
  "num_records": 2,
  "_links": {
    "self": {
      "href": "/api/security/multi-admin-verify/requests"
    }
  }
}
----

'''

```

```

[[ID39c75331ac86cf918bdf909f305de49d]]
= Retrieve multi-admin-verify requests

```

```

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/multi-admin-verify/requests`#

```

Introduced In: 9.11

Retrieves multi-admin-verify requests.

== Parameters

```

[cols=5*,options=header]
|===

```

```

|Name
|Type
|In
|Required
|Description

|user_requested
|string
|query

```

```
|False
a|Filter by user_requested
```

```
|index
|integer
|query
|False
a|Filter by index
```

```
|approve_time
|string
|query
|False
a|Filter by approve_time
```

```
|approved_users
|string
|query
|False
a|Filter by approved_users
```

```
|owner.uuid
|string
|query
|False
a|Filter by owner.uuid
```

```
|owner.name
|string
|query
|False
a|Filter by owner.name
```

```
|state
|string
|query
|False
a|Filter by state
```

```
|potential_approvers
```

```
|string
|query
|False
a|Filter by potential_approvers
```

```
|user_vetoed
|string
|query
|False
a|Filter by user_vetoed
```

```
|query
|string
|query
|False
a|Filter by query
```

```
|create_time
|string
|query
|False
a|Filter by create_time
```

```
|pending_approvers
|integer
|query
|False
a|Filter by pending_approvers
```

```
|permitted_users
|string
|query
|False
a|Filter by permitted_users
```

```
|comment
|string
|query
|False
a|Filter by comment
```

```
|required_approvers
|integer
|query
|False
a|Filter by required_approvers
```

```
|operation
|string
|query
|False
a|Filter by operation
```

```
|execution_expiry_time
|string
|query
|False
a|Filter by execution_expiry_time
```

```
|approve_expiry_time
|string
|query
|False
a|Filter by approve_expiry_time
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
```

a|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

a|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

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

```
|records
|array[link:#multi_admin_verify_request[multi_admin_verify_request]]
a|
```

```
|===
```

.Example response

[%collapsible%closed]

```
=====
```

[source,json,subs=+macros]

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "approve_expiry_time": "string",
    "approve_time": "string",
    "approved_users": {
    },
    "comment": "string",
    "create_time": "string",
    "execution_expiry_time": "string",
    "index": 0,
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "pending_approvers": 0,
    "permitted_users": {
    },
    "potential_approvers": {
    },
    "required_approvers": 0,
```



```

    "state": "pending",
    "user_requested": "string",
    "user_vetoed": "string"
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]

```

```

//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|====
|Name
|Type
|Description

|href
|string
a|

|====

[#\_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|====

[#\_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name

```

```
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

The owner of the request. This can identify the cluster or an SVM.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#multi_admin_verify_request]
[.api-collapsible-fifth-title]
multi_admin_verify_request
```

```
[cols=3*,options=header]
|===
|Name
```

```

|Type
|Description

|approve_expiry_time
|string
a|

|approve_time
|string
a|

|approved_users
|array[string]
a|The users that have approved the request.

|comment
|string
a|Optional user-provided comment that is sent to the approval-group email
indicating why the request was made.

|create_time
|string
a|

|execution_expiry_time
|string
a|

|index
|integer
a|Unique index that represents a request.

|operation
|string
a|The command to execute.

|owner
|link:#owner[owner]
a|The owner of the request. This can identify the cluster or an SVM.

|pending_approvers
|integer

```

a|The number of approvers remaining that are required to approve.

|permitted_users

|array[string]

a|List of users that can execute the operation once approved. If not set, any authorized user can perform the operation.

|potential_approvers

|array[string]

a|The users that are able to approve the request.

|query

|string

a|Identifies the specific entry upon which the user wants to operate.

|required_approvers

|integer

a|The number of required approvers, excluding the user that made the request.

|state

|string

a|The state of the request. PATCH supports approved and vetoed. The state only changes after setting to approved once no more approvers are required.

|user_requested

|string

a|The user that created the request. Automatically set by ONTAP.

* readOnly: 1

* Introduced in: 9.11

|user_vetoed

|string

a|The user that vetoed the request.

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID70fd1da31a3dc8163804174a544505e4]]
= Create a multi-admin-verify request

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/multi-admin-verify/requests`#

*Introduced In:* 9.11

Creates a multi-admin-verify request.

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

* Default value:

|===

```

== Request Body

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|approve_expiry_time
|string
a|

|approve_time
|string
a|

|approved_users
|array[string]
a|The users that have approved the request.

|comment
|string
a|Optional user-provided comment that is sent to the approval-group email
indicating why the request was made.

|create_time
|string
a|

|execution_expiry_time
|string
a|

|index
|integer
a|Unique index that represents a request.

|operation
|string
a|The command to execute.
```



```

|owner
|link:#owner[owner]
a|The owner of the request. This can identify the cluster or an SVM.

|pending_approvers
|integer
a|The number of approvers remaining that are required to approve.

|permitted_users
|array[string]
a|List of users that can execute the operation once approved. If not set,
any authorized user can perform the operation.

|potential_approvers
|array[string]
a|The users that are able to approve the request.

|query
|string
a|Identifies the specific entry upon which the user wants to operate.

|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.

|state
|string
a|The state of the request. PATCH supports approved and vetoed. The state
only changes after setting to approved once no more approvers are
required.

|user_requested
|string
a|The user that created the request. Automatically set by ONTAP.

* readOnly: 1
* Introduced in: 9.11

```

```

|user_vetoed
|string
a|The user that vetoed the request.

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "approve_expiry_time": "string",
  "approve_time": "string",
  "approved_users": {
  },
  "comment": "string",
  "create_time": "string",
  "execution_expiry_time": "string",
  "index": 0,
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svml",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "pending_approvers": 0,
  "permitted_users": {
  },
  "potential_approvers": {
  },
  "required_approvers": 0,
  "state": "pending",
  "user_requested": "string",
  "user_vetoed": "string"
}
=====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#multi_admin_verify_request[multi_admin_verify_request]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "approve_expiry_time": "string",
    "approve_time": "string",
    "approved_users": {
    },
    "comment": "string",
    "create_time": "string",
    "execution_expiry_time": "string",
    "index": 0,
    "owner": {
      "_links": {

```

```

        "self": {
            "href": "/api/resourcelink"
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "pending_approvers": 0,
    "permitted_users": {
    },
    "potential_approvers": {
    },
    "required_approvers": 0,
    "state": "pending",
    "user_requested": "string",
    "user_vetoed": "string"
}
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

===	
Error Code	Description
262148	The specified command is not recognized.
262304	Too many requests. Delete one before creating another.
262305	Can't approve non-pending request.
262306	Can't veto an expired request.
262308	The specified command is not supported by this feature.
262309	The feature must be enabled first.

```

| 262311
| Value must be greater than zero.

| 262312
| Number of required approvers must be less than the total number of
unique approvers in the approval-groups.

| 262313
| Number of unique approvers in the approval-groups must be greater than
the number of required approvers.

| 262326
| Failed to parse query.

| 262327
| Failed to crate the request.

| 262328
| There is no matching rule for this request.

| 262330
| Cannot approve/veto a request multiple times.

| 262334
| The parameter specified in the command is not supported.

| 262337
| Cannot approve/veto the user's own request.
|===

```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

The owner of the request. This can identify the cluster or an SVM.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#multi_admin_verify_request]
[.api-collapsible-fifth-title]
multi_admin_verify_request
```

```
[cols=3*,options=header]
```

```
|===
```

```

|Name
|Type
|Description

|approve_expiry_time
|string
a|

|approve_time
|string
a|

|approved_users
|array[string]
a|The users that have approved the request.

|comment
|string
a|Optional user-provided comment that is sent to the approval-group email
indicating why the request was made.

|create_time
|string
a|

|execution_expiry_time
|string
a|

|index
|integer
a|Unique index that represents a request.

|operation
|string
a|The command to execute.

|owner
|link:#owner[owner]
a|The owner of the request. This can identify the cluster or an SVM.

|pending_approvers

```



```

|integer
a|The number of approvers remaining that are required to approve.

|permitted_users
|array[string]
a|List of users that can execute the operation once approved. If not set,
any authorized user can perform the operation.

|potential_approvers
|array[string]
a|The users that are able to approve the request.

|query
|string
a|Identifies the specific entry upon which the user wants to operate.

|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.

|state
|string
a|The state of the request. PATCH supports approved and vetoed. The state
only changes after setting to approved once no more approvers are
required.

|user_requested
|string
a|The user that created the request. Automatically set by ONTAP.

* readOnly: 1
* Introduced in: 9.11

|user_vetoed
|string
a|The user that vetoed the request.

|===

```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|next
|link:#href[href]
a|
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
```

```

[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage a multi-admin-verify approval request

:leveloffset: +1

[[ID8957bbb35d6af577fcff30af4acb53aa]]
= Security multi-admin-verify requests index endpoint overview

```

== Overview

These APIs provide information about a specific multi-admin verification request.

If you need to execute a command that is protected by a multi-admin rule, you must first submit a request to be allowed to execute the command. The request must then be approved by the designated approvers according to the rule associated with the command.

+

'''

== Examples

=== Retrieving a multi-admin-verify request

Retrieves information about a specific multi-admin verification request.

+

'''

The API:

/api/security/multi-admin-verify/requests/{index}

The call:

```
curl -X GET "https://<cluster-ip>/api/security/multi-admin-verify/requests/1"
```

The response:

```
{
  "index": 1,
  "operation": "security multi-admin-verify modify",
  "query": "",
  "state": "expired",
  "required_approvers": 1,
  "pending_approvers": 1,
  "permitted_users": [
    "wenbo"
  ],
  "user_requested": "admin",
  "owner": {
    "uuid": "c1483186-6e73-11ec-bc92-005056a7ad04",
```

```

    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/c1483186-6e73-11ec-bc92-005056a7ad04"
      }
    }
  },
  "create_time": "2022-01-05T20:07:09-05:00",
  "approve_expiry_time": "2022-01-05T21:07:09-05:00",
  "_links": {
    "self": {
      "href": "/api/security/multi-admin-verify/requests/1"
    }
  }
}
}
-----

'''

=== Updating a multi-admin-verify request

Updates a specific multi-admin-verify request
+

'''

-----

# The API:
/api/security/multi-admin-verify/requests/{index}

# The call:
curl -X PATCH "https://<cluster-ip>/api/security/multi-admin-verify/requests/1" -d '{"state": "approved"}'
-----

'''

[[ID1f6011eeb7ca242b5f6598de11902288]]
= Delete a multi-admin-verify request

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/security/multi-admin-verify/requests/{index}`#

```

Introduced In: 9.11

Deletes a multi-admin-verify request.

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|index

|string

|path

|True

a|

|==

== Response

Status: 200, Ok

== Error

Status: Default, Error

[cols=3*,options=header]

|==

|Name

|Type

|Description

|error

|link:#error[error]

a|

|==

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

```

```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID5890e96c97380096c5eb433ea22c78e5]]
= Retrieve a multi-admin-verify request

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/multi-admin-verify/requests/{index}`#

*Introduced In:* 9.11

Retrieves a multi-admin-verify request.

```



```
== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|index
|string
|path
|True
a|

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|approve_expiry_time
|string
a|

|approve_time
|string
a|

|approved_users
```

```

|array[string]
a|The users that have approved the request.

|comment
|string
a|Optional user-provided comment that is sent to the approval-group email
indicating why the request was made.

|create_time
|string
a|

|execution_expiry_time
|string
a|

|index
|integer
a|Unique index that represents a request.

|operation
|string
a|The command to execute.

|owner
|link:#owner[owner]
a|The owner of the request. This can identify the cluster or an SVM.

|pending_approvers
|integer
a|The number of approvers remaining that are required to approve.

|permitted_users
|array[string]
a|List of users that can execute the operation once approved. If not set,
any authorized user can perform the operation.

|potential_approvers
|array[string]
a|The users that are able to approve the request.

```

```
|query
|string
a|Identifies the specific entry upon which the user wants to operate.
```

```
|required_approvers
|integer
a|The number of required approvers, excluding the user that made the request.
```

```
|state
|string
a|The state of the request. PATCH supports approved and vetoed. The state only changes after setting to approved once no more approvers are required.
```

```
|user_requested
|string
a|The user that created the request. Automatically set by ONTAP.
```

```
* readOnly: 1
* Introduced in: 9.11
```

```
|user_vetoed
|string
a|The user that vetoed the request.
```

```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "approve_expiry_time": "string",
  "approve_time": "string",
  "approved_users": {
  },
  "comment": "string",
  "create_time": "string",
```

```

"execution_expiry_time": "string",
"index": 0,
"owner": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"pending_approvers": 0,
"permitted_users": {
},
"potential_approvers": {
},
"required_approvers": 0,
"state": "pending",
"user_requested": "string",
"user_vetoed": "string"
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{

```

```

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

```

====

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

====

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

|===

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|self
|link:href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

The owner of the request. This can identify the cluster or an SVM.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

```

====

[[ID5f028b87d2fd003db36c1565b21e6851]]

= Update a multi-admin-verify request

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-block]#`/security/multi-admin-verify/requests/{index}`#

Introduced In: 9.11

Updates a multi-admin-verify request.

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|index

|string

|path

|True

a|

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|approve_expiry_time

|string

a|


```

|approve_time
|string
a|

|approved_users
|array[string]
a|The users that have approved the request.

|comment
|string
a|Optional user-provided comment that is sent to the approval-group email
indicating why the request was made.

|create_time
|string
a|

|execution_expiry_time
|string
a|

|index
|integer
a|Unique index that represents a request.

|operation
|string
a|The command to execute.

|owner
|link:#owner[owner]
a|The owner of the request. This can identify the cluster or an SVM.

|pending_approvers
|integer
a|The number of approvers remaining that are required to approve.

|permitted_users
|array[string]
a|List of users that can execute the operation once approved. If not set,
any authorized user can perform the operation.

```

```

|potential_approvers
|array[string]
a|The users that are able to approve the request.

|query
|string
a|Identifies the specific entry upon which the user wants to operate.

|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.

|state
|string
a|The state of the request. PATCH supports approved and vetoed. The state
only changes after setting to approved once no more approvers are
required.

|user_requested
|string
a|The user that created the request. Automatically set by ONTAP.

* readOnly: 1
* Introduced in: 9.11

|user_vetoed
|string
a|The user that vetoed the request.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "approve_expiry_time": "string",

```

```

"approve_time": "string",
"approved_users": {
},
"comment": "string",
"create_time": "string",
"execution_expiry_time": "string",
"index": 0,
"owner": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"pending_approvers": 0,
"permitted_users": {
},
"potential_approvers": {
},
"required_approvers": 0,
"state": "pending",
"user_requested": "string",
"user_vetoed": "string"
}
====

== Response

```

Status: 200, Ok

```

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 262309
| The feature must be enabled first.
| 262329

```

```

| Invalid state for PATCH.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]

```

```
|===  
|Name  
|Type  
|Description
```

```
|href  
|string  
a|
```

```
|===
```

```
[#_links]  
[.api-collapsible-fifth-title]  
_links
```

```
[cols=3*,options=header]
```

```
|===  
|Name  
|Type  
|Description
```

```
|self  
|link:#href[href]  
a|
```

```
|===
```

```
[#owner]  
[.api-collapsible-fifth-title]  
owner
```

The owner of the request. This can identify the cluster or an SVM.

```
[cols=3*,options=header]
```

```
|===  
|Name  
|Type  
|Description
```

```
|_links  
|link:#_links[_links]  
a|
```

```
|name
```

```

|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#multi_admin_verify_request]
[.api-collapsible-fifth-title]
multi_admin_verify_request

[cols=3*,options=header]
|===
|Name
|Type
|Description

|approve_expiry_time
|string
a|

|approve_time
|string
a|

|approved_users
|array[string]
a|The users that have approved the request.

|comment
|string
a|Optional user-provided comment that is sent to the approval-group email
indicating why the request was made.

|create_time
|string
a|

|execution_expiry_time
|string

```

```

a|

|index
|integer
a|Unique index that represents a request.

|operation
|string
a|The command to execute.

|owner
|link:#owner[owner]
a|The owner of the request. This can identify the cluster or an SVM.

|pending_approvers
|integer
a|The number of approvers remaining that are required to approve.

|permitted_users
|array[string]
a|List of users that can execute the operation once approved. If not set,
any authorized user can perform the operation.

|potential_approvers
|array[string]
a|The users that are able to approve the request.

|query
|string
a|Identifies the specific entry upon which the user wants to operate.

|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.

|state
|string
a|The state of the request. PATCH supports approved and vetoed. The state

```

only changes after setting to approved once no more approvers are required.

|user_requested

|string

a|The user that created the request. Automatically set by ONTAP.

* readOnly: 1

* Introduced in: 9.11

|user_vetoed

|string

a|The user that vetoed the request.

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error


```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage multi-admin-verify rules

:leveloffset: +1

[[ID32c081e58b3d0a4441be20bfab050edc]]
= Security multi-admin-verify rules endpoint overview

```

== Overview

Rules define the ONTAP commands (operations) that should be protected by multi-admin approval.

While the feature is turned on, any ONTAP operation that is defined with a rule will be enforced with multi-admin approval to execute the command (operation).

+

'''

== Examples

=== Creating a multi-admin-verify rule

Creates a rule for the specified ONTAP operation.

+

'''

The API:

/api/security/multi-admin-verify/rules

The call:

```
curl -X POST "https://<mgmt-ip>/api/security/multi-admin-verify/rules?return_records=true" -H "accept: application/hal+json" -d '{"owner.uuid": "c109634f-7011-11ec-a23d-005056a78fd5", "operation": "volume delete", "query": "-vserver vs0", "required_approvers": 1}'
```

The response:

```
{
  "num_records": 1,
  "records": [
    {
      "owner": {
        "uuid": "c109634f-7011-11ec-a23d-005056a78fd5",
        "_links": {
          "self": {
            "href": "/api/svm/svms/c109634f-7011-11ec-a23d-005056a78fd5"
          }
        }
      },
      "operation": "volume delete",
      "auto_request_create": true,
      "query": "-vserver vs0",
```

```

    "required_approvers": 1,
    "create_time": "2022-01-07T22:14:03-05:00",
    "system_defined": false,
    "_links": {
      "self": {
        "href": "/api/security/multi-admin-verify/rules/c109634f-7011-11ec-a23d-005056a78fd5/volume%20delete"
      }
    }
  }
]
}
-----

'''

=== Retrieving multi-admin-verify rules

Displays information about multi admin verification rules.
+

'''

-----

# The API:
/api/security/multi-admin-verify/rules

# The call:
curl -X GET "https://<cluster-ip>/api/security/multi-admin-verify/rules"

# The response:
{
  "records": [
    {
      "owner": {
        "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
        "name": "cluster1",
        "_links": {
          "self": {
            "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
          }
        }
      },
      "operation": "security login password",
      "_links": {

```

```

    "self": {
      "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20login%20password"
    }
  },
  {
    "owner": {
      "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
        }
      }
    },
    "operation": "security login unlock",
    "_links": {
      "self": {
        "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20login%20unlock"
      }
    }
  },
  {
    "owner": {
      "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
        }
      }
    },
    "operation": "security multi-admin-verify approval-group create",
    "_links": {
      "self": {
        "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20multi-admin-verify%20approval-group%20create"
      }
    }
  },
  {
    "owner": {
      "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",

```

```

    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
      }
    }
  },
  "operation": "security multi-admin-verify approval-group delete",
  "_links": {
    "self": {
      "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20multi-admin-verify%20approval-group%20delete"
    }
  }
},
{
  "owner": {
    "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
      }
    }
  },
  "operation": "security multi-admin-verify approval-group modify",
  "_links": {
    "self": {
      "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20multi-admin-verify%20approval-group%20modify"
    }
  }
},
{
  "owner": {
    "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
      }
    }
  },
  "operation": "security multi-admin-verify approval-group replace",

```

```

    "_links": {
      "self": {
        "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20multi-admin-verify%20approval-group%20replace"
      }
    }
  },
  {
    "owner": {
      "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
        }
      }
    },
    "operation": "security multi-admin-verify modify",
    "_links": {
      "self": {
        "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20multi-admin-verify%20modify"
      }
    }
  },
  {
    "owner": {
      "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
        }
      }
    },
    "operation": "security multi-admin-verify rule create",
    "_links": {
      "self": {
        "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20multi-admin-verify%20rule%20create"
      }
    }
  },
  {
    "owner": {

```

```

    "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
      }
    }
  },
  "operation": "security multi-admin-verify rule delete",
  "_links": {
    "self": {
      "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20multi-admin-verify%20rule%20delete"
    }
  }
},
{
  "owner": {
    "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
      }
    }
  },
  "operation": "security multi-admin-verify rule modify",
  "_links": {
    "self": {
      "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/security%20multi-admin-verify%20rule%20modify"
    }
  }
},
{
  "owner": {
    "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
      }
    }
  },
  "operation": "volume delete",
  "_links": {

```

```

        "self": {
            "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/volume%20delete"
        }
    }
},
"num_records": 11,
"_links": {
    "self": {
        "href": "/api/security/multi-admin-verify/rules"
    }
}
}
}
----

'''

```

```

[[ID14908806f57e7d073f8774fc5cd2efd4]]
= Retrieve multi-admin-verify rules

```

```

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/multi-admin-verify/rules`#

```

Introduced In: 9.11

Retrieves multi-admin-verify rules.

== Parameters

```

[cols=5*,options=header]
|===

```

```

|Name
|Type
|In
|Required
|Description

|system_defined
|boolean
|query

```



```
|False
a|Filter by system_defined

|query
|string
|query
|False
a|Filter by query

|approval_groups.name
|string
|query
|False
a|Filter by approval_groups.name

|approval_expiry
|string
|query
|False
a|Filter by approval_expiry

|required_approvers
|integer
|query
|False
a|Filter by required_approvers

|execution_expiry
|string
|query
|False
a|Filter by execution_expiry

|operation
|string
|query
|False
a|Filter by operation

|create_time
```

```
|string
|query
|False
a|Filter by create_time
```

```
|auto_request_create
|boolean
|query
|False
a|Filter by auto_request_create
```

```
|owner.uuid
|string
|query
|False
a|Filter by owner.uuid
```

```
|owner.name
|string
|query
|False
a|Filter by owner.name
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|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

a|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

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

```

|records
|array[link:#multi_admin_verify_rule[multi_admin_verify_rule]]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "approval_groups": {
    },
    "create_time": "string",
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

```

```

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#approval_groups]
[.api-collapsible-fifth-title]
approval_groups

[cols=3*,options=header]
|===
|Name
|Type
|Description

|name
|string
a|Name of the approval group.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]

```

```

|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#owner]
[.api-collapsible-fifth-title]
owner

The owner of the rule. The only valid owner is currently the cluster.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#multi_admin_verify_rule]
[.api-collapsible-fifth-title]
multi_admin_verify_rule

[cols=3*,options=header]

```

```

|===
|Name
|Type
|Description

|approval_expiry
|string
a|Time for requests to be approved, in ISO-8601 duration format. If not
set, the global setting is used.

|approval_groups
|array[link:#approval_groups[approval_groups]]
a|List of approval groups that are allowed to approve requests for rules
that don't have approval groups.

|auto_request_create
|boolean
a|When true, ONTAP automatically creates a request for any failed
operation where there is no matching pending request.

* Default value:
* Introduced in: 9.11

|create_time
|string
a|

|execution_expiry
|string
a|Time for requests to be executed once approved, in ISO-8601 duration
format. If not set, the global setting is used.

|operation
|string
a|Command that requires one or more approvals.

|owner
|link:#owner[owner]
a|The owner of the rule. The only valid owner is currently the cluster.

|query

```



```
|string
a|When specified, this property limits the entries that require approvals
to those that match the specified query.
```

```
|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.
```

```
|system_defined
|boolean
a|Specifies whether the rule is system-defined or user-defined.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====


[[ID256f255d41d7ebdfff15f2e681e9715a]]
= Create a multi-admin-verify rule


[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/multi-admin-verify/rules`#


*Introduced In:* 9.11


Creates a multi-admin-verify rule.


== Parameters


[cols=5*,options=header]

```

```

|===

|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|approval_expiry
|string
a|Time for requests to be approved, in ISO-8601 duration format. If not
set, the global setting is used.

|approval_groups
|array[link:#approval_groups[approval_groups]]
a|List of approval groups that are allowed to approve requests for rules
that don't have approval groups.

|auto_request_create
|boolean
a|When true, ONTAP automatically creates a request for any failed
operation where there is no matching pending request.

* Default value: 1
* Introduced in: 9.11

```

```

|create_time
|string
a|

|execution_expiry
|string
a|Time for requests to be executed once approved, in ISO-8601 duration
format. If not set, the global setting is used.

|operation
|string
a|Command that requires one or more approvals.

|owner
|link:#owner[owner]
a|The owner of the rule. The only valid owner is currently the cluster.

|query
|string
a|When specified, this property limits the entries that require approvals
to those that match the specified query.

|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.

|system_defined
|boolean
a|Specifies whether the rule is system-defined or user-defined.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{

```

```

"approval_groups": {
},
"create_time": "string",
"owner": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
}
}
====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#multi_admin_verify_rule[multi_admin_verify_rule]]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{

```

```

    "_links": {
      "next": {
        "href": "/api/resourcelink"
      },
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "records": {
      "approval_groups": {
      },
      "create_time": "string",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  }
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

```

|====
| Error Code | Description
|
| 262148
| The specified command is not recognized.
|
| 262308
| The specified command is not supported by this feature.
|
| 262309
| The feature must be enabled first.
|
| 262311
| Value must be greater than zero.

```

```

| 262312
| Number of required approvers must be less than the total number of
unique approvers in the approval-groups.

| 262313
| Number of unique approvers in the approval-groups must be greater than
the number of required approvers.

| 262314
| Some approval-groups were not found.

| 262316
| Value must be in the range one second to two weeks.

| 262326
| Failed to parse query.

| 262335
| The query string must be contained in either the "operation" or "query"
parameters but not in both.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },

```

```

    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#approval_groups]
[.api-collapsible-fifth-title]
approval_groups

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|name
|string
a|Name of the approval group.

```

```

|===

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```



```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

The owner of the rule. The only valid owner is currently the cluster.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```

[#multi_admin_verify_rule]
[.api-collapsible-fifth-title]
multi_admin_verify_rule

[cols=3*,options=header]
|===
|Name
|Type
|Description

|approval_expiry
|string
a|Time for requests to be approved, in ISO-8601 duration format. If not
set, the global setting is used.

|approval_groups
|array[link:#approval_groups[approval_groups]]
a|List of approval groups that are allowed to approve requests for rules
that don't have approval groups.

|auto_request_create
|boolean
a|When true, ONTAP automatically creates a request for any failed
operation where there is no matching pending request.

* Default value: 1
* Introduced in: 9.11

|create_time
|string
a|

|execution_expiry
|string
a|Time for requests to be executed once approved, in ISO-8601 duration
format. If not set, the global setting is used.

|operation
|string
a|Command that requires one or more approvals.

```

```
|owner
|link:#owner[owner]
a|The owner of the rule. The only valid owner is currently the cluster.
```

```
|query
|string
a|When specified, this property limits the entries that require approvals
to those that match the specified query.
```

```
|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.
```

```
|system_defined
|boolean
a|Specifies whether the rule is system-defined or user-defined.
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|next
|link:#href[href]
a|
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

:leveloffset: -1

= Manage a multi-admin-verify rule

:leveloffset: +1

[[ID330ae64e4fbc7a42522ccd705664fb99]]
= Security multi-admin-verify rules owner.uuid operation endpoint overview

== Overview

These APIs provide information about a specific multi-admin verification
rule.
Rules define the ONTAP commands (operations) that should be protected by
multi-admin approval.
While the feature is turned on, any ONTAP operation that is defined with a
rule will be enforced with multi-admin approval to execute the command
(operation).
+
'''

== Examples

=== Retrieving a multi-admin-verify rule

Displays information about a specific multi admin verification rule.
+

```

```
'''
----

# The API:
/api/security/multi-admin-verify/rules/{owner.uuid}/{operation}

# The call:
curl -X GET "https://<cluster-ip>/api/security/multi-admin-
verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/volume+delete"

# The response:
{
  "owner": {
    "uuid": "52b75787-7011-11ec-a23d-005056a78fd5",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/52b75787-7011-11ec-a23d-005056a78fd5"
      }
    }
  },
  "operation": "volume delete",
  "auto_request_create": true,
  "query": "-vserver vs0",
  "required_approvers": 1,
  "create_time": "2022-01-07T22:14:03-05:00",
  "system_defined": false,
  "_links": {
    "self": {
      "href": "/api/security/multi-admin-verify/rules/52b75787-7011-11ec-
a23d-005056a78fd5/volume+delete"
    }
  }
}
}
----

'''

=== Updating a multi-admin-verify rule

Modifies the attributes of the rule.
+

'''
```

```

-----

# The API:
/api/security/multi-admin-verify/rules/{owner.uuid}/{operation}

# The call:
curl -X PATCH "https://<cluster-ip>/api/security/multi-admin-
verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/volume+delete" -d
'{"required_approvers": 1}'
-----

'''

=== Deleting a multi-admin-verify rule

Deletes the specified approval group.
+

'''

-----

# The API:
/api/security/multi-admin-verify/rules/{owner.uuid}/{operation}

# The call:
curl -X DELETE "https://<cluster-ip>/api/security/multi-admin-
verify/rules/52b75787-7011-11ec-a23d-005056a78fd5/volume+delete"
-----

'''

[[ID8e5e35842b09fb76750e3e1c1196cb20]]
= Delete a multi-admin-verify rule

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/multi-admin-verify/rules/{owner.uuid}/{operation}`#

*Introduced In:* 9.11

Deletes a multi-admin-verify rule.

```

```

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|owner.uuid
|string
|path
|True
a|

|operation
|string
|path
|True
a|
|===

== Response

```

Status: 200, Ok

```

== Error

```

Status: Default

```

ONTAP Error Response Codes

|===
| Error Code | Description

| 262310
| System rules cannot be deleted or have their query modified.
|===

[cols=3*,options=header]
|===

```



```

|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code

```

```

|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
[[ID217333532c7dbe540d80ec6ba291ec06]]
```

= Retrieve a multi-admin-verify rule

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/multi-admin-verify/rules/{owner.uuid}/{operation}`#
```

Introduced In: 9.11

Retrieves a multi-admin-verify rule.

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|owner.uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|
```

```
|operation
```

```
|string
```

```
|path
```

```
|True
```

```
a|
```

```
|fields
```

```
|array[string]
```

```
|query
```

```
|False
```

```
a|Specify the fields to return.
```

```
|===
```

== Response

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|approval_expiry
|string
a|Time for requests to be approved, in ISO-8601 duration format. If not
set, the global setting is used.

|approval_groups
|array[link:#approval_groups[approval_groups]]
a|List of approval groups that are allowed to approve requests for rules
that don't have approval groups.

|auto_request_create
|boolean
a|When true, ONTAP automatically creates a request for any failed
operation where there is no matching pending request.

* Default value: 1
* Introduced in: 9.11

|create_time
|string
a|

|execution_expiry
|string
a|Time for requests to be executed once approved, in ISO-8601 duration
format. If not set, the global setting is used.

|operation
|string
a|Command that requires one or more approvals.

|owner
|link:#owner[owner]
```

a|The owner of the rule. The only valid owner is currently the cluster.

|query

|string

a|When specified, this property limits the entries that require approvals to those that match the specified query.

|required_approvers

|integer

a|The number of required approvers, excluding the user that made the request.

|system_defined

|boolean

a|Specifies whether the rule is system-defined or user-defined.

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "approval_groups": {
  },
  "create_time": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

====

== Error

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#approval_groups]
[.api-collapsible-fifth-title]
approval_groups

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|name
|string
a|Name of the approval group.
```

```
|===
```

```
[#href]
[.api-collapsible-fifth-title]
href
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|href
|string
a|
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

The owner of the rule. The only valid owner is currently the cluster.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#error_arguments]
```

```
[.api-collapsible-fifth-title]
```

```
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```



```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDda2f6d178e3bd8f98ee0ba9f43fb6113]]
= Update a multi-admin-verify rule

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/multi-admin-verify/rules/{owner.uuid}/{operation}`#

*Introduced In:* 9.11

```

Updates a multi-admin-verify rule.

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```

```
|owner.uuid
|string
|path
|True
a|
```

```
|operation
|string
|path
|True
a|
|===
```

== Request Body

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|approval_expiry
|string
a|Time for requests to be approved, in ISO-8601 duration format. If not
set, the global setting is used.
```

```
|approval_groups
|array[link:#approval_groups[approval_groups]]
a|List of approval groups that are allowed to approve requests for rules
```

that don't have approval groups.

|auto_request_create

|boolean

a|When true, ONTAP automatically creates a request for any failed operation where there is no matching pending request.

* Default value: 1

* Introduced in: 9.11

|create_time

|string

a|

|execution_expiry

|string

a|Time for requests to be executed once approved, in ISO-8601 duration format. If not set, the global setting is used.

|operation

|string

a|Command that requires one or more approvals.

|owner

|link:#owner[owner]

a|The owner of the rule. The only valid owner is currently the cluster.

|query

|string

a|When specified, this property limits the entries that require approvals to those that match the specified query.

|required_approvers

|integer

a|The number of required approvers, excluding the user that made the request.

|system_defined

|boolean

a|Specifies whether the rule is system-defined or user-defined.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "approval_groups": {
  },
  "create_time": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

====

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 262310

| System rules cannot be deleted or have their query modified.

| 262311

| Value must be greater than zero.

| 262312

```
| Number of required approvers must be less than the total number of  
unique approvers in the approval-groups.
```

```
| 262313
```

```
| Number of unique approvers in the approval-groups must be greater than  
the number of required approvers.
```

```
| 262316
```

```
| Value must be in the range one second to two weeks.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

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

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```

[%collapsible%closed]
//Start collapsible Definitions block
====
[#approval_groups]
[.api-collapsible-fifth-title]
approval_groups

[cols=3*,options=header]
|===
|Name
|Type
|Description

|name
|string
a|Name of the approval group.

|===

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

The owner of the rule. The only valid owner is currently the cluster.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#multi_admin_verify_rule]
[.api-collapsible-fifth-title]
multi_admin_verify_rule
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```

|approval_expiry
|string
a|Time for requests to be approved, in ISO-8601 duration format. If not
set, the global setting is used.

|approval_groups
|array[link:#approval_groups[approval_groups]]
a|List of approval groups that are allowed to approve requests for rules
that don't have approval groups.

|auto_request_create
|boolean
a|When true, ONTAP automatically creates a request for any failed
operation where there is no matching pending request.

* Default value: 1
* Introduced in: 9.11

|create_time
|string
a|

|execution_expiry
|string
a|Time for requests to be executed once approved, in ISO-8601 duration
format. If not set, the global setting is used.

|operation
|string
a|Command that requires one or more approvals.

|owner
|link:#owner[owner]
a|The owner of the rule. The only valid owner is currently the cluster.

|query
|string
a|When specified, this property limits the entries that require approvals
to those that match the specified query.

```



```
|required_approvers
|integer
a|The number of required approvers, excluding the user that made the
request.
```

```
|system_defined
|boolean
a|Specifies whether the rule is system-defined or user-defined.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
:leveloffset: -1
```

```
= Manage security roles
```

```
:leveloffset: +1
```

```
[[IDef056dfb27d741dd872b68a7a0c3609c]]
= 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 `_api/storage/volumes/{volume.uuid}/snapshots_` and `_api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" 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/application/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/application/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

`_/_api/storage/volumes/{volume.uuid}/snapshots_ and`

`_/_api/storage/volumes/*/snapshots_. "*" is a wildcard character denoting "all" volumes.`

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/6519986e-7752-11eb-8d4e-

0050568ed6bd/snapshots"}, {"access":"readonly","path":"/api/application/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?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%2F738e3c9f-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%2Fe621583b-f445-4713-ba9e-a052d53c8a83%2Fsnapshots"
            }
        }
    }
],
"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": "svml",
        "_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": 8,
  "_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"
```

[[ID1bf9ec65f876779589db33905dc88248]]

= Retrieve a list of roles configured in the cluster

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/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

* xref:{relative_path}security_roles_endpoint_overview.html[DOC

```
/security/roles]
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|comment
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by comment
```

```
* Introduced in: 9.11
```

```
|privileges.path
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by privileges.path
```

```
* Introduced in: 9.7
```

```
|privileges.query
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by privileges.query
```

```
* Introduced in: 9.11
```

```
|privileges.access
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by privileges.access
```

* Introduced in: 9.7

|name
|string
|query
|False
a|Filter by name

* Introduced in: 9.7

|builtin
|boolean
|query
|False
a|Filter by builtin

* Introduced in: 9.7

|owner.uuid
|string
|query
|False
a|Filter by owner.uuid

* Introduced in: 9.7

|owner.name
|string
|query
|False
a|Filter by owner.name

* Introduced in: 9.7

|scope
|string
|query
|False
a|Filter by scope

* Introduced in: 9.7


```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|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
a|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
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.
```

```
|===
```

== Response

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|num_records
|integer
a|Number of records
```

```
|records
|array[link:#role[role]]
a|
```

```
|===
```

.Example response

[%collapsible%closed]

=====

[source,json,subs=+macros]

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
}
```

```

"comment": "string",
"name": "admin",
"owner": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svml",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"privileges": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access": "readonly",
  "path": [
    "/api/cluster/jobs",
    "/api/storage/volumes",
    "job schedule interval",
    "volume move"
  ],
  "query": [
    "-days <1 -hours >12",
    "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
  ]
},
"scope": "cluster"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error

```

```

|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|next
|link:href[href]
a|
```

```
|self
|link:href[href]
a|
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the role.

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role_privilege]
[.api-collapsible-fifth-title]
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 `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|access
|string
```

a|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

a|Either of REST URI/endpoint OR command/command directory path.

|query

|string

a|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]

[.api-collapsible-fifth-title]

role

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

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|builtin

|boolean

a|Indicates if this is a built-in (pre-defined) role which cannot be modified or deleted.

```

|comment
|string
a|Comment

|name
|string
a|Role name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the role.

|privileges
|array[link:#role_privilege[role_privilege]]
a|The list of privileges that this role has been granted.

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message

```



```

|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID700dc4528ed063ac14bfd60565e77ae9]]
= Create a new cluster-scoped or SVM-scoped role

```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-block]#`/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

- * xref:{relative_path}security_roles_endpoint_overview.html[DOC /security/roles]

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|builtin
|boolean
a|Indicates if this is a built-in (pre-defined) role which cannot be
modified or deleted.

|comment
|string
a|Comment

|name
|string
a|Role name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the role.

|privileges
|array[link:#role_privilege[role_privilege]]

```

a|The list of privileges that this role has been granted.

|scope

|string

a|Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "comment": "string",
  "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/cluster/jobs",
      "/api/storage/volumes",
      "job schedule interval",
      "volume move"
    ],
  },
}
```

```

    "query": [
        "-days <1 -hours >12",
        "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
    ]
},
"scope": "cluster"
}
====

== Response

```

Status: 201, Created

```

== Error

```

Status: Default

ONTAP Error Response Codes

```

|====
| Error Code | Description

| 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.

| 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.

| 13434890
| Vserver-ID failed for Vserver roles.

| 13434891
| UUID lookup failed for Vserver roles.

| 13434892
| Roles is a required field.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

```

    }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#owner]
[.api-collapsible-fifth-title]

```

owner

Owner name and UUID that uniquely identifies the role.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role_privilege]
```

```
[.api-collapsible-fifth-title]
```

```
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 `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. `"*"` is a wildcard character denoting "all" volumes.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```



```
|_links
|link:#_links[_links]
a|
```

```
|access
|string
a|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
a|Either of REST URI/endpoint OR command/command directory path.
```

```
|query
|string
a|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]
[.api-collapsible-fifth-title]
role
```

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

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
```

```

|link:#_links[_links]
a|

|builtin
|boolean
a|Indicates if this is a built-in (pre-defined) role which cannot be
modified or deleted.

|comment
|string
a|Comment

|name
|string
a|Role name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the role.

|privileges
|array[link:#role_privilege[role_privilege]]
a|The list of privileges that this role has been granted.

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= View or delete a role
```

```
:leveloffset: +1
```

```
[[ID2aef50d83c9867f485d64359acaa1d38]]
```

```
= 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.

NOTE: 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": "svml",
    "_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"
        }
      }
    }
  ],
  "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": "svml",
    "_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"
----

[[ID3d033ac7524e9c65445ab16c2d6fba6d]]
= Delete a role

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/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

*
xref:{relative_path}security_roles_owner.uuid_name_endpoint_overview.html[
DOC /security/roles/{owner.uuid}/{name}]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]

== Parameters

[cols=5*,options=header]
|===

Name
Type
In
Required
Description

owner.uuid
string
path
True
a Role owner UUID

name
string
path
True
a Role name to be deleted.

|===

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 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.  
|===
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

```

```
//end collapsible .Definitions block
====
```

```
[[ID92319377fecae83e68e6fffbcef9a0c2a]]
= Retrieve the details of a role
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/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

```
*
xref:{relative_path}security_roles_owner.uuid_name_endpoint_overview.html[
DOC /security/roles/{owner.uuid}/{name}]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]
```

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```

```
|owner.uuid
|string
|path
|True
a|Role owner UUID
```

```

|name
|string
|path
|True
a|Role name

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|builtin
|boolean
a|Indicates if this is a built-in (pre-defined) role which cannot be
modified or deleted.

|comment
|string
a|Comment

|name
|string
a|Role name

```

```

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the role.

|privileges
|array[link:#role_privilege[role_privilege]]
a|The list of privileges that this role has been granted.

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

```

```
|===
```

```

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "comment": "string",
  "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/cluster/jobs",
        "/api/storage/volumes",
        "job schedule interval",
        "volume move"
    ],
    "query": [
        "-days <1 -hours >12",
        "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
    ]
},
"scope": "cluster"
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",

```

```

    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```



```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the role.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role_privilege]
[.api-collapsible-fifth-title]
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 `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. `"*"` is a wildcard character denoting "all" volumes.

```
[cols=3*,options=header]
|===
|Name
```

```

|Type
|Description

|_links
|link:#_links[_links]
a|

|access
|string
a|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
a|Either of REST URI/endpoint OR command/command directory path.

|query
|string
a|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]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
:leveloffset: -1
```

```
= Manage role privilege details
```

```
:leveloffset: +1
```

```
[[ID2b44a4f80ed9f08034350829849b6d50]]
```

```
= Security roles owner.uuid name privileges endpoint overview
```

```
== Overview
```

This API is used to configure the role privileges (tuples of REST URI paths or command/command directory paths, their access levels and optional queries, where the tuples refer to command/command directory paths). It also retrieves all of the privilege tuples for a role and can add a tuple to an existing role. The "path" attribute can be a resource-qualified endpoint. Currently, the only supported resource-qualified endpoints are `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

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

Specify the owner UUID and the role name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the role has been created and can be obtained from the response body of a GET request performed on one of the following APIs:

`_/api/security/roles_` for all the roles

`_/api/security/roles/?scope=svm_` for SVM-scoped roles

`_/api/security/roles/?owner.name=+++<svm-name>+++</i>` for roles in a specific SVM This API response contains the complete URI for each role and can be used after suffixing it with `_"privileges"_.+++</svm-name>+++_`

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

```
== Examples
```

```
=== Adding a privilege tuple for a REST URI/endpoint to an existing custom role
```

```
----
```

```

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

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

=== Adding a privilege tuple for a command or command directory to an
existing custom role

----

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_role1/privileges" -d
'{"access":"all","path":"statistics volume show","query":"-vserver
vs1&#124;vs2 -aggregate aggr1&#124;aggr2"}'
----

=== Retrieving all the privilege tuples for a REST role

----

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

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

# The response:
{
  "records": [
    {
      "path": "/api/application",
      "access": "all",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/svm_role1/privileges/%2Fapi%2Fapplication"
        }
      }
    }
  ]
}

```

```

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

```

=== Retrieving all the privilege tuples for a custom legacy role

The API:

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

The call:

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

The response:

```

{
  "records": [
    {
      "path": "network interface",
      "access": "readonly",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/network%20interface"
        }
      }
    },
    {
      "path": "security",
      "access": "readonly",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/security"
        }
      }
    },
    {
      "path": "security certificate",
      "access": "all",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/security%20certificate"
        }
      }
    },
    {
      "path": "security password",
      "access": "all",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/security%20password"
        }
      }
    }
  ],
  "num_records": 4,
  "_links": {
    "self": {

```

```
"href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges"
    }
}
}
----
```

```
[[ID7e1cccc7398dc7397e97ad37004638fd]]
= Retrieve privilege details of the specified role
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/roles/{owner.uuid}/{name}/privileges`#
```

Introduced In: 9.6

Retrieves privilege details of the specified role.

== Related ONTAP commands

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

== Learn more

```
*
xref:{relative_path}security_roles_owner.uuid_name_privileges_endpoint_ove
rview.html[DOC /security/roles/{owner.uuid}/{name}/privileges]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]
```

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description

|owner.uuid
```



```
|string
|path
|True
a|Role owner UUID
```

```
|name
|string
|path
|True
a|Role name
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|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
a|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

a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|num_records

|integer

a|Number of records

|records

|array[link:#role_privilege[role_privilege]]

a|

|===

.Example response

[%collapsible%closed]

=====

[source,json,subs=+macros]

{

 "_links": {

 "next": {

```

    "href": "/api/resourcelink"
  },
  "self": {
    "href": "/api/resourcelink"
  }
},
"records": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access": "readonly",
  "path": [
    "/api/cluster/jobs",
    "/api/storage/volumes",
    "job schedule interval",
    "volume move"
  ],
  "query": [
    "-days <1 -hours >12",
    "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
  ]
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error

```

```

[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===

```

```
|Name
|Type
|Description

|next
|link:#href[href]
a|
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
```

```
|===
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#role_privilege]
[.api-collapsible-fifth-title]
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 `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|access
|string
a|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
a|Either of REST URI/endpoint OR command/command directory path.

|query
|string
a|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]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code

```

```

|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
[[ID3f72168431745d09e57bfc59cf31ac7b]]
```

= Add a privilege tuple to an existing role

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/roles/{owner.uuid}/{name}/privileges`#
```

Introduced In: 9.6

Adds a privilege tuple (of REST URI or command/command directory path, its access level and an optional query, if the "path" refers to a command/command directory path) to an existing role.

== Required parameters

* `owner.uuid` - UUID of the SVM that houses this role.

* `name` - Name of the role to be updated.

* `path` - REST URI path (example: `_/api/storage/volumes_`) or command/command directory path (example: `_snaplock compliance-clock_`). Can be a resource-qualified endpoint (example: `_/api/storage/volumes/43256a71-be02-474d-a2a9-9642e12a6a2c/snapshots_`). Currently, resource-qualified endpoints are limited to the "snapshots" endpoint: `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

* `access` - Desired access level for the REST URI path or command/command directory.

== Related ONTAP commands

* `security login rest-role create`

* `security login role create`

== Learn more

*

xref:{relative_path}security_roles_owner.uuid_name_privileges_endpoint_overview.html[DOC /security/roles/{owner.uuid}/{name}/privileges]

* xref:{relative_path}security_roles_endpoint_overview.html[DOC /security/roles]

== Parameters

```
[cols=5*,options=header]
```



```

|===

|Name
|Type
|In
|Required
|Description

|owner.uuid
|string
|path
|True
a|Role owner UUID


|name
|string
|path
|True
a|Role name


|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body


[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|access

```

|string
a|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
a|Either of REST URI/endpoint OR command/command directory path.

|query
|string
a|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.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
 "_links": {
 "self": {
 "href": "/api/resourcelink"
 }
 },
 "access": "readonly",
 "path": [
 "/api/cluster/jobs",
 "/api/storage/volumes",
 "job schedule interval",
 "volume move"
],
 "query": [
 "-days <1 -hours >12",
 "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
]
}

```
]
}
====
```

== Response

Status: 201, Created

== Error

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description

| 5636129
| A role with given name has not been defined.

| 5636143
| A Vserver admin cannot use the API with this access level.

| 5636144
| The value specified for the access level is not valid.

| 5636169
| A character in the URI is not valid.

| 5636170
| The URI does not exist.

| 5636173
| This feature requires an effective cluster version of 9.6 or later.

| 5636175
| Vserver admin cannot have access to given API.

| 5636184
| Expanded REST roles for granular resource control feature is currently
disabled.

| 5636185
| The specified UUID was not found.
```

```

| 5636186
| Expanded REST roles for granular resource control requires an effective
cluster version of 9.10.1 or later.

| 13434890
| Vserver-ID failed for Vserver roles.

| 13434891
| UUID LookUp failed for Vserver roles.

| 13434892
| Roles is a required field.

| 13434893
| The SVM does not exist.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

```

====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#role_privilege]
[.api-collapsible-fifth-title]
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 `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|access
```

```
|string
```

```
a|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
```

```
a|Either of REST URI/endpoint OR command/command directory path.
```

```
|query
```

```
|string
```

```
a|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]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
:leveloffset: -1
```

```
= Manage role privilege path
```

```
:leveloffset: +1
```

```
[[IDeea001515bfe88a3cbffb4cca7c24be4]]
```

```
= Security roles owner.uuid name privileges path endpoint overview
```

```
== Overview
```

A role can comprise of multiple tuples and each tuple consists of a REST API path or command/command directory path and its access level. If the tuple refers to a command/command directory path, it may optionally be associated with a query. These APIs can be used to retrieve or modify the associated access level and optional query. They can also be used to delete one of the constituent REST API paths or command/command directory paths within a role. The REST API path can be a resource-qualified endpoint. Currently, the only supported resource-qualified endpoints are `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

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

Specify the owner UUID and the role name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the role has been created and can be obtained from the response body of a GET request performed on one of the following APIs:


```
_ /api/security/roles_ for all roles
_ /api/security/roles/?scope=svm_ for SVM-scoped roles
_ /api/security/roles/?owner.name=+++<svm-name>+++</i> for roles in a
specific SVM This API response contains the complete URI for each tuple of
the role and can be used for GET, PATCH, or DELETE operations.+++</svm-
name>+++_
```

NOTE: The access level for paths in pre-defined roles cannot be updated.

== Examples

=== Updating the access level for a REST API path in the privilege tuple of an existing role

The API:

```
PATCH "/api/security/roles/{owner.uuid}/{name}/privileges/{path}"
```

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols" -d
'{"access":"all"}'
```

=== Updating the access level for a command/command directory path in the privilege tuple of an existing role

The API:

```
PATCH "/api/security/roles/{owner.uuid}/{name}/privileges/{path}"
```

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_role1/privileges/netp%20port" -d
'{"access":"readonly","query":"-type if-group&#124;vlan"}'
```

=== Updating the access level for a resource-qualified endpoint in the privilege tuple of an existing role

The API:

```
PATCH "/api/security/roles/{owner.uuid}/{name}/privileges/{path}"
```

```

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fstorage%2Fvolumes%2F742ef001-24f0-4d5a-9ec1-2fdaadb282f4%2Fsnapshots" -d '{"access":"readonly"}'
----

=== Retrieving the access level for a REST API path in the privilege tuple
of an existing role

----

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

# The call:
curl -X GET "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols"

# The response:
{
  "owner": {
    "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25"
  },
  "name": "svm_role1",
  "path": "/api/protocols",
  "access": "all",
  "_links": {
    "self": {
      "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols"
    }
  }
}
----

=== Retrieving the access level for a command/command directory path in
the privilege tuple of an existing role

----

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

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

```

```
0050568e2e25/svm_role1/privileges/net%20port"
```

```
# The response:
```

```
{
  "owner": {
    "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25"
  },
  "name": "svm_role1",
  "path": "net port",
  "query": "-type if-group&#124;vlan",
  "access": "readonly",
  "_links": {
    "self": {
      "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/net%20port"
    }
  }
}
```

```
----
```

=== Retrieving the access level for a resource-qualified endpoint in the privilege tuple of an existing role

```
----
```

```
# The API:
```

```
GET "/api/security/roles/{owner.uuid}/{name}/privileges/{path}"
```

```
# The call:
```

```
curl -X GET "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fstorage%2Fvolumes%2Fd0f3b91a-4ce7-4de4-afb9-7eda668659dd%2F%2Fsnapshots"
```

```
# The response:
```

```
{
  "owner": {
    "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25"
  },
  "name": "svm_role1",
  "path": "/api/storage/volumes/d0f3b91a-4ce7-4de4-afb9-7eda668659dd/snapshots",
  "access": "all",
  "_links": {
    "self": {
      "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fstorage%2Fvolumes%2Fd0f3b91a-
```

```
4ce7-4de4-afb9-7eda668659dd%2Fsnapshots"
```

```
}
```

```
}
```

```
}
```

```
----
```

=== Deleting a privilege tuple, containing a REST API path, from an existing role

```
----
```

The API:

```
DELETE "/api/security/roles/{owner.uuid}/{name}/privileges/{path}"
```

The call:

```
curl -X DELETE "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols"
```

```
----
```

=== Deleting a privilege tuple, containing a command/command directory path, from an existing role

```
----
```

The API:

```
DELETE "/api/security/roles/{owner.uuid}/{name}/privileges/{path}"
```

The call:

```
curl -X DELETE "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/net%20port"
```

```
----
```

=== Deleting a privilege tuple, containing a resource-qualified endpoint, from an existing role

```
----
```

The API:

```
DELETE "/api/security/roles/{owner.uuid}/{name}/privileges/{path}"
```

The call:

```
curl -X DELETE "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fstorage%2Fvolumes%2F742ef001-24f0-4d5a-9ec1-2fdaadb282f4%2Fsnapshots"
```

```
----
```

```
[[ID4f48bbaf0173b0727084e21fb3f8cf65]]
```

= Delete a privilege tuple from the role

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-  
block]#`/security/roles/{owner.uuid}/{name}/privileges/{path}`#
```

Introduced In: 9.6

Deletes a privilege tuple (of REST URI or command/command directory path, its access level and an optional query) from the role. The REST URI can be a resource-qualified endpoint. Currently, the only supported resource-qualified endpoints are `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

== Required parameters

- * ``owner.uuid`` - UUID of the SVM which houses this role.
- * ``name`` - Name of the role to be updated.
- * ``path`` - Constituent REST API path or command/command directory path to be deleted from this role. Can be a resource-qualified endpoint (example: `_/api/storage/volumes/43256a71-be02-474d-a2a9-9642e12a6a2c/snapshots_`). Currently, resource-qualified endpoints are limited to the "snapshots" endpoint: `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

== Related ONTAP commands

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

== Learn more

- *
`xref:{relative_path}security_roles_owner.uuid_name_privileges_path_endpoi
nt_overview.html[DOC
/security/roles/{owner.uuid}/\{name}/privileges/\{path}]`
* `xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]`

== Parameters

```

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|owner.uuid
|string
|path
|True
a|Role owner UUID

|name
|string
|path
|True
a|Role name

|path
|string
|path
|True
a|REST API path or command/command directory path

|===

== Response

```

Status: 200, Ok

```

== Error

```

Status: Default

```

ONTAP Error Response Codes

|===
| Error Code | Description

```

```

| 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
| This feature requires 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.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

```

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

```



```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID51c3fdf745095f7885cf820c11d574d1]]
= Retrieve the access level for a REST API path or command/command
directory path for a role

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/roles/{owner.uuid}/{name}/privileges/{path}`#

*Introduced In:* 9.6

```

Retrieves the access level for a REST API path or command/command directory path for the specified role. Optionally retrieves the query, if 'path' refers to a command/command directory path. The REST API path can be a resource-qualified endpoint. Currently, the only supported resource-qualified endpoints are `_/api/storage/volumes/{volume.uuid}/snapshots_` and `_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

== Related ONTAP commands

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

== Learn more

```
*  
xref:{relative_path}security_roles_owner.uuid_name_privileges_path_endpoi  
t_overview.html[DOC  
/security/roles/{owner.uuid}/\{name}/privileges/\{path}]  
* xref:{relative_path}security_roles_endpoint_overview.html[DOC  
/security/roles]
```

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|owner.uuid  
|string  
|path  
|True  
a|Role owner UUID
```

```
|name  
|string  
|path  
|True  
a|Role name
```

```
|path
|string
|path
|True
a|REST API path or command/command directory path
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|access
```

```
|string
```

```
a|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
```

```
a|Either of REST URI/endpoint OR command/command directory path.
```

```
|query
```

```
|string
```

```
a|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.

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access": "readonly",
  "path": [
    "/api/cluster/jobs",
    "/api/storage/volumes",
    "job schedule interval",
    "volume move"
  ],
  "query": [
    "-days <1 -hours >12",
    "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
  ]
}
```

====

== Error

Status: Default, Error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

```

|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID47f6f8fc1805fc2ff840e3ca1830e950]]
= Update the access level for a REST API path or command/command directory
path

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/roles/{owner.uuid}/{name}/privileges/{path}`#

*Introduced In:* 9.6

Updates the access level for a REST API path or command/command directory
path. Optionally updates the query, if 'path' refers to a command/command
directory path. The REST API path can be a resource-qualified endpoint.
Currently, the only supported resource-qualified endpoints are
_/api/storage/volumes/{volume.uuid}/snapshots_ and
_/api/storage/volumes/*/snapshots_. "*" is a wildcard character denoting
"all" volumes.

```

== Required parameters

- * `owner.uuid` - UUID of the SVM that houses this role.
- * `name` - Name of the role to be updated.
- * `path` - Constituent REST API path or command/command directory path, whose access level and/or query are/is to be updated. Can be a resource-qualified endpoint (example: `_/api/storage/volumes/43256a71-be02-474d-a2a9-9642e12a6a2c/snapshots_`). Currently, resource-qualified endpoints are limited to the "snapshots" endpoint:
`_/api/storage/volumes/{volume.uuid}/snapshots_` and
`_/api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.
- * `access` - Access level for the path.

== Optional parameters

- * `query` - Optional query, if the path refers to a command/command directory path.

== Related ONTAP commands

- * `security login rest-role modify`
- * `security login role modify`

== Learn more

*
xref:{relative_path}security_roles_owner.uuid_name_privileges_path_endpoint_overview.html[DOC
/security/roles/{owner.uuid}/{name}/privileges/{path}]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]

== Parameters

[cols=5*,options=header]
|==

|Name
|Type
|In
|Required
|Description

|owner.uuid


```
|string
|path
|True
a|Role owner UUID
```

```
|name
|string
|path
|True
a|Role name
```

```
|path
|string
|path
|True
a|REST API path or command/command directory path
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
 |_links
|link:#_links[_links]
a|
```

```
|access
|string
a|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
a|Either of REST URI/endpoint OR command/command directory path.
```

```
|query
|string
a|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.
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access": "readonly",
  "path": [
    "/api/cluster/jobs",
    "/api/storage/volumes",
    "job schedule interval",
    "volume move"
  ],
  "query": [
    "-days <1 -hours >12",
    "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
  ]
}
```

```
====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#role_privilege]
[.api-collapsible-fifth-title]
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 `_api/storage/volumes/{volume.uuid}/snapshots_` and `_api/storage/volumes/*/snapshots_`. "*" is a wildcard character denoting "all" volumes.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|_links
|link:#_links[_links]
a|

|access
|string
a|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
a|Either of REST URI/endpoint OR command/command directory path.

|query
|string
a|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]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message

```

```

|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

```

= Manage SSH server

:leveloffset: +1

[[IDe98b462bf4ebb7649887c987013b3edc]]

= Security SSH endpoint overview

== Overview

ONTAP supports SSH server that can be accessed from any standard SSH client. A user account needs to be associated with SSH as the application (refer the documentation for `_api/security/accounts_xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]` . Upon connecting from a client, the user is authenticated and a command line shell is presented.

This endpoint is used to retrieve or modify the SSH configuration at the cluster level. The configuration consists of SSH security parameters (security algorithms and maximum authentication retry attempts allowed before closing the connection) and SSH connection limits.

The security algorithms include SSH key exchange algorithms, ciphers for payload encryption, and MAC algorithms. This configuration is the default for all newly created SVMs; existing SVM configurations are not impacted. The SSH connection limits include maximum connections per second, maximum simultaneous sessions from the same client host, and overall maximum SSH connections at any given point in time. The connection limits are per node and will be the same for all nodes in the cluster.

== Examples

=== Updating the SSH security parameters

Specify the algorithms in the body of the PATCH request.

The API:

PATCH "/api/security/ssh"

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/ssh" -d '{ "ciphers": [
"aes256_ctr", "aes192_ctr" ], "key_exchange_algorithms": [
```

```
"diffie_hellman_group_exchange_sha256", "diffie_hellman_group14_sha1" ],
"mac_algorithms": [ "hmac_sha2_512_etm", "umac_128_etm" ],
"max_authentication_retry_count": 3 }'
----
```

=== Updating the SSH connection limits

Specify the connection limits in the body of the PATCH request.

The API:

PATCH "/api/security/ssh"

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/ssh" -d '{
"connections_per_second": 8, "max_instances": 10, "per_source_limit": 5 }'
```

=== Retrieving the cluster SSH server configuration

The API:

GET "/api/security/ssh"

The call:

```
curl -X GET "https://<mgmt-ip>/api/security/ssh"
```

The response:

```
{
"cipher": [
  "aes256_ctr",
  "aes192_ctr"
],
"key_exchange_algorithms": [
  "diffie_hellman_group_exchange_sha256",
  "diffie_hellman_group14_sha1"
],
"mac_algorithms": [
  "hmac_sha2_512_etm",
  "umac_128_etm"
],
"max_authentication_retry_count": 3,
"connections_per_second": 8,
"max_instances": 10,
"per_source_limit": 5,
```



```

"_links": {
  "self": {
    "href": "/api/security/ssh"
  }
}
}
}
-----

```

```

[[ID2707855d3b9a69c41d99953bc6932176]]
= Retrieve cluster SSH server ciphers, MAC algorithms, key exchange
algorithms, and connection limits

```

```

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/ssh`#

```

Introduced In: 9.7

Retrieves the cluster SSH server ciphers, MAC algorithms, key exchange algorithms, and connection limits.

== Related ONTAP commands

```

* `security ssh`
* `security protocol ssh`

```

== Response

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ciphers
|array[string]

```

a|Ciphers for encrypting the data.

|connections_per_second
|integer

a|Maximum connections allowed per second.

|key_exchange_algorithms
|array[string]
a|Key exchange algorithms.

|mac_algorithms
|array[string]
a|MAC algorithms.

|max_authentication_retry_count
|integer
a|Maximum authentication retries allowed before closing the connection.

|max_instances
|integer
a|Maximum possible simultaneous connections.

|per_source_limit
|integer
a|Maximum connections from the same client host.

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
```

```

    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "hmac_sha2_512_etm"
  ]
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

```

    }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]

```

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

```

|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID11a30e7fb1bf6c12d9e6b3e88a99ce59]]
= Update the SSH server setting for a cluster

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/ssh`#

*Introduced In:* 9.7

Updates the SSH server setting for a cluster.

== Optional parameters

* `ciphers` - Encryption algorithms for the payload
* `key_exchange_algorithms` - SSH key exchange algorithms
* `mac_algorithms` - MAC algorithms
* `max_authentication_retry_count` - Maximum authentication retries
allowed before closing the connection
* `connections_per_second` - Maximum allowed connections per second
* `max_instances` - Maximum allowed connections per node
* `per_source_limit` - Maximum allowed connections from the same client
host

== Related ONTAP commands

* `security ssh`
* `security protocol ssh`

== Request Body

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|_links
|link:#_links[_links]
a|

|ciphers
|array[string]
a|Ciphers for encrypting the data.

|connections_per_second
|integer
a|Maximum connections allowed per second.

|key_exchange_algorithms
|array[string]
a|Key exchange algorithms.

|mac_algorithms
|array[string]
a|MAC algorithms.

|max_authentication_retry_count
|integer
a|Maximum authentication retries allowed before closing the connection.

|max_instances
|integer
a|Maximum possible simultaneous connections.

|per_source_limit
|integer
a|Maximum connections from the same client host.

|===

.Example request
[%collapsible%closed]

```

```

=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "hmac_sha2_512_etm"
  ]
}
=====

```

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

=====	
Error Code	Description
10682372	There must be at least one key exchange algorithm associated with the SSH configuration.
10682373	There must be at least one cipher associated with the SSH configuration.
10682375	


```
| Failed to modify SSH key exchange algorithms.

| 10682378
| Failed to modify SSH ciphers.

| 10682399
| Key exchange algorithm not supported in FIPS enabled mode.

| 10682400
| Failed to modify SSH MAC algorithms.

| 10682401
| MAC algorithm not supported in FIPS enabled mode.

| 10682403
| There must be at least one MAC algorithm with the SSH configuration.

| 10682413
| Failed to modify maximum authentication retry attempts.

| 10682413
| Failed to modify maximum authentication retry attempts.

| 10682418
| Cipher not supported in FIPS enabled mode.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
```

```

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

```

====

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

====

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

|===

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self
|link:#href[href]
a|

|===

[#cluster_ssh_server]
[.api-collapsible-fifth-title]
cluster_ssh_server

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ciphers
|array[string]
a|Ciphers for encrypting the data.

|connections_per_second
|integer
a|Maximum connections allowed per second.

|key_exchange_algorithms
|array[string]
a|Key exchange algorithms.

|mac_algorithms
|array[string]
a|MAC algorithms.

|max_authentication_retry_count
|integer
a|Maximum authentication retries allowed before closing the connection.

|max_instances

```

```

|integer
a|Maximum possible simultaneous connections.

|per_source_limit
|integer
a|Maximum connections from the same client host.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]

```

```

a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```

|===

```

```

//end collapsible .Definitions block
====

```

```

:leveloffset: -1

```

```

= View SSH SVMs

```

```

:leveloffset: +1

```

```

[[IDa1f09b44bcf5fceda399a6bd0852b692]]
= Security SSH svms endpoint overview

```

```

=== Overview

```

This endpoint is used to retrieve the SSH security configuration for all SVMs. The configuration consists of SSH security parameters. The security algorithms include SSH key exchange algorithms, ciphers for payload encryption, MAC algorithms, and the maximum authentication retry attempts allowed before closing the connection. The SSH configuration for a newly created SVM is the same as the SSH configuration at cluster level. When

the cluster SSH configuration is updated using `_/security/ssh_` endpoint, the SSH configuration of existing SVMs is not impacted. To customize the SSH security parameters for a particular SVM, perform a PATCH operation on the `_api/security/ssh/svms/{svm.uuid}_` endpoint.

== Example

=== Retrieving the SSH security configuration of all SVMs.

The API:

GET `"/api/security/ssh/svms"`

The call:

curl -X GET `"https://<mgmt-ip>/api/security/ssh/svms"`

The response:

```
{
  "num_records": 1,
  "records": [
    {
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7",
        "_links": {
          "self": {
            "href": "/api/svm/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
          }
        }
      },
      "ciphers": [
        "aes256_ctr",
        "aes192_ctr",
        "aes128_ctr"
      ],
      "key_exchange_algorithms": [
        "diffie_hellman_group_exchange_sha256",
        "diffie_hellman_group14_sha1"
      ],
      "mac_algorithms": [
        "hmac_sha1",
        "hmac_sha2_512_etm"
      ],
      "max_authentication_retry_count": 6,
      "_links": {
```

```

    "self": {
      "href": "/api/security/ssh/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
],
"_links": {
  "next": {
    "href": "/api/resourcelink"
  },
  "self": {
    "href": "/api/resourcelink"
  }
}
}
}
----

```

[[ID41f322cbc9700585ad1596dda37b6e5c]]

= Retrieve the SSH server configuration for all SVMs

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/ssh/svms`#

Introduced In: 9.10

Retrieves the SSH server configuration for all the SVMs.

== Related ONTAP commands

* `security ssh`

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

```
|ciphers
|string
|query
|False
a|Filter by ciphers
```

```
|key_exchange_algorithms
|string
|query
|False
a|Filter by key_exchange_algorithms
```

```
|mac_algorithms
|string
|query
|False
a|Filter by mac_algorithms
```

```
|max_authentication_retry_count
|integer
|query
|False
a|Filter by max_authentication_retry_count
```

```
* Max value: 6
* Min value: 2
```

```
|svm.uuid
|string
|query
|False
a|Filter by svm.uuid
```

```
|svm.name
|string
|query
|False
a|Filter by svm.name
```

```
|fields
```



```

|array[string]
|query
|False
a|Specify the fields to return.

|max_records
|integer
|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|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
a|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.

* Max value: 120
* Min value: 0
* Default value: 1

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

```

== Response

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records.

|records
|array[link:#svm_ssh_server[svm_ssh_server]]
a|

|===
```

```
.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "ciphers": [
      "aes256_ctr",
      "aes192_ctr",
```

```

    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{

```

```

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

```

====

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

====

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

|===

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

SVM name and UUID for which the SSH server is configured.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string

```

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#svm_ssh_server]

[.api-collapsible-fifth-title]

svm_ssh_server

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|ciphers

|array[string]

a|Ciphers for encrypting the data.

|key_exchange_algorithms

|array[string]

a|Key exchange algorithms.

|mac_algorithms

|array[string]

a|MAC algorithms.

|max_authentication_retry_count

|integer

a|Maximum authentication retries allowed before closing the connection.

|svm

|link:#svm[svm]

a|SVM name and UUID for which the SSH server is configured.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

|===

|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
:leveloffset: -1
```

```
= Manage SSH security configuration
```

```
:leveloffset: +1
```

```
[[ID72ab046744a60a58b9c0f6640ed00bd8]]
= Security SSH svms svm.uuid endpoint overview
```

```
== Overview
```

This endpoint is used to retrieve or modify the SSH security configuration to an SVM.

The SSH security algorithms include key exchange algorithms, ciphers for payload encryption, MAC algorithms, and the maximum authentication retry attempts allowed before closing the connection. svm.uuid corresponds to the UUID of the SVM for which the SSH security setting is being retrieved or modified and it is obtained from the response body of a GET operation performed on the `_api/security/ssh/svms_` API.

```
== Examples
```



```
=== Updating the SSH security parameters
```

Specify the algorithms in the body of the PATCH request.

```
----
```

```
# The API:
```

```
PATCH "/api/security/ssh/svms/{svm.uuid}"
```

```
# The call:
```

```
curl -X PATCH "https://<mgmt-ip>/api/security/ssh/svms/02c9e252-41be-11e9-81d5-00a0986138f7" -d '{ "ciphers": [ "aes256_ctr", "aes192_ctr" ],  
"key_exchange_algorithms": [ "diffie_hellman_group_exchange_sha256",  
"diffie_hellman_group14_sha1" ], "mac_algorithms": [ "hmac_sha2_512_etm",  
"umac_128_etm" ], "max_authentication_retry_count": 3 }'
```

```
----
```

```
=== Retrieving the SSH security configuration of an SVM
```

```
----
```

```
# The API:
```

```
GET "/api/security/ssh/svms/{svm.uuid}"
```

```
# The call:
```

```
curl -X GET "https://<mgmt-ip>/api/security/ssh/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
```

```
# The response:
```

```
{  
  "ciphers": [  
    "aes256_ctr",  
    "aes192_ctr"  
  ],  
  "key_exchange_algorithms": [  
    "diffie_hellman_group_exchange_sha256",  
    "diffie_hellman_group14_sha1"  
  ],  
  "mac_algorithms": [  
    "hmac_sha2_512_etm",  
    "umac_128_etm"  
  ],  
  "max_authentication_retry_count": 3,  
  "svm": {  
    "name": "svm1",  
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7",
```

```

    "_links": {
      "self": {
        "href": "/api/svm/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    },
    "_links": {
      "self": {
        "href": "/api/security/ssh/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  }
}
-----

```

[[IDe59d061409a5345c0262e5fb98e8e88c]]
 = Retrieve the SSH server configuration for an SVM

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/ssh/svms/{svm.uuid}`#

Introduced In: 9.10

Retrieves the SSH server configuration for the specified SVM.

== Related ONTAP commands

* `security ssh`

== Parameters

[cols=5*,options=header]
 |===

Name
Type
In
Required
Description

svm.uuid
string
path

```
|True
a|SVM UUID

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===
```

== Response

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ciphers
|array[string]
a|Ciphers for encrypting the data.

|key_exchange_algorithms
|array[string]
a|Key exchange algorithms.

|mac_algorithms
|array[string]
a|MAC algorithms.

|max_authentication_retry_count
|integer
a|Maximum authentication retries allowed before closing the connection.
```

```
|svm
|link:#svm[svm]
a|SVM name and UUID for which the SSH server is configured.
```

```
|===
```

.Example response

[%collapsible%closed]

=====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

=====

== Error

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|href
|string
a|
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

SVM name and UUID for which the SSH server is configured.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
```

```

|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDcedd65d07c1ce286edcf22372f0dda81]]
= Update the SSH server configuration for an SVM

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/ssh/svms/{svm.uuid}`#

*Introduced In:* 9.10

Updates the SSH server configuration for the specified SVM.

== Optional parameters

* `ciphers` - Encryption algorithms for the payload
* `key_exchange_algorithms` - SSH key exchange algorithms
* `mac_algorithms` - MAC algorithms
* `max_authentication_retry_count` - Maximum authentication retries
allowed before closing the connection

== Related ONTAP commands

* `security ssh`

== Parameters

```



```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|svm.uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|SVM UUID
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
 |_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|ciphers
```

```
|array[string]
```

```
a|Ciphers for encrypting the data.
```

```
|key_exchange_algorithms
```

```
|array[string]
```

```
a|Key exchange algorithms.
```

```
|mac_algorithms
```

```
|array[string]
```

```
a|MAC algorithms.
```

```
|max_authentication_retry_count
```

```
|integer
a|Maximum authentication retries allowed before closing the connection.

|svm
|link:#svm[svm]
a|SVM name and UUID for which the SSH server is configured.
```

```
|===
```

```
.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
=====
```

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

Error Code	Description
------------	-------------

10682372	
----------	--

	There must be at least one key exchange algorithm associated with the SSH configuration.
--	--

10682373	
----------	--

	There must be at least one cipher associated with the SSH configuration.
--	--

10682375	
----------	--

	Failed to modify SSH key exchange algorithms.
--	---

10682378	
----------	--

	Failed to modify SSH ciphers.
--	-------------------------------

10682399	
----------	--

	Key exchange algorithm not supported in FIPS-enabled mode.
--	--

10682400	
----------	--

	Failed to modify SSH MAC algorithms.
--	--------------------------------------

10682401	
----------	--

	MAC algorithm not supported in FIPS-enabled mode.
--	---

10682403	
----------	--

	There must be at least one MAC algorithm with the SSH configuration.
--	--

10682413	
----------	--

	Failed to modify maximum authentication retry attempts.
--	---

10682418	
----------	--

	Cipher not supported in FIPS-enabled mode.
--	--

|===

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

SVM name and UUID for which the SSH server is configured.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

```

```

|uuid
|string
a|The unique identifier of the SVM.

|===

[#svm_ssh_server]
[.api-collapsible-fifth-title]
svm_ssh_server

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ciphers
|array[string]
a|Ciphers for encrypting the data.

|key_exchange_algorithms
|array[string]
a|Key exchange algorithms.

|mac_algorithms
|array[string]
a|MAC algorithms.

|max_authentication_retry_count
|integer
a|Maximum authentication retries allowed before closing the connection.

|svm
|link:#svm[svm]
a|SVM name and UUID for which the SSH server is configured.

```

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

|===

|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
:leveloffset: -1
```

```
:leveloffset: -1
```

```
:leveloffset: -1
```

```
<<<
```

```
*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 [link:http://www.netapp.com/TM](http://www.netapp.com/TM)^[http://www.netapp.com/TM^] are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.