Security

REST API reference

NetApp
February 07, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9171/security_endpoints.html on February 07, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Security . . . 1
ONTAP REST API Security endpoints . . . 1
Overview . . . 1
Manage security-related operations . . . 1
Manage security-related operations . . . 1
Retrieve information about security configured on the cluster . . . 12
Update the software FIPS mode or enable conversion of non-encrypted metadata volumes non-NAE aggregates . . . 19
Manage security-related accounts . . . 28
Manage security-related accounts . . . 28
Retrieve user accounts in the cluster . . . 37
Create a new user account . . . 46
Manage scoped user accounts . . . 54
Manage scoped user accounts . . . 54
Delete a user account . . . 57
Retrieve a specific user account . . . 59
Update a user account . . . 64
Manage the anti-ransomware package . . . 72
Manage the anti-ransomware package . . . 72
Retrieve the anti-ransomware version of the nodes in the cluster . . . 75
Update the anti-ransomware package on the cluster . . . 78
View suspect files generated by anti-ransomware . . . 83
View suspect files generated by anti-ransomware . . . 83
Retrieve information on the suspects generated by anti-ransomware analytics . . . 83
Delete suspect files . . . 90
Delete suspect files . . . 90
Clear suspect files of a volume . . . 90
Manage data-entropy statistics . . . 94
Manage data-entropy statistics . . . 95
Retrieve data-entropy statistics for volumes . . . 96
Retrieve a data-entropy statistic for a volume . . . 102
View and update audit settings . . . 107
View and update audit settings . . . 107
Retrieve administrative audit settings for GET requests . . . 108
Update administrative audit settings for GET requests . . . 110
Forward audit logs to syslog/splunk servers . . . 113
Define a remote syslog or splunk server to receive audit information . . . 113
Define the remote syslog or splunk server information . . . 119
Delete the remote syslog or splunk server information . . . 126
Retrieve the remote syslog or splunk server information . . . 128
Update the remote syslog or splunk server information . . . 132
View administrative audit logs . . . 137
View administrative audit logs . . . 137

Retrieve the administrative audit log viewer . . . 138
Manage data SVM account information . . . 146
Manage data SVM account information . . . 146
Delete a data SVM configured as a tunnel . . . 148
Retrieve SVM information configured as an Active Directory domain-tunnel . . . 149
Update a data SVM configured as a tunnel . . . 153
Configure a data SVM as a proxy . . . 156
Manage LDAP server configuration . . . 159
Manage LDAP server configuration . . . 159
Delete the LDAP configuration for the cluster . . . 162
Retrieve the LDAP configuration for the cluster . . . 163
Update the LDAP configuration for the cluster . . . 172
Create the LDAP configuration for the cluster . . . 185
Manage NIS configuration . . . 207
Manage NIS configuration . . . 207
Delete the NIS configuration for the cluster . . . 209
Retrieve the NIS configuration for the cluster . . . 211
Update the NIS configuration for the cluster . . . 215
Create the NIS configuration for the cluster . . . 219
View and update OAuth 2.0 status . . . 224
View and update OAuth 2.0 status . . . 224
Retrieve the OAuth 2.0 status . . . 225
Update the OAuth 2.0 status . . . 227
View and create OAuth 2.0 configurations . . . 228
View and create OAuth 2.0 configurations . . . 228
Retrieve security certificates . . . 732
Create or install security certificates . . . 743
Sign security certificates . . . 758
Delete security certificates . . . 761
Retrieve security certificates . . . 764
Manage external-role-mapping entries . . . 770
Manage external-role-mapping entries . . . 770
Retrieve all external-role-mapping entries . . . 771
Create an external-role-mapping entry . . . 777
Delete an external-role-mapping entry . . . 782
Retrieve an external-role-mapping entry . . . 783
Update an external-role-mapping entry . . . 788
Manage Google Cloud KMS . . . 792
Manage Google Cloud KMS . . . 792
Retrieve a Google Cloud KMS configurations for all clusters and SVMs . . . 798
Create a Google Cloud KMS configuration for an SVM . . . 811
Re-key the external key in the key hierarchy for an SVM . . . 825
Delete a Google Cloud KMS configuration . . . 830
Retrieve the Google Cloud KMS configuration . . . 832
Update the Google Cloud KMS configuration . . . 841

Re-key the internal key in the key hierarchy for an SVM . . . 854
Restore keys for an SVM from a Google Cloud KMS . . . 858
Manage group-to-role mapping entries . . . 861
Manage group-to-role mapping entries . . . 861
Retrieve all group-to-role mapping entries . . . 862
Create a group-to-role mapping entry . . . 868
Delete a group-to-role mapping entry . . . 872
Retrieve a group-to-role mapping entry . . . 873
Update a configured group role-mapping entry . . . 878
Manage group configurations . . . 881
Manage group configurations . . . 881
Retrieve all group entries . . . 882
Create a group entry . . . 889
Delete a group entry . . . 894
Retrieve a group entry . . . 896
Update configured group information . . . 901
View and update IPsec configuration . . . 904
View and update IPsec configuration . . . 904
Retrieve an IPsec configuration . . . 904
Update an IPsec configuration . . . 907
Manage IPsec security certificates . . . 911
Manage IPsec security certificates . . . 911
Retrieve IPsec CA certificates configured for the cluster and all SVMs . . . 911
Add a CA certificate to IPsec . . . 916
Delete a CA certificate with the specified UUID from IPsec . . . 920
Retrieve a CA certificate configured for IPpsec . . . 922
Manage IPsec policies . . . 926
Manage IPsec policies . . . 926
Retrieve IPsec policies . . . 926
Create an IPsec policy . . . 936
Delete an IPsec policy . . . 949
Retrieve an IPsec policy . . . 951
Update an IPsec policy . . . 957
View IPsec security associations . . . 964
View IPsec security associations . . . 964
Retrieve IPsec and IKE security associations . . . 965
Retrieve an IPsec or IKE security association . . . 976
Manage JIT privilege user configurations . . . 984
Manage JIT privilege user configurations . . . 984
Retrieve the JIT privilege user configurations for an SVM . . . 985
Create JIT privilege user configurations for an SVM . . . 992
Delete JIT privilege user configurations for an SVM . . . 998
Related ONTAP commands . . . 998
Required properties . . . 998
Parameters . . . 998

Response 998
Error 998
Definitions 999
Retrieve the JIT privilege user configurations for an SVM 1000
Related ONTAP commands 1000
Parameters 1000
Response 1000
Error 1002
Definitions 1003
Manage global JIT privilege configurations 1005
Manage global JIT privilege configurations 1005
Retrieve global JIT privilege configurations for an SVM 1006
Retrieve JIT privilege configurations for an SVM 1012
Related ONTAP commands 1012
Parameters 1012
Response 1013
Error 1014
Definitions 1015
Modify JIT privilege configurations for an SVM 1017
Related ONTAP commands 1017
Parameters 1017
Request Body 1017
Response 1017
Error 1018
Definitions 1018
View and update key manager configurations 1020
View and update key manager configurations 1020
Retrieve key manager configurations 1024
Update key manager configurations 1029
Manage key managers 1035
Manage key managers 1035
Retrieve key managers 1058
Create a key manager 1074
Delete key managers 1088
Retrieve key managers 1091
Update key managers 1103
Manage authentication keys 1114
Manage authentication keys 1114
The API: 1148
The call: 1148
The response: 1148
Retrieve key manager configurations 1148
Retrieve key management key information for specified keys 1158
Retrieve and restore unrestored keys 1164
Migrate SVM keys between security key managers 1169

Required properties . . . 1169
Related ONTAP commands . . . 1169
Parameters . . . 1169
Request Body . . . 1170
Response . . . 1171
Response . . . 1171
Error . . . 1171
Definitions . . . 1172
List key servers configured in an external key manager . . . 1174
Expensive properties . . . 1174
Examples . . . 1174
Related ONTAP commands . . . 1174
Parameters . . . 1174
Response . . . 1176
Error . . . 1180
Definitions . . . 1180
Add primary key servers to an external key manager . . . 1184
Required properties . . . 1184
Related ONTAP commands . . . 1184
Parameters . . . 1184
Request Body . . . 1185
Response . . . 1185
Error . . . 1186
Definitions . . . 1187
Delete a primary key server . . . 1190
Optional parameters: . . . 1190
Related ONTAP commands . . . 1190
Parameters . . . 1190
Response . . . 1190
Error . . . 1190
Definitions . . . 1191
Retrieve key servers configured in an external key manager . . . 1192
Expensive properties . . . 1192
Examples . . . 1192
Related ONTAP commands . . . 1193
Parameters . . . 1193
Response . . . 1193
Error . . . 1195
Definitions . . . 1196
Update a primary key server . . . 1199
Related ONTAP commands . . . 1199
Parameters . . . 1199
Request Body . . . 1199
Response . . . 1200
Error . . . 1200

Definitions 1201
Manage keystores 1204
Manage keystores 1204
Retrieve keystores 1207
Delete an inactive keystore configuration 1214
Retrieve keystore configuration details with the specified UUID 1216
Enable a keystore configuration 1222
Manage security login messages 1231
Manage security login messages 1231
Retrieve the login banner and messages of the day 1241
Retrieve a login message configuration by UUID 1247
Update a login message configuration 1252
View and create TOTP profiles 1256
View and create TOTP profiles 1256
Retrieve TOTP profiles configured for user accounts 1260
Create the TOTP profile for a user account 1265
Manage TOTP profiles 1272
Manage TOTP profiles 1272
Delete the TOTP profile for a user account 1274
Retrieve the TOTP profile for a user account 1276
Update a TOTP profile for a user account 1281
Manage the multi-admin-verify global setting 1284
Manage the multi-admin-verify global setting 1284
Retrieve a multi-admin-verify configuration 1285
Modify a multi-admin-verify configuration 1288
View and create multi-admin-verify approval groups 1292
View and create multi-admin-verify approval groups 1292
Retrieve multi-admin-verify approval groups 1294
Create a multi-admin-verify approval group 1300
Manage multi-admin-verify approval groups 1304
Manage multi-admin-verify approval groups 1304
Delete a multi-admin-verify approval group 1306
Retrieve a multi-admin-verify approval group 1308
Update a multi-admin-verify approval group 1312
Manage multi-admin-verify approval requests 1315
Manage multi-admin-verify approval requests 1315
Retrieve multi-admin-verify requests 1317
Create a multi-admin-verify request 1325
Manage a multi-admin-verify approval request 1333
Manage a multi-admin-verify approval request 1333
Delete a multi-admin-verify request 1335
Retrieve a multi-admin-verify request 1336
Update a multi-admin-verify request 1342
Manage multi-admin-verify rules 1347
Manage multi-admin-verify rules 1347

Retrieve multi-admin-verify rules . . . 1353
Create a multi-admin-verify rule . . . 1360
Manage a multi-admin-verify rule . . . 1367
Manage a multi-admin-verify rule . . . 1367
Delete a multi-admin-verify rule . . . 1369
Retrieve a multi-admin-verify rule . . . 1371
Update a multi-admin-verify rule . . . 1376
Manage security roles . . . 1380
Manage security roles . . . 1381
Retrieve a list of roles configured in the cluster . . . 1392
Create a new cluster-scoped or SVM-scoped role . . . 1401
View or delete a role . . . 1407
View or delete a role . . . 1407
Delete a role . . . 1411
Retrieve the details of a role . . . 1413
Manage role privilege details . . . 1419
Manage role privilege details . . . 1419
Retrieve privilege details of the specified role . . . 1423
Add a privilege tuple to an existing role . . . 1429
Manage role privilege path . . . 1435
Manage role privilege path . . . 1435
Delete a privilege tuple from the role . . . 1440
Retrieve the access level for a REST API path or command/command directory path for a role . . . 1443
Update the access level for a REST API path or command/command directory path . . . 1447
Manage SSH server . . . 1453
Manage SSH server . . . 1453
Retrieve cluster SSH server ciphers, MAC algorithms, key exchange algorithms, and connection limits . . . 1455
Update the SSH server setting for a cluster . . . 1459
View SSH SVMs . . . 1464
View SSH SVMs . . . 1464
Retrieve the SSH server configuration for all SVMs . . . 1467
Manage SSH security configuration . . . 1474
Manage SSH security configuration . . . 1474
Retrieve the SSH server configuration for an SVM . . . 1476
Update the SSH server configuration for an SVM . . . 1481
Manage WebAuthn credentials . . . 1486
Manage WebAuthn credentials . . . 1486
Retrieve all WebAuthn credentials entries . . . 1487
Delete a WebAuthn credentials entry . . . 1494
Retrieve a WebAuthn credentials entry . . . 1496
View WebAuthn global settings for a cluster and all SVMs . . . 1501
View WebAuthn global settings for a cluster and all SVMs . . . 1501
Retrieve WebAuthn global settings for a cluster and all SVMs . . . 1502
View a WebAuthn global setting entry . . . 1507
View a WebAuthn global setting entry . . . 1508

Retrieve a WebAuthn global setting entry . . . 1508
View all WebAuthn supported algorithms . . . 1513
View all WebAuthn supported algorithms . . . 1513
Retrieve all WebAuthn supported algorithms entries . . . 1513
View a WebAuthn supported algorithms entry . . . 1518
View a WebAuthn supported algorithms entry . . . 1519
Retrieve a WebAuthn supported algorithms entry . . . 1519

Security

ONTAP REST API Security endpoints

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

Manage security-related operations

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 Onboard Key Manager 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. All protocol versions at or above the lowest version level specified are enabled, including those that are not explicitly specified.

– GET /api/security

– GET /api/security?fields=tls

– PATCH /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"] } }'

"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
},
"software_data_encryption": {
  "conversion_enabled": false,
  "disabled_by_default": false,
  "encryption_state": "unencrypted"
},
"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",
    "TLS_AES_128_GCM_SHA256",
    "TLS_AES_256_GCM_SHA384",
    "TLS_CHACHA20_POLY1305_SHA256"
  ],
  "protocol_versions": [
    "TLSv1.3",
    "TLSv1.2"
  ]
},
"management_protocols": {
  "rsh_enabled": false,
  "telnet_enabled": false
 }
}
```

PATCH Examples

Enabling software encryption conversion in the cluster

The following example shows how to enable software encryption conversion in the cluster.

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

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

# 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 API:
/api/cluster/jobs/{uuid}

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

# 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"
  }
}
}
```

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
}'

# 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 API:
/api/cluster/jobs/{uuid}

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

# 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"
  }
}
}
```

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_AES_256_GCM_SHA384"] } }'

# 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 API:
/api/cluster/jobs/{uuid}

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

# 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"
  }
}
}
```

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 } }'

# 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"

# The response:
{
"management_protocols": {
  "rsh_enabled": false,
  "telnet_enabled": false
},
"_links": {
  "self": {
    "href": "/api/security"
  }
}
}
```

Retrieve information about security configured on the cluster

GET `/security`

Introduced In: 9.7

Retrieves information about the security configured on the cluster.

Related ONTAP commands

- `security config show`

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
fips	fips	Cluster-wide Federal Information Processing Standards (FIPS) mode information.
management_protocols	management_protocols	Cluster-wide security protocols related information.
onboard_key_manager_configurable_status	onboard_key_manager_configurable_status	Indicates whether the Onboard Key Manager can be configured in the cluster.
software_data_encryption	software_data_encryption	Cluster-wide software data encryption related information.
tls	tls	Cluster-wide Transport Layer Security (TLS) configuration information

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "onboard_key_manager_configurable_status": {
    "code": 65537300,
    "message": "No platform support for volume encryption in following
nodes - node1, node2."
  },
  "software_data_encryption": {
    "encryption_state": "string"
  },
  "tls": {
    "cipher_suites": [
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
    ],
    "protocol_versions": [
      "string"
    ]
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

fips

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

Name	Type	Description
enabled	boolean	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

Cluster-wide security protocols related information.

Name	Type	Description
rsh_enabled	boolean	Indicates whether or not security protocol rsh is enabled on the cluster.
telnet_enabled	boolean	Indicates whether or not security protocol telnet is enabled on the cluster.

onboard_key_manager_configurable_status

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

Name	Type	Description
code	integer	Code corresponding to the status message. Returns a 0 if the Onboard Key Manager can be configured in the cluster.
message	string	Reason that Onboard Key Manager cannot be configured in the cluster.
supported	boolean	Set to true if the Onboard Key Manager can be configured in the cluster.

software_data_encryption

Cluster-wide software data encryption related information.

Name	Type	Description
conversion_enabled	boolean	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	Indicates whether or not default software data at rest encryption is disabled on the cluster.

Name	Type	Description
encryption_state	string	Software data encryption state. encrypted ‐ All the volumes are encrypted. encrypting ‐ Encryption conversion operation is in progress. partial ‐ Some volumes are encrypted, and others remains in plain text. rekeying ‐ All volumes are currently being encrypted with a new key. unencrypted ‐ None of the volumes are encrypted. conversion_paused ‐ Encryption conversion operation is paused on one or more volumes. rekey_paused ‐ Encryption rekey operation is paused on one or more volumes.
rekey	boolean	

tls

Cluster-wide Transport Layer Security (TLS) configuration information

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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

PATCH `/security`

Introduced In: 9.8

Updates the software FIPS mode or modifies software data encryption. The PATCH request can be used to enable conversion of non-encrypted metadata volumes to encrypted metadata volumes and non-NAE aggregates to NAE aggregates.

Related ONTAP commands

- `security config modify`

Parameters

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
fips	fips	Cluster-wide Federal Information Processing Standards (FIPS) mode information.
management_protocols	management_protocols	Cluster-wide security protocols related information.
software_data_encryption	software_data_encryption	Cluster-wide software data encryption related information.

Name	Type	Description
tls	tls	Cluster-wide Transport Layer Security (TLS) configuration information

Example request

```
{
  "software_data_encryption": {
    "encryption_state": "string"
  },
  "tls": {
    "cipher_suites": [
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
    ],
    "protocol_versions": [
      "string"
    ]
  }
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636142	This operation is not supported in a mixed-release cluster.
5636145	This operation is not supported when cluster security is configured with FIPS mode.
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.
65536987	One or more key servers are unavailable.
196608047	Operation is not allowed when volume move is in progress.
196608070	Key manager is not configured on the cluster. Configure either an external Key Management Server or an onboard key manager.
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.
196608368	Failed to perform the requested operation. One or more data volume in offline state.
196608369	Conversion cannot be enabled because the cluster contains read-only or primordial logical data-protection volumes. Retry the patch operation after deleting those volumes.
196608370	The conversion of non-encrypted volumes to NVE (NetApp Volume Encryption) volumes is already running. Monitor the NVE conversion status by querying the "software_data_encryption.encryption_state" field on the "/api/security" endpoint.

Error Code	Description
196608371	NVE (NetApp Volume Encryption) volumes are already being rekeyed. Monitor the NVE rekey status by querying the "software_data_encryption.encryption_state" field on the "/api/security" endpoint.
196608372	An automated ONTAP update is in progress, retry the PATCH request after it is completed.
196608373	Unable to perform the encryption operation because of a mixed-release cluster. Complete the upgrade or revert operation, then try the PATCH request again.
196608374	Failed to perform the requested operation. One or more SVMs not in admin running state.
196608375	Failed to perform the requested operation. One or more volume is of temporary type.
196608376	Internal error. Could not get volume encryption information.
196608377	Internal error. The Volume Location Database (VLDB) is inconsistent. Contact support personnel to resolve this issue.
196608378	Failed to perform the requested operation. Data SVM Key manager configuration is in mixed state.
196608379	Internal error. The encryption metadata for the volume is inconsistent. Contact technical support for assistance.
196608380	Failed to perform the requested operation. Wafliron is currently active.
196608381	Failed to perform the requested operation. A clone split operation is in progress.
196608382	Failed to perform the requested operation. A volume rehost operation is in progress.
196608383	Failed to perform the requested operation. The cluster contains one or more SnapLock volume.
196608384	The PATCH request to start rekey failed because the cluster contains one or more plain text volumes. Retry the PATCH request after converting the existing plain text volumes to encrypted volumes.
196608385	Failed to perform the requested operation. Keystore configuration is being switched. Wait until the keystore is in the active state and then try the PATCH request again.

Error Code	Description
196608386	Failed to perform the requested operation. Rekey operation for one or more SVMs is in progress. Wait until the keystore is in the active state and then try the PATCH request again.
196608387	"software_data_encryption.conversion_enabled" cannot be set to "false" in a PATCH request.
196608388	Both "software_data_encryption.conversion_enabled" and "software_data_encryption.disabled_by_default" cannot be set to "true" in a single PATCH request.
196608389	Both "software_data_encryption.conversion_enabled" and "software_data_encryption.rekey" cannot be set to "true" in a single PATCH request.
196608390	"software_data_encryption.rekey" cannot be set to "false" in a PATCH request.
196608391	Both "software_data_encryption.rekey" and "software_data_encryption.disabled_by_default" cannot be set to "true" in a single PATCH request.
196608392	The PATCH request for cluster level rekey requires an effective cluster version of 9.16.1 or later.
196608393	The PATCH request for cluster level rekey is not supported on this platform.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

fips

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

Name	Type	Description
enabled	boolean	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

Cluster-wide security protocols related information.

Name	Type	Description
rsh_enabled	boolean	Indicates whether or not security protocol rsh is enabled on the cluster.
telnet_enabled	boolean	Indicates whether or not security protocol telnet is enabled on the cluster.

onboard_key_manager_configurable_status

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

Name	Type	Description
code	integer	Code corresponding to the status message. Returns a 0 if the Onboard Key Manager can be configured in the cluster.
message	string	Reason that Onboard Key Manager cannot be configured in the cluster.
supported	boolean	Set to true if the Onboard Key Manager can be configured in the cluster.

software_data_encryption

Cluster-wide software data encryption related information.

Name	Type	Description
conversion_enabled	boolean	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	Indicates whether or not default software data at rest encryption is disabled on the cluster.

Name	Type	Description
encryption_state	string	Software data encryption state. encrypted ‐ All the volumes are encrypted. encrypting ‐ Encryption conversion operation is in progress. partial ‐ Some volumes are encrypted, and others remains in plain text. rekeying ‐ All volumes are currently being encrypted with a new key. unencrypted ‐ None of the volumes are encrypted. conversion_paused ‐ Encryption conversion operation is paused on one or more volumes. rekey_paused ‐ Encryption rekey operation is paused on one or more volumes.
rekey	boolean	

tls

Cluster-wide Transport Layer Security (TLS) configuration information

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

security_config

Name	Type	Description
fips	fips	Cluster-wide Federal Information Processing Standards (FIPS) mode information.
management_protocols	management_protocols	Cluster-wide security protocols related information.

Name	Type	Description
software_data_encryption	software_data_encryption	Cluster-wide software data encryption related information.
tls	tls	Cluster-wide Transport Layer Security (TLS) configuration information

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage security-related accounts

Manage security-related accounts

Overview

A valid user account is required to login to and provision, monitor, and manage the cluster. The scope of the management operation can be at the cluster level or at an individual SVM level. There is a need to create user accounts with specific privileges apart from the default user accounts, "admin", for cluster and "vsadmin" for

SVM. Custom user accounts can be configured to perform specific (scoped) operations. User accounts can either be created locally (on the Netapp system) or referenced from an external directory server (NIS, LDAP, or Active Directory). Apart from creation, modification, and deletion of a user account, locking and unlocking of a user account or resetting the password (for local accounts only) is possible.

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

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

Restrictions

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

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

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

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

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

Application	Supported Authentication Methods
amqp	password
console	password
service_processor	password, publickey
HTTP	password, domain, nsswitch, certificate
ONTAPI	password, domain, nsswitch, certificate
SSH	password, publickey (key pair), domain, nsswitch, totp

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

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

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

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

Examples

Creating a cluster-scoped user account

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

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

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

# The call to create a cluster user account with applications ssh, http
and password authentication scheme:
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"name":"cluster_user1","applications":[{"application":"ssh","authenticat
ion_methods":["password"],"second_authentication_method":"none"},{"applica
tion":"http","authentication_methods":["password"]}],"role":"admin","passw
ord":"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","au
thentication_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
"svm1":
curl -X GET "https://<mgmt-ip>/api/security/accounts/?owner.name=svm1"

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

Creating an Active Directory users with publickey authentication

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

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

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

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

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

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

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

Retrieving the configured Active directory user accounts

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

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

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

Creating a user with MFA (password+TOTP)

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

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

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

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

```
#The API

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

Creating an SP user with MFA (password + publickey)

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

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

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

Retrieving the configured SP user accounts

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

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

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

Retrieve user accounts in the cluster

GET `/security/accounts`

Introduced In: 9.6

Retrieves a list of user accounts in the cluster.

Related ONTAP commands

- `security login show`

Learn more

- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
name	string	query	False	Filter by name • maxLength: 64 • minLength: 3 • Introduced in: 9.7
scope	string	query	False	Filter by scope • Introduced in: 9.7
locked	boolean	query	False	Filter by locked • Introduced in: 9.7
password_hash_algorithm	string	query	False	Filter by password_hash_algorithm • Introduced in: 9.11
role.name	string	query	False	Filter by role.name • Introduced in: 9.7
applications.authentication_methods	string	query	False	Filter by applications.authentication_methods • Introduced in: 9.7

Name	Type	In	Required	Description
applications.second_authentication_method	string	query	False	Filter by applications.second_authentication_method • Introduced in: 9.7
applications.application	string	query	False	Filter by applications.application • Introduced in: 9.7
applications.is_ns_switch_group	boolean	query	False	Filter by applications.is_ns_switch_group • Introduced in: 9.15
applications.is_ldap_fastbind	boolean	query	False	Filter by applications.is_ldap_fastbind • Introduced in: 9.14
comment	string	query	False	Filter by comment • Introduced in: 9.7
owner.name	string	query	False	Filter by owner.name • Introduced in: 9.7
owner.uuid	string	query	False	Filter by owner.uuid • Introduced in: 9.7
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_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[account]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "applications": [
        {
          "application": "string",
          "authentication_methods": [
            "string"
          ],
          "second_authentication_method": "string"
        }
      ],
      "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": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

account_application

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

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

owner

Owner name and UUID that uniquely identifies the user account.

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

role

Name	Type	Description
_links	_links	
name	string	Role name

account

Name	Type	Description
_links	_links	
applications	array[account_application]	

Name	Type	Description
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a new user account

POST `/security/accounts`

Introduced In: 9.6

Creates a new user account.

Required parameters

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

Optional parameters

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

Related ONTAP commands

- `security login create`

Learn more

- DOC /security/accounts

Parameters

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

Request Body

Name	Type	Description
applications	array[account_application]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example request


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


Response

```
Status: 201, Created
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1261215	The role was not found.
1261225	Invalid command directory name.
1263343	Cannot lock user with password not set or non-password authentication method.
2621475	This operation is not supported on a node SVM.
2621601	This operation is not supported on a system SVM.
2621706	The specified owner.uuid and owner.name refer to different SVMs.
5636099	User creation with a non-admin role is not supported for service-processor application.
5636121	The user account name is reserved for use by the system.
5636126	Cannot create a user with the username or role as autosupport because it is reserved by the system.
5636136	Specifying "is_ns_switch_group" as "true" is supported only for authentication method "nsswitch".
5636140	Creating a login with application console for a data SVM is not supported.
5636141	Creating a login with application service-processor for a data SVM is not supported.
5636164	The authentication method and the second authentication method cannot be any combination of 'nsswitch' and 'password'.
5636165	Second authentication method is not supported for NIS or LDAP group based accounts.
5636176	The application and authentication-method combination is invalid.
5636178	An invalid value is specified for field "application".
5636179	Creating an AMQP application login for a data SVM is not supported.
5636197	LDAP fastbind combination for application and authentication method is not supported.
5636198	LDAP fastbind authentication is supported only for nsswitch.
5636206	Non-domain user cannot have a backslash in the username.
5636207	If the value for either the authentication-method or second-authentication-method parameters is domain, the other parameter must be publickey or none.

Error Code	Description
5636212	TOTP is supported only when the primary authentication method is password or public key.
5636214	Configuring the user with TOTP as a secondary authentication method requires an effective cluster version of 9.13.1 or later.
5636223	Specifying "is_ns_switch_group" as "true" is supported only for SSH, ONTAPI, and HTTP applications.
5636224	Configuring a Service Processor (SP) user with two-factor authentication requires an effective cluster version of 9.15.1 or later.
5636225	For a Service Processor (SP) user, the second factor of authentication must be one of publickey or none.
5636226	Internal error. Failed to check for ONTAP capability.
5636250	The "second_authentication_method" parameter is supported for HTTP, SSH, and Service Processor (SP) applications only.
5636251	For HTTP application, "publickey" is the only supported value for the "second_authentication_method" parameter; and can be specified only if the "authentication_methods" parameter has value "password" or "domain" or "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.

Error Code	Description
7078900	An admin password is not set. Set the password by including it in the request.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

account_application

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

owner

Owner name and UUID that uniquely identifies the user account.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

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

role

Name	Type	Description
name	string	Role name

account

Name	Type	Description
applications	array[account_application]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage scoped user accounts

Manage scoped user accounts

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></i> for a specific SVM This API response contains the complete URI for each user account that can be used.</svm-name>

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": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
  "name": "svm1",
  "_links": {
    "self": {
      "href": "/api/svm/svms/aaef7c38-4bd3-11e9-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"
```

Delete a user account

DELETE `/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

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID
name	string	path	True	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.

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

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a specific user account

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

Introduced In: 9.6

Retrieves a specific user account.

Related ONTAP commands

- `security login show`

Learn more

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID
name	string	path	True	User account name

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
applications	array[account_application]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": [
    {
      "application": "string",
      "authentication_methods": [
        "string"
      ],
      "second_authentication_method": "string"
    }
  ],
  "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": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

account_application

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

owner

Owner name and UUID that uniquely identifies the user account.

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

role

Name	Type	Description
_links	_links	
name	string	Role name

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update a user account

PATCH `/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* and *service_processor* applications. 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.
- `is_ldap_fastbind` - Set to true/false to enable LDAP Fastbind Authentication.
- `is_ns_switch_group` - Set to true/false to specify whether the user is an LDAP or NIS group.

Related ONTAP commands

- `security login create`
- `security login modify`
- `security login password`
- `security login lock`
- `security login unlock`

Learn more

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID
name	string	path	True	User account name

Request Body

Name	Type	Description
applications	array[account_application]	

Name	Type	Description
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example request

```
{
  "applications": [
    {
      "application": "string",
      "authentication_methods": [
        "string"
      ],
      "second_authentication_method": "string"
    }
  ],
  "comment": "string",
  "password": "string",
  "password_hash_algorithm": "sha512",
  "role": {
    "name": "admin"
  },
  "scope": "string"
}
```

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.

Error Code	Description
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.
5636136	Specifying "is_ns_switch_group" as "true" is supported only for authentication method "nsswitch".
5636154	For mixed-version cluster the second authentication method parameter is supported for SSH and Service Processor (SP) applications only.
5636159	For a given user and application, if the second-authentication-method is specified, only one such login entry is supported.
5636164	The authentication method and the second authentication method cannot be any combination of 'nsswitch' and 'password'.
5636165	Second authentication method is not supported for NIS or LDAP group based accounts.
5636197	LDAP fastbind combination for application and authentication method is not supported.
5636198	LDAP fastbind authentication is supported only for nsswitch.
5636212	TOTP is supported only when the primary authentication method is password or public key.
5636214	Configuring the user with TOTP as a secondary authentication method requires an effective cluster version of 9.13.1 or later.
5636223	Specifying "is_ns_switch_group" as "true" is supported only for SSH, ONTAPI and HTTP applications.
5636224	Configuring a Service Processor (SP) user with two-factor authentication requires an effective cluster version of 9.15.1 or later.
5636225	For a Service Processor (SP) user, the second factor of authentication must be one of publickey or none.
5636226	Internal error. Failed to check for ONTAP capability.
5636233	User modification failed because LDAP is not configured for the SVM or the LDAP connection is not secure.
7077896	Cannot lock the account of the last console admin user.

Error Code	Description
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.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

account_application

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

owner

Owner name and UUID that uniquely identifies the user account.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

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

role

Name	Type	Description
name	string	Role name

account

Name	Type	Description
applications	array[account_application]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

error_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage the anti-ransomware package

Manage the anti-ransomware package

Overview

This API displays and manages the anti-ransomware package version.

Examples

Retrieving the anti-ransomware package version of all nodes in the cluster.

The following example shows how to retrieve anti-ransomware package version.

```
# The API:
GET /security/anti-ransomware

# The call:
curl -X GET "https://<mgmt-ip>/api/security/anti-ransomware" -H "accept:
application/hal+json"

# The response:
{
"nodes": [
  {
    "name": "sti11-vsim-ucs573i",
    "version": "1.0"
  },
  {
    "name": "sti11-vsim-ucs573j",
    "version": "1.0"
  }
],
"_links": {
  "self": {
    "href": "/api/security/anti-ransomware/"
  }
}
}
```

Updating the anti-ransomware package

The following example shows how to update the anti-ransomware package on the cluster.

```
# The API:
PATCH /security/anti-ransomware

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/anti-ransomware" -H "accept:
application/hal+json" -d '{"uri": "http://server/package"}'

# The response:
{
"job": {
  "uuid": "74d0faef-3e1a-11ef-af89-005056ac6d8a",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/74d0faef-3e1a-11ef-af89-005056ac6d8a"
    }
  }
}
}
```

The call to update the anti-ransomware package returns the job UUID, including a HAL link to retrieve details about the job. The job object includes a `state` field and a message to indicate the progress of the job. When the job is complete and the application is fully created, the message indicates success and the job `state` field is set to `success`.

```
# The API:
/api/cluster/jobs/{uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/cluster/jobs/74d0faef-3e1a-11ef-af89-
005056ac6d8a" -H "accept: application/hal+json"

# The response:
{
"uuid": "74d0faef-3e1a-11ef-af89-005056ac6d8a",
"description": "PATCH /api/security/anti-ransomware",
"state": "success",
"message": "success",
"code": 0,
"_links": {
  "self": {
    "href": "/api/cluster/jobs/74d0faef-3e1a-11ef-af89-005056ac6d8a"
  }
}
}
```

Retrieve the anti-ransomware version of the nodes in the cluster

GET `/security/anti-ransomware`

Introduced In: 9.16

Retrieves the anti-ransomware package version of the nodes in the cluster.

Related ONTAP commands

- `security anti-ransomware show`

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0

Response

```
Status: 200, Ok
```

Name	Type	Description
nodes	array[anti_ransomware_node]	
uri	string	URI of the anti-ransomware package through a server

Example response


```
{
  "nodes": [
    {
      "name": "node1",
      "version": "1.0"
    }
  ],
  "uri": "http://server/package"
}
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
917775	Operation is not supported on offline volumes.
203161606	Failed to check the "anti-ransomware-state" of the volume.
203162108	Operation is not supported on volumes that contain LUNs or namespaces.
203162109	Operation is not supported on an anti-ransomware disable-in-progress volume.

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

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

anti_ransomware_node

Name	Type	Description
name	string	Name of the node.
version	string	Anti-ransomware version.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the anti-ransomware package on the cluster

PATCH `/security/anti-ransomware`

Introduced In: 9.16

Updates the anti-ransomware package on the cluster.

Required properties

- `uri` - URI of the anti-ransomware package

Related ONTAP commands

- `security anti-ransomware update-package-from-uri`

Parameters

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
nodes	array[anti_ransomware_node]	
uri	string	URI of the anti-ransomware package through a server

Example request

```
{
  "nodes": [
    {
      "name": "node1",
      "version": "1.0"
    }
  ],
  "uri": "http://server/package"
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
203161684	Autonomous Ransomware Protection (ARP) package file must be either a .tar or .tgz file.
203161685	Autonomous Ransomware Protection (ARP) package file download failed.
203161686	Autonomous Ransomware Protection (ARP) package file unzip failed.
203161687	Autonomous Ransomware Protection (ARP) package file untar failed.
203161688	Autonomous Ransomware Protection (ARP) package archive invalid. No ARP version file found.
203161689	Internal error. Filesystem error while installing Autonomous Ransomware Protection (ARP) package file.
203161690	Autonomous Ransomware Protection (ARP) package update requires an effective cluster version of 9.16.1 or later.
203161691	Autonomous Ransomware Protection (ARP) package file is invalid. The checksum verification of the ARP configuration files failed.
203161692	Autonomous Ransomware Protection (ARP) package update failed because one or more nodes are not healthy.
203161694	Failed to update the Autonomous Ransomware Protection (ARP) package file because the `uri` property was not specified.

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

Definitions

See Definitions

anti_ransomware_node

Name	Type	Description
name	string	Name of the node.
version	string	Anti-ransomware version.

anti_ransomware

Name	Type	Description
nodes	array[anti_ransomware_node]	
uri	string	URI of the anti-ransomware package through a server

href

Name	Type	Description
href	string	

_links

job_link

Name	Type	Description
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

returned_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.

View suspect files generated by anti-ransomware

View suspect files generated by anti-ransomware

Retrieving information on suspected files

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

Retrieve information on the suspects generated by anti-ransomware analytics

GET `/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

Name	Type	In	Required	Description
file.reason	string	query	False	Filter by file.reason • Introduced in: 9.11
file.format	string	query	False	Filter by file.format
file.path	string	query	False	Filter by file.path
file.name	string	query	False	Filter by file.name
file.suspect_time	string	query	False	Filter by file.suspect_time

Name	Type	In	Required	Description
volume.uuid	string	query	False	Filter by volume.uuid
volume.name	string	query	False	Filter by volume.name
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[anti_ransomware_suspect]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "file": {
        "format": "pdf",
        "name": "test_file",
        "path": "d1/d2/d3",
        "reason": "High Entropy",
        "suspect_time": "2021-05-12 11:00:16 -0400"
      },
      "volume": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "volume1",
        "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

file

Name	Type	Description
format	string	File format of the suspected file.
name	string	Name of the suspected file.
path	string	Path of the suspected file.
reason	string	Reason behind this file being suspected
suspect_time	string	Time when the file was detected as a potential suspect in date-time format.

volume

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.

Name	Type	Description
uuid	string	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 • x-nullable: true

anti_ransomware_suspect

File suspected to be potentially attacked by ransomware.

Name	Type	Description
_links	_links	
file	file	
volume	volume	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete suspect files

Delete suspect files

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

Clear suspect files of a volume

DELETE `/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

Name	Type	In	Required	Description
volume.uuid	string	path	True	Identification of the Anti-ransomware suspect file for the deletion. • format: uuid
is_false_positive	boolean	query	False	Specifies whether the suspected ransomware activity is a false positive or not. • Default value:
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0

Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response


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


Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
203161673	Operation is not supported on a data protection volume.
203162105	Clearing a suspect by specifying the file format is not supported when an attack is detected by encryption_percentage_analysis.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage data-entropy statistics

Manage data-entropy statistics

Overview

This API returns the percentage of data classified as encrypted using an entropy algorithm, measured at various time intervals at the volume level. If no volume UUID is specified, entropy statistics of all the volumes will be returned. The entropy_stats_type parameter can be used to retrieve statistics with sub_hourly, hourly, or daily granularity. Additionally, it can be used to identify intervals that exhibited high (high_enc_pct) percentages of encrypted data. If no type is specified, all types of entropy statistics will be returned for the volumes.

Examples

Retrieving volume stats

In this example, the API returns the data-entropy statistics for the volumes.

```
# The API:
/security/anti-ransomware/volume/entropy-stats

# The call:
curl -X GET "https://<mgmt-ip>/api/security/anti-
ransomware/volume/entropy-stats" -H "accept: application/json"

# The response:
{
"records": [
  {
     "volume": {
     "uuid": "61edb8bb-b7d1-11ef-932d-005056bbaeff",
     "name": "v2"
     },
     "entropy_stats_type": "sub_hourly",
     "timestamp": "2024-12-13T03:36:24-05:00",
     "data_written_in_bytes": 13249687,
     "encryption_percentage": 51,
     "duration": "PT10M21S",
     "_links": {
      "self": {
       "href": "/api/security/anti-ransomware/volume/entropy-
stats/61edb8bb-b7d1-11ef-932d-005056bbaeff/sub_hourly/2024-12-
13T03%3A36%3A24-05%3A00"
      }
     }
  },
  {
     "volume": {
     "uuid": "61edb8bb-b7d1-11ef-932d-005056bbaeff",
     "name": "v2"
```

```
      },
      "entropy_stats_type": "hourly",
      "timestamp": "2024-12-13T04:16:06-05:00",
      "data_written_in_bytes": 13249687,
      "encryption_percentage": 51,
      "duration": "PT1H2M36S",
      "_links": {
       "self": {
        "href": "/api/security/anti-ransomware/volume/entropy-
stats/61edb8bb-b7d1-11ef-932d-005056bbaeff/hourly/2024-12-13T04%3A16%3A06-
05%3A00"
       }
      }
   }
],
"num_records": 20,
"_links": {
 "self": {
   "href": "/api/security/anti-ransomware/volume/entropy-stats/61edb8bb-
b7d1-11ef-932d-005056bbaeff"
  }
 }
}
```


Retrieve data-entropy statistics for volumes

GET `/security/anti-ransomware/volume/entropy-stats`

Introduced In: 9.17

Retrieves the data-entropy statistics for the volumes.

Parameters

Name	Type	In	Required	Description
timestamp	string	query	False	Filter by timestamp
duration	string	query	False	Filter by duration
data_written_in_bytes	integer	query	False	Filter by data_written_in_bytes
entropy_stats_type	string	query	False	Filter by entropy_stats_type

Name	Type	In	Required	Description
volume.uuid	string	query	False	Filter by volume.uuid
volume.name	string	query	False	Filter by volume.name
encryption_percentage	integer	query	False	Filter by encryption_percentage
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[records]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "data_written_in_bytes": 0,
      "duration": "PT15M",
      "encryption_percentage": 0,
      "entropy_stats_type": "string",
      "timestamp": "string",
      "volume": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "volume1",
        "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

volume

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	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 • x-nullable: true

records

Volume data-entropy statistics derived from block analysis.

Name	Type	Description
_links	_links	
data_written_in_bytes	integer	The amount of data written.

Name	Type	Description
duration	string	The duration of the interval associated with this statistic. The duration is represented in ISO-8601 standard format.
encryption_percentage	integer	The percentage of data that is encrypted.
entropy_stats_type	string	Volume metrics are retrieved based on this statistic type.
timestamp	string	Start time in date-time format.
volume	volume	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a data-entropy statistic for a volume

GET `/security/anti-ransomware/volume/entropy-stats/{volume.uuid}/{entropy_stats_type}/{timestamp}`

Introduced In: 9.17

Retrieves a data-entropy statistic for the volumes.

Parameters

Name	Type	In	Required	Description
volume.uuid	string	path	True	The UUID of the volume.
entropy_stats_type	string	path	True	The type of entropy statistics. • enum: ["sub_hourly", "hourly", "daily", "high_enc_pct"]
timestamp	string	path	True	The timestamp of the statistics. • format: date-time
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
data_written_in_bytes	integer	The amount of data written.
duration	string	The duration of the interval associated with this statistic. The duration is represented in ISO-8601 standard format.
encryption_percentage	integer	The percentage of data that is encrypted.
entropy_stats_type	string	Volume metrics are retrieved based on this statistic type.
timestamp	string	Start time in date-time format.
volume	volume	

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "data_written_in_bytes": 0,
  "duration": "PT15M",
  "encryption_percentage": 0,
  "entropy_stats_type": "string",
  "timestamp": "string",
  "volume": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

volume

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	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 • x-nullable: true

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

View and update audit settings

View and update audit settings

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}'
```

Retrieve administrative audit settings for GET requests

GET `/security/audit`

Introduced In: 9.6

Retrieves administrative audit settings for GET requests.

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
cli	boolean	Enable auditing of CLI GET Operations. Valid in PATCH
http	boolean	Enable auditing of HTTP GET Operations. Valid in PATCH

Name	Type	Description
ontapi	boolean	Enable auditing of ONTAP API GET operations. Valid in PATCH • Introduced in: 9.6 • x-nullable: true

Example response

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

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update administrative audit settings for GET requests

PATCH `/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

Name	Type	Description
cli	boolean	Enable auditing of CLI GET Operations. Valid in PATCH
http	boolean	Enable auditing of HTTP GET Operations. Valid in PATCH
ontapi	boolean	Enable auditing of ONTAP API GET operations. Valid in PATCH • Introduced in: 9.6 • x-nullable: true

Response

```
Status: 200, Ok
```

Name	Type	Description
cli	boolean	Enable auditing of CLI GET Operations. Valid in PATCH
http	boolean	Enable auditing of HTTP GET Operations. Valid in PATCH
ontapi	boolean	Enable auditing of ONTAP API GET operations. Valid in PATCH • Introduced in: 9.6 • x-nullable: true

Error

```
Status: Default, Error
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

security_audit

Name	Type	Description
cli	boolean	Enable auditing of CLI GET Operations. Valid in PATCH
http	boolean	Enable auditing of HTTP GET Operations. Valid in PATCH
ontapi	boolean	Enable auditing of ONTAP API GET operations. Valid in PATCH • Introduced in: 9.6 • x-nullable: true

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Forward audit logs to syslog/splunk servers

Define a remote syslog or splunk server to receive audit information

GET `/security/audit/destinations`

Introduced In: 9.6

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

Parameters

Name	Type	In	Required	Description
ipspace.name	string	query	False	Filter by ipspace.name • Introduced in: 9.12
ipspace.uuid	string	query	False	Filter by ipspace.uuid • Introduced in: 9.12
port	integer	query	False	Filter by port
timestamp_format_override	string	query	False	Filter by timestamp_format_override • Introduced in: 9.13
facility	string	query	False	Filter by facility
address	string	query	False	Filter by address
verify_server	boolean	query	False	Filter by verify_server
protocol	string	query	False	Filter by protocol
hostname_format_override	string	query	False	Filter by hostname_format_override • Introduced in: 9.13

Name	Type	In	Required	Description
message_format	string	query	False	Filter by message_format • Introduced in: 9.13
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
Specify the fields to return.	max_records	integer	query	False
Limit the number of records returned.	return_timeout	integer	query	False
The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0	return_records	boolean	query	False

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records

Name	Type	Description
records	array[security_audit_log_forward]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "address": "1.1.1.1",
      "facility": "string",
      "hostname_format_override": "string",
      "ipspace": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "Default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "message_format": "string",
      "port": 514,
      "protocol": "string",
      "timestamp_format_override": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

ipspace

Name	Type	Description
_links	_links	
name	string	IPspace name
uuid	string	IPspace UUID

security_audit_log_forward

Name	Type	Description
address	string	Destination syslog|splunk host to forward audit records to. This can be an IP address (IPv4|IPv6) or a hostname.
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
hostname_format_override	string	Syslog Hostname Format Override
ipspace	ipspace	

Name	Type	Description
message_format	string	Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format.
port	integer	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	Log forwarding protocol
timestamp_format_override	string	Syslog Timestamp Format Override.
verify_server	boolean	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

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message

Name	Type	Description
target	string	The target parameter that caused the error.

Define the remote syslog or splunk server information

POST `/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` (1 - 65535)
- `ipspace`
- `protocol`
- `facility`
- `verify_server` (Can only be "true" when protocol is "tcp_encrypted")
- `message_format` (Can be either "legacy-netapp" or "rfc-5424")
- `timestamp_format_override` (Can be either "no-override", "rfc-3164", "iso-8601-utc" or "iso-8601-local-time")
- `hostname_format_override` (Can be either "no-override", "fqdn" or "hostname-only")

Parameters

Name	Type	In	Required	Description
force	boolean	query	False	Skip the Connectivity Test • Default value:

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

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

Name	Type	Description
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
hostname_format_override	string	Syslog Hostname Format Override
ipspace	ipspace	
message_format	string	Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format.
port	integer	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	Log forwarding protocol
timestamp_format_override	string	Syslog Timestamp Format Override.
verify_server	boolean	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

```
{
  "address": "1.1.1.1",
  "facility": "string",
  "hostname_format_override": "string",
  "ipspace": {
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "message_format": "string",
  "port": 514,
  "protocol": "string",
  "timestamp_format_override": "string"
}
```

Response

```
Status: 202, Accepted
```

Name	Type	Description
num_records	integer	Number of records
records	array[security_audit_log_forward]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "address": "1.1.1.1",
      "facility": "string",
      "hostname_format_override": "string",
      "ipspace": {
        "name": "Default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "message_format": "string",
      "port": 514,
      "protocol": "string",
      "timestamp_format_override": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
15661	The object specified could not be found
13114	Internal error
13115	Invalid input

Error Code	Description
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.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ipspace

Name	Type	Description
name	string	IPspace name
uuid	string	IPspace UUID

security_audit_log_forward

Name	Type	Description
address	string	Destination syslog|splunk host to forward audit records to. This can be an IP address (IPv4|IPv6) or a hostname.
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
hostname_format_override	string	Syslog Hostname Format Override
ipspace	ipspace	
message_format	string	Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format.
port	integer	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	Log forwarding protocol

Name	Type	Description
timestamp_format_override	string	Syslog Timestamp Format Override.
verify_server	boolean	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

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete the remote syslog or splunk server information

DELETE `/security/audit/destinations/{address}/{port}`

Introduced In: 9.6

Deletes remote syslog/splunk server information.

Parameters

Name	Type	In	Required	Description
address	string	path	True	IP address of remote syslog/splunk server.
port	integer	path	True	Port number of remote syslog/splunk server.

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the remote syslog or splunk server information

GET `/security/audit/destinations/{address}/{port}`

Introduced In: 9.6

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

Parameters

Name	Type	In	Required	Description
address	string	path	True	IP address of remote syslog/splunk server.
port	integer	path	True	Port number of remote syslog/splunk server.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
address	string	Destination syslog|splunk host to forward audit records to. This can be an IP address (IPv4|IPv6) or a hostname.
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
hostname_format_override	string	Syslog Hostname Format Override
ipspace	ipspace	
message_format	string	Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format.
port	integer	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	Log forwarding protocol
timestamp_format_override	string	Syslog Timestamp Format Override.
verify_server	boolean	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


```
{
  "address": "1.1.1.1",
  "facility": "string",
  "hostname_format_override": "string",
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "message_format": "string",
  "port": 514,
  "protocol": "string",
  "timestamp_format_override": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

ipspace

Name	Type	Description
_links	_links	
name	string	IPspace name
uuid	string	IPspace UUID

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the remote syslog or splunk server information

PATCH `/security/audit/destinations/{address}/{port}`

Introduced In: 9.6

Updates remote syslog/splunk server information.

Parameters

Name	Type	In	Required	Description
address	string	path	True	IP address of remote syslog/splunk server.
port	integer	path	True	Port number of remote syslog/splunk server.

Request Body

Name	Type	Description
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
hostname_format_override	string	Syslog Hostname Format Override
ipspace	ipspace	
message_format	string	Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format.
timestamp_format_override	string	Syslog Timestamp Format Override.
verify_server	boolean	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

```
{
  "facility": "string",
  "hostname_format_override": "string",
  "ipspace": {
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "message_format": "string",
  "timestamp_format_override": "string"
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
hostname_format_override	string	Syslog Hostname Format Override
ipspace	ipspace	
message_format	string	Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format.
timestamp_format_override	string	Syslog Timestamp Format Override.
verify_server	boolean	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


```
{
  "facility": "string",
  "hostname_format_override": "string",
  "ipspace": {
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "message_format": "string",
  "timestamp_format_override": "string"
}
```


Error

```
Status: Default, Default
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ipspace

Name	Type	Description
name	string	IPspace name
uuid	string	IPspace UUID

security_audit_log_forward

Name	Type	Description
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
hostname_format_override	string	Syslog Hostname Format Override
ipspace	ipspace	
message_format	string	Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format.
timestamp_format_override	string	Syslog Timestamp Format Override.
verify_server	boolean	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

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View administrative audit logs

View administrative audit logs

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. Note: The index field is used to order the audit log messages before they are displayed. If multiple entries for the same node and timestamp occur simultaneously, the index assigns an order to ensure logical consistency.

```
# 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",
    "role": "admin"
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/security/audit/messages"
  }
}
}
```

Retrieve the administrative audit log viewer

GET `/security/audit/messages`

Introduced In: 9.6

Retrieves the administrative audit log viewer.

Parameters

Name	Type	In	Required	Description
role	string	query	False	Filter by role • Introduced in: 9.17
state	string	query	False	Filter by state
scope	string	query	False	Filter by scope
user	string	query	False	Filter by user
session_id	string	query	False	Filter by session_id
timestamp	string	query	False	Filter by timestamp
svm.name	string	query	False	Filter by svm.name
message	string	query	False	Filter by message
application	string	query	False	Filter by application
node.uuid	string	query	False	Filter by node.uuid
node.name	string	query	False	Filter by node.name
input	string	query	False	Filter by input
location	string	query	False	Filter by location
index	integer	query	False	Filter by index
command_id	string	query	False	Filter by command_id
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
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[security_audit_log]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "application": "string",
      "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"
      },
      "role": "string",
      "scope": "string",
      "session_id": "string",
      "state": "string",
      "svm": {
        "name": "string"
      },
      "timestamp": "string",
      "user": "string"
    }
  ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

node

Node where the audit message resides.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

svm

This is the SVM through which the user connected.

Name	Type	Description
name	string	

security_audit_log

Name	Type	Description
_links	_links	
application	string	This identifies the "application" by which the request was processed.

Name	Type	Description
command_id	string	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	Internal index for accessing records with the same time and node. This is a 64-bit unsigned value that is used to order the audit log messages before they are displayed. If multiple entries for the same node and timestamp occur simultaneously, the index assigns an order to ensure logical consistency.
input	string	The request.
location	string	This identifies the location of the remote user. This is an IP address or "console".
message	string	This is an optional field that might contain "error" or "additional information" about the status of a command.
node	node	Node where the audit message resides.
role	string	Role of the remote user.
scope	string	Set to "svm" when the request is on a data SVM; otherwise set to "cluster".
session_id	string	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	State of of this request.

Name	Type	Description
svm	svm	This is the SVM through which the user connected.
timestamp	string	Log entry timestamp. Valid in URL
user	string	Username of the remote user.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage data SVM account information

Manage data SVM account information

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"
  }
}
}
```

Delete a data SVM configured as a tunnel

DELETE `/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

- DOC /security/authentication/cluster/ad-proxy
- DOC /security/accounts

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve SVM information configured as an Active Directory domain-tunnel

GET `/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

- DOC /security/authentication/cluster/ad-proxy
- DOC /security/accounts

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
svm	svm	SVM, applies only to SVM-scoped objects.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

svm

SVM, applies only to SVM-scoped objects.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update a data SVM configured as a tunnel

PATCH `/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

- DOC /security/authentication/cluster/ad-proxy
- DOC /security/accounts

Request Body

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.

Example request

```
{
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
2621516	This operation is only supported on a data SVM.
2621706	The specified `svm.uuid` and `svm.name` refer to different SVMs.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

SVM, applies only to SVM-scoped objects.

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

cluster_ad_proxy

The SVM configured as proxy for Active Directory authentication of cluster accounts.

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Configure a data SVM as a proxy

POST `/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

- DOC /security/authentication/cluster/ad-proxy
- DOC /security/accounts

Request Body

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.

Example request

```
{
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

```
Status: 201, Created
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
2621516	This operation is only supported on a data SVM.
2621706	The specified `svm.uuid` and `svm.name` refer to different SVMs.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

SVM, applies only to SVM-scoped objects.

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

cluster_ad_proxy

The SVM configured as proxy for Active Directory authentication of cluster accounts.

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Manage LDAP server configuration

Manage LDAP server configuration

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\": \"<BIND-PASSWORD>\", \"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\": \"<BIND-PASSWORD>\", \"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"
```

Delete the LDAP configuration for the cluster

DELETE `/security/authentication/cluster/ldap`

Introduced In: 9.6

Deletes the LDAP configuration of the cluster.

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the LDAP configuration for the cluster

GET `/security/authentication/cluster/ldap`

Introduced In: 9.6

Retrieves the cluster LDAP configuration.

Related ONTAP commands

- `ldap show`
- `ldap check -vserver vs0`
- `ldap check-ipv6 -vserver vs0`

Important notes

- The status.code, status.dn_message, status.message, and status.state fields have the same status fields that are returned using the "ldap check" CLI command.
- Refer to the ipv4 or ipv6 objects available in the status field to get specific information about the code, dn_messages, or message and state information for ipv4 or ipv6.

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
base_dn	string	Specifies the default base DN for all searches.
base_scope	string	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

Name	Type	Description
bind_as_cifs_server	boolean	Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.
bind_dn	string	Specifies the user that binds to the LDAP servers.
group_dn	string	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	Specifies the custom filter used for group membership lookups from an LDAP server.
group_scope	string	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	Specifies whether or not netgroup by host querying is enabled.
is_owner	boolean	Specifies whether or not the SVM owns the LDAP client configuration.
ldaps_enabled	boolean	Specifies whether or not LDAPS is enabled.
min_bind_level	string	The minimum bind authentication level. Possible values are: • anonymous - anonymous bind • simple - simple bind • sasl - Simple Authentication and Security Layer (SASL) bind

Name	Type	Description
netgroup_byhost_dn	string	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	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.
netgroup_scope	string	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	The port used to connect to the LDAP Servers.
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.

Name	Type	Description
schema	string	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]	
session_security	string	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
status	status	
try_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.
user_dn	string	Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups.
user_scope	string	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


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_dn": "string",
  "base_scope": "string",
  "bind_dn": "string",
  "group_dn": "string",
  "group_membership_filter": "string",
  "group_scope": "string",
  "min_bind_level": "string",
  "netgroup_byhost_dn": "string",
  "netgroup_byhost_scope": "string",
  "netgroup_dn": "string",
  "netgroup_scope": "string",
  "port": 389,
  "schema": "string",
  "servers": [
    "string"
  ],
  "session_security": "string",
  "skip_config_validation": true,
  "status": {
    "code": 65537300,
    "dn_message": [
      "string"
    ],
    "ipv4": {
      "code": 65537300,
      "dn_messages": [
        "string"
      ],
      "message": "string",
      "state": "string"
    },
    "ipv4_state": "string",
    "ipv6": {
      "code": 65537300,
      "dn_messages": [
        "string"
      ],
      "message": "string",
```

```
      "state": "string"
    },
    "ipv6_state": "string",
    "message": "string",
    "state": "string"
  },
  "user_dn": "string",
  "user_scope": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

ipv4

Name	Type	Description
code	integer	Code corresponding to the error message. If there is no error, it is 0 to indicate success.
dn_messages	array[string]	
message	string	Provides additional details on the error.
state	string	Status of the LDAP service.

ipv6

Name	Type	Description
code	integer	Code corresponding to the error message. If there is no error, it is 0 to indicate success.
dn_messages	array[string]	
message	string	Provides additional details on the error.
state	string	Status of the LDAP service.

status

Name	Type	Description
code	integer	This field is no longer supported. Use ipv4.code or ipv6.code instead.

Name	Type	Description
dn_message	array[string]	
ipv4	ipv4	
ipv4_state	string	This field is no longer supported. Use ipv4.state instead.
ipv6	ipv6	
ipv6_state	string	This field is no longer supported. Use ipv6.state instead.
message	string	This field is no longer supported. Use ipv4.message or ipv6.message instead.
state	string	The status of the LDAP service for the SVM. The LDAP service is up if either `ipv4_state` or `ipv6_state` is up. The LDAP service is down if both `ipv4_state` and `ipv6_state` are down.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the LDAP configuration for the cluster

PATCH `/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:

1. The server does not have LDAP installed.
2. The server is invalid.
3. The server is unreachable.

Request Body

Name	Type	Description
base_dn	string	Specifies the default base DN for all searches.
base_scope	string	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	Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.
bind_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.
group_dn	string	Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups.

Name	Type	Description
group_membership_filter	string	Specifies the custom filter used for group membership lookups from an LDAP server.
group_scope	string	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	Specifies whether or not netgroup by host querying is enabled.
is_owner	boolean	Specifies whether or not the SVM owns the LDAP client configuration.
ldaps_enabled	boolean	Specifies whether or not LDAPS is enabled.
min_bind_level	string	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups.

Name	Type	Description
netgroup_byhost_scope	string	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.
netgroup_scope	string	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	The port used to connect to the LDAP Servers.
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.

Name	Type	Description
schema	string	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]	
session_security	string	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	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	status	
try_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.
user_dn	string	Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups.

Name	Type	Description
user_scope	string	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


```
{
  "base_dn": "string",
  "base_scope": "string",
  "bind_dn": "string",
  "bind_password": "string",
  "group_dn": "string",
  "group_membership_filter": "string",
  "group_scope": "string",
  "min_bind_level": "string",
  "netgroup_byhost_dn": "string",
  "netgroup_byhost_scope": "string",
  "netgroup_dn": "string",
  "netgroup_scope": "string",
  "port": 389,
  "schema": "string",
  "servers": [
    "string"
  ],
  "session_security": "string",
  "status": {
    "code": 65537300,
    "dn_message": [
      "string"
    ],
    "ipv4": {
      "code": 65537300,
      "dn_messages": [
        "string"
      ],
      "message": "string",
      "state": "string"
    },
    "ipv4_state": "string",
    "ipv6": {
      "code": 65537300,
      "dn_messages": [
        "string"
      ],
      "message": "string",
      "state": "string"
    },
    "ipv6_state": "string",
    "message": "string",
    "state": "string"
```

```
  },
  "user_dn": "string",
  "user_scope": "string"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
4915203	The specified LDAP schema does not exist.
262222	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.

Error Code	Description
4915252	LDAP referral is not supported with STARTTLS, with session security levels sign, seal or with LDAPS.
4915244	RPC failure occurred during validation of the LDAP configuration.
4915265	The specified bind password or bind DN is invalid

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ipv4

Name	Type	Description
code	integer	Code corresponding to the error message. If there is no error, it is 0 to indicate success.
dn_messages	array[string]	
message	string	Provides additional details on the error.
state	string	Status of the LDAP service.

ipv6

Name	Type	Description
code	integer	Code corresponding to the error message. If there is no error, it is 0 to indicate success.
dn_messages	array[string]	
message	string	Provides additional details on the error.
state	string	Status of the LDAP service.

status

Name	Type	Description
code	integer	This field is no longer supported. Use ipv4.code or ipv6.code instead.
dn_message	array[string]	
ipv4	ipv4	

Name	Type	Description
ipv4_state	string	This field is no longer supported. Use ipv4.state instead.
ipv6	ipv6	
ipv6_state	string	This field is no longer supported. Use ipv6.state instead.
message	string	This field is no longer supported. Use ipv4.message or ipv6.message instead.
state	string	The status of the LDAP service for the SVM. The LDAP service is up if either `ipv4_state` or `ipv6_state` is up. The LDAP service is down if both `ipv4_state` and `ipv6_state` are down.

cluster_ldap

Name	Type	Description
base_dn	string	Specifies the default base DN for all searches.
base_scope	string	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	Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.
bind_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.

Name	Type	Description
group_dn	string	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	Specifies the custom filter used for group membership lookups from an LDAP server.
group_scope	string	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	Specifies whether or not netgroup by host querying is enabled.
is_owner	boolean	Specifies whether or not the SVM owns the LDAP client configuration.
ldaps_enabled	boolean	Specifies whether or not LDAPS is enabled.
min_bind_level	string	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups.

Name	Type	Description
netgroup_byhost_scope	string	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.
netgroup_scope	string	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	The port used to connect to the LDAP Servers.
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.

Name	Type	Description
schema	string	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]	
session_security	string	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	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	status	
try_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.
user_dn	string	Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups.

Name	Type	Description
user_scope	string	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

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create the LDAP configuration for the cluster

POST `/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.

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_dn` - Specifies the user that binds to the LDAP servers.
- `base_dn` - Specifies the default base DN for all searches.
- `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:

1. The server does not have LDAP installed.
2. The server is invalid.
3. The server is unreachable.

Request Body

Name	Type	Description
base_dn	string	Specifies the default base DN for all searches.
base_scope	string	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	Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.
bind_dn	string	Specifies the user that binds to the LDAP servers.

Name	Type	Description
bind_password	string	Specifies the bind password for the LDAP servers.
group_dn	string	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	Specifies the custom filter used for group membership lookups from an LDAP server.
group_scope	string	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	Specifies whether or not netgroup by host querying is enabled.
is_owner	boolean	Specifies whether or not the SVM owns the LDAP client configuration.
ldaps_enabled	boolean	Specifies whether or not LDAPS is enabled.
min_bind_level	string	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups.

Name	Type	Description
netgroup_byhost_scope	string	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.
netgroup_scope	string	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	The port used to connect to the LDAP Servers.
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.

Name	Type	Description
schema	string	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]	
session_security	string	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	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	status	
try_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.
user_dn	string	Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups.

Name	Type	Description
user_scope	string	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


```
{
  "base_dn": "string",
  "base_scope": "string",
  "bind_dn": "string",
  "bind_password": "string",
  "group_dn": "string",
  "group_membership_filter": "string",
  "group_scope": "string",
  "min_bind_level": "string",
  "netgroup_byhost_dn": "string",
  "netgroup_byhost_scope": "string",
  "netgroup_dn": "string",
  "netgroup_scope": "string",
  "port": 389,
  "schema": "string",
  "servers": [
    "string"
  ],
  "session_security": "string",
  "status": {
    "code": 65537300,
    "dn_message": [
      "string"
    ],
    "ipv4": {
      "code": 65537300,
      "dn_messages": [
        "string"
      ],
      "message": "string",
      "state": "string"
    },
    "ipv4_state": "string",
    "ipv6": {
      "code": 65537300,
      "dn_messages": [
        "string"
      ],
      "message": "string",
      "state": "string"
    },
    "ipv6_state": "string",
    "message": "string",
    "state": "string"
```

```
  },
  "user_dn": "string",
  "user_scope": "string"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of LDAP records.
records	array[ldap_service]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "ad_domain": "example.com",
      "base_dn": "dc=domainB,dc=example,dc=com",
      "base_scope": "string",
      "bind_dn":
"cn=Administrators,cn=users,dc=domainB,dc=example,dc=com",
      "bind_password": "abc",
      "group_dn": "cn=abc,users,dc=com",
      "group_membership_filter": "",
      "group_scope": "string",
      "min_bind_level": "string",
      "netgroup_byhost_dn": "cn=abc,users,dc=com",
      "netgroup_byhost_scope": "string",
      "netgroup_dn": "cn=abc,users,dc=com",
      "netgroup_scope": "string",
      "port": 389,
      "preferred_ad_servers": [
        "11.11.11.11"
      ],
      "schema": "ad_idmu",
      "servers": [
        [
          "10.10.10.10",
          "domainB.example.com"
        ]
      ],
      "session_security": "string",
      "status": {
        "code": 65537300,
        "dn_message": [
          "string"
        ],
        "ipv4": {
          "code": 65537300,
          "dn_messages": [
            "string"
          ],
          "message": "string",
          "state": "string"
        },
        "ipv4_state": "string",
```

```
        "ipv6": {
          "code": 65537300,
          "dn_messages": [
            "string"
          ],
          "message": "string",
          "state": "string"
        },
        "ipv6_state": "string",
        "message": "string",
        "state": "string"
      },
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "user_dn": "cn=abc,users,dc=com",
      "user_scope": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
4915203	The specified LDAP schema does not exist.
262222	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.

Error Code	Description
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.
4915265	The specified bind password or bind DN is invalid

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ipv4

Name	Type	Description
code	integer	Code corresponding to the error message. If there is no error, it is 0 to indicate success.
dn_messages	array[string]	
message	string	Provides additional details on the error.
state	string	Status of the LDAP service.

ipv6

Name	Type	Description
code	integer	Code corresponding to the error message. If there is no error, it is 0 to indicate success.
dn_messages	array[string]	
message	string	Provides additional details on the error.
state	string	Status of the LDAP service.

status

Name	Type	Description
code	integer	This field is no longer supported. Use ipv4.code or ipv6.code instead.
dn_message	array[string]	
ipv4	ipv4	

Name	Type	Description
ipv4_state	string	This field is no longer supported. Use ipv4.state instead.
ipv6	ipv6	
ipv6_state	string	This field is no longer supported. Use ipv6.state instead.
message	string	This field is no longer supported. Use ipv4.message or ipv6.message instead.
state	string	The status of the LDAP service for the SVM. The LDAP service is up if either `ipv4_state` or `ipv6_state` is up. The LDAP service is down if both `ipv4_state` and `ipv6_state` are down.

cluster_ldap

Name	Type	Description
base_dn	string	Specifies the default base DN for all searches.
base_scope	string	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	Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.
bind_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.

Name	Type	Description
group_dn	string	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	Specifies the custom filter used for group membership lookups from an LDAP server.
group_scope	string	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	Specifies whether or not netgroup by host querying is enabled.
is_owner	boolean	Specifies whether or not the SVM owns the LDAP client configuration.
ldaps_enabled	boolean	Specifies whether or not LDAPS is enabled.
min_bind_level	string	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups.

Name	Type	Description
netgroup_byhost_scope	string	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.
netgroup_scope	string	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	The port used to connect to the LDAP Servers.
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.

Name	Type	Description
schema	string	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]	
session_security	string	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	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	status	
try_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.
user_dn	string	Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups.

Name	Type	Description
user_scope	string	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

svm

SVM, applies only to SVM-scoped objects.

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

ldap_service

Name	Type	Description
ad_domain	string	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	Specifies the default base DN for all searches.

Name	Type	Description
base_scope	string	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	Specifies whether or not CIFS server's credentials are used to bind to the LDAP server.
bind_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.
group_dn	string	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	Specifies the custom filter used for group membership lookups from an LDAP server.
group_scope	string	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	Specifies whether or not netgroup by host querying is enabled.

Name	Type	Description
is_owner	boolean	Specifies whether or not the SVM owns the LDAP client configuration.
ldaps_enabled	boolean	Specifies whether or not LDAPS is enabled.
min_bind_level	string	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	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	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	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.

Name	Type	Description
netgroup_scope	string	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	The port used to connect to the LDAP Servers.
preferred_ad_servers	array[string]	
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.
referral_enabled	boolean	Specifies whether or not LDAP referral is enabled.
restrict_discovery_to_site	boolean	Specifies whether or not LDAP server discovery is restricted to site-scope.
schema	string	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]	

Name	Type	Description
session_security	string	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	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	status	
svm	svm	SVM, applies only to SVM-scoped objects.
try_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.
user_dn	string	Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups.
user_scope	string	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

Name	Type	Description
code	string	Argument code

Name	Type	Description
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage NIS configuration

Manage NIS configuration

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"
```

Delete the NIS configuration for the cluster

DELETE `/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
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the NIS configuration for the cluster

GET `/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

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	

Name	Type	Description
binding_details	array[binding_details]	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]	
domain	string	The NIS domain to which this configuration belongs.
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "binding_details": [
    {
      "server": "string",
      "status": {
        "code": "string",
        "message": "string"
      }
    }
  ],
  "bound_servers": [
    "string"
  ],
  "domain": "string",
  "servers": [
    "string"
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

binding_status

Name	Type	Description
code	string	Code corresponding to the server's binding status.
message	string	Detailed description of the server's binding status.

binding_details

Name	Type	Description
server	string	Hostname/IP address of the NIS server in the domain.
status	binding_status	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Update the NIS configuration for the cluster

PATCH `/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

Name	Type	Description
binding_details	array[binding_details]	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]	
domain	string	The NIS domain to which this configuration belongs.
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

Example request


```
{
  "binding_details": [
    {
      "server": "string",
      "status": {
        "code": "string",
        "message": "string"
      }
    }
  ],
  "bound_servers": [
    "string"
  ],
  "domain": "string",
  "servers": [
    "string"
  ]
}
```


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.

Error Code	Description
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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

binding_status

Name	Type	Description
code	string	Code corresponding to the server's binding status.
message	string	Detailed description of the server's binding status.

binding_details

Name	Type	Description
server	string	Hostname/IP address of the NIS server in the domain.
status	binding_status	

cluster_nis_service

Name	Type	Description
binding_details	array[binding_details]	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]	
domain	string	The NIS domain to which this configuration belongs.
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create the NIS configuration for the cluster

POST `/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. The servers field 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

Name	Type	Description
binding_details	array[binding_details]	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]	
domain	string	The NIS domain to which this configuration belongs.

Name	Type	Description
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

Example request

```
{
  "binding_details": [
    {
      "server": "string",
      "status": {
        "code": "string",
        "message": "string"
      }
    }
  ],
  "bound_servers": [
    "string"
  ],
  "domain": "string",
  "servers": [
    "string"
  ]
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of NIS domain records.
records	array[cluster_nis_service]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "binding_details": [
        {
          "server": "string",
          "status": {
            "code": "string",
            "message": "string"
          }
        }
      ],
      "bound_servers": [
        "string"
      ],
      "domain": "string",
      "servers": [
        "string"
      ]
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1966253	IPv6 is not enabled in the cluster.

Error Code	Description
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.
23724111	Invalid value specified for nis-servers. The value must be a valid hostname or IP address.
23724087	The specified IPv6 address is not supported because it is one of the following: ::, link-local, multicast, v4-compatible, v4-mapped, loopback.
23724086	The specified IPv4 address is not supported because it is one of the following: multicast, loopback, 0.0.0.0 or broadcast.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

binding_status

Name	Type	Description
code	string	Code corresponding to the server's binding status.
message	string	Detailed description of the server's binding status.

binding_details

Name	Type	Description
server	string	Hostname/IP address of the NIS server in the domain.
status	binding_status	

cluster_nis_service

Name	Type	Description
binding_details	array[binding_details]	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]	
domain	string	The NIS domain to which this configuration belongs.
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View and update OAuth 2.0 status

View and update OAuth 2.0 status

Overview

This API is used to enable and disable OAuth 2.0 in the cluster. The PATCH request enables and disables OAuth 2.0 in the cluster.

Examples

Retrieving the OAuth 2.0 status in the cluster

The following output shows the OAuth 2.0 status of the cluster.

```
# The API:
/api/security/authentication/cluster/oauth2

# The call:
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/oauth2"
-H "accept: application/hal+json"

# The response:
{
"enabled": false
}
```

Enabling the OAuth 2.0 in the cluster

The following output shows how to enable the OAuth 2.0 in the cluster.

```
# The API:
/api/security/authentication/cluster/oauth2

# The call:
curl -X PATCH "https://<mgmt-
ip>/api/security/authentication/cluster/oauth2" -H "accept:
application/hal+json" -d '{ "enabled": true }'
```

Retrieve the OAuth 2.0 status

GET `/security/authentication/cluster/oauth2`

Introduced In: 9.14

Retrieves the OAuth 2.0 status.

Related ONTAP commands

- `security oauth2 show`

Parameters

Name	Type	In	Required	Description
enabled	boolean	query	False	Filter by enabled

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
enabled	boolean	Indicates whether OAuth 2.0 is enabled or disabled globally. Default value is false.

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the OAuth 2.0 status

PATCH `/security/authentication/cluster/oauth2`

Introduced In: 9.14

Updates the OAuth 2.0 status.

Related ONTAP commands

- `security oauth2 modify`

Request Body

Name	Type	Description
enabled	boolean	Indicates whether OAuth 2.0 is enabled or disabled globally. Default value is false.

Response

```
Status: 200, Ok
```

Error

```
Status: Default,
```

Definitions

See Definitions

security_oauth2_global

Name	Type	Description
enabled	boolean	Indicates whether OAuth 2.0 is enabled or disabled globally. Default value is false.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View and create OAuth 2.0 configurations

View and create OAuth 2.0 configurations

Overview

This API is used to retrieve and configure relevant information pertaining to the OAuth 2.0 configuration in the cluster. The POST request creates the OAuth 2.0 configuration if there is none present. Various responses are shown in the examples below.

Examples

Retrieving the OAuth 2.0 configuration in the cluster

The following output shows the OAuth 2.0 configuration in the cluster.

```
# The API:
/api/security/authentication/cluster/oauth2/clients

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/authentication/cluster/oauth2/clients" -H "accept:
application/hal+json"

# The response:
{
 "records": [
{
  "name": "auth0"
}
 ],
 "num_records": 1
}
```

Creating the OAuth 2.0 configuration

The following output shows how to create the OAuth 2.0 configuration in the cluster.

```
= The API:

/api/security/authentication/cluster/oauth2/clients

= The call:

curl -X POST "https://+++<mgmt-
ip>+++/api/security/authentication/cluster/oauth2/clients?return_records=t
rue" -H "accept: application/hal+json" -d '{ "name": "name",
"application": "http", "issuer": "https://examplelab.customer.com",
"audience": "aud", "client_id": "client_id", "client_secret": "+++<CLIENT-
SECRET>+++", "introspection": {"endpoint_uri":
"https://examplelab.customer.com/server/endpoint", "interval": "PT1H" },
```

```
"remote_user_claim": "user_claim", "outgoing_proxy":
"https://johndoe:somesecret@proxy.example.com:8080",
"use_local_roles_if_present": false, "use_mutual_tls": "required"
}'+++</CLIENT-SECRET>++++++</mgmt-ip>+++

= The response:

{
"job": {
  "uuid": "e45b123b-c228-11e8-aa20-0050568e36bb",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/e45b123b-c228-11e8-aa20-0050568e36bb"
    }
  }
}
}

'''




[[ID055c4232528a977a0b4f494e70feb659]]
= Retrieve all OAuth 2.0 configurations

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/oauth2/clients`#

*Introduced In:* 9.14

Retrieves all OAuth 2.0 configurations.

== Related ONTAP commands

* `security oauth2 client show`


== Parameters

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

|Name
|Type
|In
```

```
|Required
|Description

|introspection.interval
|string
|query
|False
a|Filter by introspection.interval


|introspection.endpoint_uri
|string
|query
|False
a|Filter by introspection.endpoint_uri


|issuer
|string
|query
|False
a|Filter by issuer


|remote_user_claim
|string
|query
|False
a|Filter by remote_user_claim


|use_mutual_tls
|string
|query
|False
a|Filter by use_mutual_tls


|outgoing_proxy
|string
|query
|False
a|Filter by outgoing_proxy


|client_id
|string
```

```
|query
|False
a|Filter by client_id


|application
|string
|query
|False
a|Filter by application


|audience
|string
|query
|False
a|Filter by audience


|provider
|string
|query
|False
a|Filter by provider

* Introduced in: 9.16


|use_local_roles_if_present
|boolean
|query
|False
a|Filter by use_local_roles_if_present


|hashed_client_secret
|string
|query
|False
a|Filter by hashed_client_secret


|jwks.provider_uri
|string
|query
|False
a|Filter by jwks.provider_uri
```

```
|jwks.refresh_interval
|string
|query
|False
a|Filter by jwks.refresh_interval


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


|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: 15
* 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.


|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|

|num_records
|integer
a|Number of records.


|records
|array[link:#security_oauth2[security_oauth2]]
a|

|===


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

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "application": "string",
      "audience": "string",
      "client_id": "string",
      "hashed_client_secret": "string",
      "introspection": {
        "endpoint_uri":
"https://examplelab.customer.com/token/introspect",
        "interval": "PT1H"
      },
      "issuer": "https://examplelab.customer.com",
      "jwks": {
        "provider_uri": "https://examplelab.customer.com/pf/JWKS",
        "refresh_interval": "PT2H"
      },
      "name": "auth0",
      "outgoing_proxy":
"https://johndoe:secretpass@proxy.example.com:8080",
      "provider": "entra",
      "remote_user_claim": "string",
      "skip_uri_validation": true,
      "use_mutual_tls": "string"
    }
  ]
}
====

== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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|

|===
```

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

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

|endpoint_uri
|string
a|The token introspection endpoint URI.


|interval
|string
a|The refresh interval for caching tokens, in ISO-8601 format. This can be
set to the value "disabled" to disable caching of tokens. When set to 0,
tokens are cached according to the expiry period in them. Otherwise, it
can be set to a value from 1 second to 2147483647 seconds.


|===


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

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

|provider_uri
|string
a|The URI on which the JSON Web Key Set (JWKS) are hosted.


|refresh_interval
|string
a|The refresh interval for the JSON Web Key Set (JWKS), in ISO-8601
format. This can be set to a value from 300 seconds to 2147483647 seconds.
```

```
|===


[#security_oauth2]
[.api-collapsible-fifth-title]
security_oauth2

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

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

|application
|string
a|The name of the application using OAuth 2.0. Required for POST
operations.


|audience
|string
a|The OAuth 2.0 Audience.


|client_id
|string
a|The OAuth 2.0 client ID. Required in POST operations for remote
introspection.


|hashed_client_secret
|string
a|The OAuth 2.0 client secret as a SHA256 HMAC hashed value created with
the cluster UUID as its HMAC secret key.


|introspection
|link:#introspection[introspection]
a|

|issuer
|string
```

```
a|The OAuth 2.0 Issuer.


|jwks
|link:#jwks[jwks]
a|

|name
|string
a|The configuration name. Required for POST operations.


|outgoing_proxy
|string
a|Outgoing proxy to access external identity providers (IdPs). If not
specified, no proxy is configured.


|provider
|string
a|The Identity Provider type.


|remote_user_claim
|string
a|The remote user claim.


|use_local_roles_if_present
|boolean
a|Indicates whether or not to use locally configured roles, if present.
Default value is false.


|use_mutual_tls
|string
a|OAuth 2.0 mutual TLS authentication setting. Set this value to "none" to
disable mutual TLS authentication. Set this value to "required" to enforce
mutual TLS authentication for all access tokens and reject any token that
does not have x5t#S256 property in the cnf section. The default value is
"request" which means mutual TLS authentication is enforced only if the
x5t#S256 property is present in the cnf section of the access token.


|===
```

```
[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID55a6fa7bd5cfc29b51f735afe0a6149c]]
= Create the OAuth 2.0 configuration

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/cluster/oauth2/clients`#

*Introduced In:* 9.14

Creates the OAuth 2.0 configuration.

== Required properties

* `name`
* `application`
* `issuer`

== Optional properties

* `audience`
* `client_id`
* `client_secret`
* `introspection.endpoint_uri`
* `introspection.interval`
* `remote_user_claim`
* `jwks.provider_uri`
* `jwks.refresh_interval`
* `outgoing_proxy`
* `use_local_roles_if_present`
* `skip_uri_validation`
* `use_mutual_tls`
* `provider`

== Related ONTAP commands
```

```
* `security oauth2 client create`


== 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: 0
* 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

|application
|string
a|The name of the application using OAuth 2.0. Required for POST
operations.


|audience
|string
a|The OAuth 2.0 Audience.


|client_id
|string
a|The OAuth 2.0 client ID. Required in POST operations for remote
introspection.


|client_secret
|string
a|The OAuth 2.0 client secret. Required in POST operations for remote
introspection.


|hashed_client_secret
|string
a|The OAuth 2.0 client secret as a SHA256 HMAC hashed value created with
the cluster UUID as its HMAC secret key.


|introspection
|link:#introspection[introspection]
a|

|issuer
|string
a|The OAuth 2.0 Issuer.


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

```
|name
|string
a|The configuration name. Required for POST operations.


|outgoing_proxy
|string
a|Outgoing proxy to access external identity providers (IdPs). If not
specified, no proxy is configured.


|provider
|string
a|The Identity Provider type.


|remote_user_claim
|string
a|The remote user claim.


|skip_uri_validation
|boolean
a|Indicates whether or not to validate the input URIs. Default value is
false.


|use_local_roles_if_present
|boolean
a|Indicates whether or not to use locally configured roles, if present.
Default value is false.


|use_mutual_tls
|string
a|OAuth 2.0 mutual TLS authentication setting. Set this value to "none" to
disable mutual TLS authentication. Set this value to "required" to enforce
mutual TLS authentication for all access tokens and reject any token that
does not have x5t#S256 property in the cnf section. The default value is
"request" which means mutual TLS authentication is enforced only if the
x5t#S256 property is present in the cnf section of the access token.


|===


.Example request
```

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "application": "string",
  "audience": "string",
  "client_id": "string",
  "client_secret": "string",
  "hashed_client_secret": "string",
  "introspection": {
    "endpoint_uri": "https://examplelab.customer.com/token/introspect",
    "interval": "PT1H"
  },
  "issuer": "https://examplelab.customer.com",
  "jwks": {
    "provider_uri": "https://examplelab.customer.com/pf/JWKS",
    "refresh_interval": "PT2H"
  },
  "name": "auth0",
  "outgoing_proxy": "https://johndoe:secretpass@proxy.example.com:8080",
  "provider": "entra",
  "remote_user_claim": "string",
  "use_mutual_tls": "string"
}
====

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

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 203817010
| Client ID is required for remote introspection.

| 203817011
| Client secret is required for remote introspection.

| 203817012
| Client ID and client secret required for remote introspection.

| 203817013
| JWKS URI should not be configured for remote introspection.

| 203817014
| JWKS refresh interval should not be specified for remote introspection.

| 203817015
| The token introspection endpoint is required for remote introspection.

| 203817016
| JWKS refresh interval provided without providing JWKS URI.

| 203817017
| Minimum supported value of JWKS refresh interval is 300 seconds.

| 203817018
| Required parameters for either local validation or remote introspection
are missing. Provide either the JWKS URI for local validation, or metadata
configuration URI or token introspection endpoint with client ID and
secret for remote introspection.

| 203817019
| Failed to add new IDP client because number of maximum supported IDP
clients is already reached.

| 203817020
| Internal error. Failed to validate provider URI.
```

```
| 203817021
| OAuth 2.0 Provider URI validation failed with error.

| 203817022
| OAuth 2.0 Provider JWKS URI validation failed. Received empty response
message from the JWKS URI.

| 203817023
| OAuth 2.0 Provider JWKS URI validation failed. No keys were found in
response message received from the JWKS URI.

| 203817024
| Internal error. Unable to allocate memory for CURL response.

| 203817025
| Maximum value of JWKS refresh interval is 2147483647 seconds.

| 203817033
| OAuth 2.0 Provider Introspection endpoint validation failed. Received
empty response message from the Introspection endpoint.

| 203817034
| OAuth 2.0 Provider Introspection endpoint validation failed. Received
invalid response message for Introspection request.

| 203817037
| An entry cannot be created as another entry with the same configuration
name has the same issuer and audience.

| 203817042
| Maximum value of introspection interval is 2147483647 seconds.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#introspection]
[.api-collapsible-fifth-title]
introspection

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

|endpoint_uri
|string
a|The token introspection endpoint URI.


|interval
|string
a|The refresh interval for caching tokens, in ISO-8601 format. This can be
set to the value "disabled" to disable caching of tokens. When set to 0,
tokens are cached according to the expiry period in them. Otherwise, it
can be set to a value from 1 second to 2147483647 seconds.


|===


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

```
jwks

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

|provider_uri
|string
a|The URI on which the JSON Web Key Set (JWKS) are hosted.


|refresh_interval
|string
a|The refresh interval for the JSON Web Key Set (JWKS), in ISO-8601
format. This can be set to a value from 300 seconds to 2147483647 seconds.


|===


[#security_oauth2]
[.api-collapsible-fifth-title]
security_oauth2

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

|application
|string
a|The name of the application using OAuth 2.0. Required for POST
operations.


|audience
|string
a|The OAuth 2.0 Audience.


|client_id
|string
a|The OAuth 2.0 client ID. Required in POST operations for remote
introspection.
```

```
|client_secret
|string
a|The OAuth 2.0 client secret. Required in POST operations for remote
introspection.


|hashed_client_secret
|string
a|The OAuth 2.0 client secret as a SHA256 HMAC hashed value created with
the cluster UUID as its HMAC secret key.


|introspection
|link:#introspection[introspection]
a|

|issuer
|string
a|The OAuth 2.0 Issuer.


|jwks
|link:#jwks[jwks]
a|

|name
|string
a|The configuration name. Required for POST operations.


|outgoing_proxy
|string
a|Outgoing proxy to access external identity providers (IdPs). If not
specified, no proxy is configured.


|provider
|string
a|The Identity Provider type.


|remote_user_claim
|string
a|The remote user claim.
```

```
|skip_uri_validation
|boolean
a|Indicates whether or not to validate the input URIs. Default value is
false.


|use_local_roles_if_present
|boolean
a|Indicates whether or not to use locally configured roles, if present.
Default value is false.


|use_mutual_tls
|string
a|OAuth 2.0 mutual TLS authentication setting. Set this value to "none" to
disable mutual TLS authentication. Set this value to "required" to enforce
mutual TLS authentication for all access tokens and reject any token that
does not have x5t#S256 property in the cnf section. The default value is
"request" which means mutual TLS authentication is enforced only if the
x5t#S256 property is present in the cnf section of the access token.


|===


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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 delete an OAuth 2.0 configuration

:leveloffset: +1


[[ID07fa2c291e9eb1f6d381e0daaeb7098f]]
= View and delete an OAuth 2.0 configuration



== Overview

This API is used to retrieve and delete the OAuth 2.0 configuration in the
cluster. The GET request retrieves the OAuth 2.0 configuration. The DELETE
request removes the OAuth 2.0 configuration.  Various responses are shown
in the examples below.
 +

'''

== Examples

=== Retrieving the OAuth 2.0 configuration in the cluster

The following output shows the OAuth 2.0 configuration in the cluster.
 +

'''

----

# The API:
```

```
/api/security/authentication/cluster/oauth2/clients/{name}

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/authentication/cluster/oauth2/clients/auth0" -H "accept:
application/hal+json"

# The response:
{
"name": "auth0",
"application": "http",
"issuer": "https://examplelab.customer.com",
"audience": "aud",
"client_id": "client_id",
"hashed_client_secret": "<HASHED-CLIENT-SECRET>",
"introspection": {
  "endpoint_uri": "https://examplelab.customer.com/server/endpoint",
  "interval": "PT1H"
},
"remote_user_claim": "user_claim",
"jwks": {
  "provider_uri": "https://examplelab.customer.com/pf/JWKS",
  "refresh_interval": "PT1H"
},
"use_local_roles_if_present": false,
"outgoing_proxy": "https://johndoe:secretpass@proxy.example.com:8080",
"_links": {
  "self": {
    "href": "/api/security/authentication/cluster/oauth2/clients"
  }
},
"use_mutual_tls": "required"
}
----

'''

=== Deleting the OAuth 2.0 configuration

'''

----

# The API:
/api/security/authentication/cluster/oauth2/clients/{name}
```

```
# The call:
curl -X DELETE "https://<mgmt-
ip>/api/security/authentication/cluster/oauth2/clients/auth0"
----

'''




[[IDeaac7db0658128007899ed905032c64a]]
= Delete an OAuth 2.0 configuration

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/cluster/oauth2/clients/{name}`#

*Introduced In:* 9.14

Deletes the OAuth 2.0 configuration with the specified name.

== Required properties

***** `config_name`

== Related ONTAP commands

* `security oauth2 client delete`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|name
|string
|path
|True
a|OAuth 2.0 configuration name.
```

```
|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 203816995
| OAuth 2.0 must be disabled before the configuration can be removed.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID7ef5bcac3419dc64f858b413df483433]]
= Retrieve an OAuth 2.0 configuration with the specified name

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/oauth2/clients/{name}`#

*Introduced In:* 9.14

Retrieves the OAuth 2.0 configuration with the specified name.

== Related ONTAP commands

* `security oauth2 client show`
```

```
== Parameters

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

|Name
|Type
|In
|Required
|Description

|name
|string
|path
|True
a|OAuth 2.0 configuration name.


|introspection.interval
|string
|query
|False
a|Filter by introspection.interval


|introspection.endpoint_uri
|string
|query
|False
a|Filter by introspection.endpoint_uri


|issuer
|string
|query
|False
a|Filter by issuer


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

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


|outgoing_proxy
|string
|query
|False
a|Filter by outgoing_proxy


|client_id
|string
|query
|False
a|Filter by client_id


|application
|string
|query
|False
a|Filter by application


|audience
|string
|query
|False
a|Filter by audience


|provider
|string
|query
|False
a|Filter by provider

* Introduced in: 9.16


|use_local_roles_if_present
|boolean
|query
```

```
|False
a|Filter by use_local_roles_if_present


|hashed_client_secret
|string
|query
|False
a|Filter by hashed_client_secret


|jwks.provider_uri
|string
|query
|False
a|Filter by jwks.provider_uri


|jwks.refresh_interval
|string
|query
|False
a|Filter by jwks.refresh_interval


|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
|string
a|The name of the application using OAuth 2.0. Required for POST
operations.


|audience
|string
a|The OAuth 2.0 Audience.


|client_id
|string
a|The OAuth 2.0 client ID. Required in POST operations for remote
introspection.


|hashed_client_secret
|string
a|The OAuth 2.0 client secret as a SHA256 HMAC hashed value created with
the cluster UUID as its HMAC secret key.


|introspection
|link:#introspection[introspection]
a|

|issuer
|string
a|The OAuth 2.0 Issuer.


|jwks
|link:#jwks[jwks]
a|

|name
|string
a|The configuration name. Required for POST operations.


|outgoing_proxy
|string
a|Outgoing proxy to access external identity providers (IdPs). If not
specified, no proxy is configured.
```

```
|provider
|string
a|The Identity Provider type.


|remote_user_claim
|string
a|The remote user claim.


|use_local_roles_if_present
|boolean
a|Indicates whether or not to use locally configured roles, if present.
Default value is false.


|use_mutual_tls
|string
a|OAuth 2.0 mutual TLS authentication setting. Set this value to "none" to
disable mutual TLS authentication. Set this value to "required" to enforce
mutual TLS authentication for all access tokens and reject any token that
does not have x5t#S256 property in the cnf section. The default value is
"request" which means mutual TLS authentication is enforced only if the
x5t#S256 property is present in the cnf section of the access token.


|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "application": "string",
  "audience": "string",
  "client_id": "string",
  "hashed_client_secret": "string",
  "introspection": {
    "endpoint_uri": "https://examplelab.customer.com/token/introspect",
    "interval": "PT1H"
```

```
  },
  "issuer": "https://examplelab.customer.com",
  "jwks": {
    "provider_uri": "https://examplelab.customer.com/pf/JWKS",
    "refresh_interval": "PT2H"
  },
  "name": "auth0",
  "outgoing_proxy": "https://johndoe:secretpass@proxy.example.com:8080",
  "provider": "entra",
  "remote_user_claim": "string",
  "skip_uri_validation": true,
  "use_mutual_tls": "string"
}
====

== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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|

|===
```

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

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

|endpoint_uri
|string
a|The token introspection endpoint URI.


|interval
|string
a|The refresh interval for caching tokens, in ISO-8601 format. This can be
set to the value "disabled" to disable caching of tokens. When set to 0,
tokens are cached according to the expiry period in them. Otherwise, it
can be set to a value from 1 second to 2147483647 seconds.


|===


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

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

|provider_uri
|string
a|The URI on which the JSON Web Key Set (JWKS) are hosted.


|refresh_interval
|string
a|The refresh interval for the JSON Web Key Set (JWKS), in ISO-8601
format. This can be set to a value from 300 seconds to 2147483647 seconds.
```

```
|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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


[[ID6ab5dec4adde4a0ead5d020cb82a07ce]]
= Manage SAML service



== 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"
},
"_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/"
----

'''
```

```
[[IDd29ab60759df8c706f2032d5addef758]]
= Delete an 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.

| 12320832
| Internal Error. Failed to execute the command, web server setup is in
progress. Retry after some time.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

```
|Type
|Description

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
```

```
====



[[IDba53ddcda9541a08f07bc5ba449744ab]]
= Retrieve an 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

|certificate.serial_number
|string
|query
|False
a|Filter by certificate.serial_number

* maxLength: 40
* minLength: 1
* Introduced in: 9.7


|certificate.ca
|string
|query
|False
a|Filter by certificate.ca

* maxLength: 256
* minLength: 1
* Introduced in: 9.7
```

```
|certificate.common_name
|string
|query
|False
a|Filter by certificate.common_name

* Introduced in: 9.7


|host
|string
|query
|False
a|Filter by host

* Introduced in: 9.7


|enabled
|boolean
|query
|False
a|Filter by enabled

* Introduced in: 9.7


|idp_uri
|string
|query
|False
a|Filter by idp_uri

* 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": {
    "ca": "string",
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "host": "string",
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-
06/FederationMetadata.xml"
}
====

== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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
```

```
|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID2958ac3b3162bc0bc33fffcaa7f42161]]
= Update an 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

|enabled
|boolean
a|The SAML service provider is enabled.  Valid for PATCH and GET
operations only.


|===


== 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.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.
```

```
== 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
[#certificate]
[.api-collapsible-fifth-title]
certificate
[#security_saml_sp]
[.api-collapsible-fifth-title]
security_saml_sp

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

|enabled
|boolean
a|The SAML service provider is enabled.  Valid for PATCH and GET
operations only.
```

```
|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID1f0adc6f38451e7a789dd5375f25cfa3]]
= Create an 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: 0
* Max value: 120
* Min value: 0

|===

== Request Body



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

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

```
|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]
{
  "certificate": {
    "ca": "string",
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "enabled": true,
  "host": "string",
  "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": {
    "uuid": "string"
  }
}
====

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== 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.

| 12320819
| Use the HTTPS scheme for the `idp_uri` or set `verify_metadata_server`
to false.

| 12320820
| No certificate is installed with the specified `certificate.ca` and
`certificate.serial`.

| 12320821
| No certificate is installed with the specified
```

```
`certificate.common_name`.

| 12320823
| 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.

| 12320827
| The certificate authority specified in the default metadata
configuration does not match the provided certificate authority.

| 12320828
| The SAML service provider host specified in the default metadata
configuration does not match the provided SAML service provider host.

| 12320829
| The certificate serial number specified in the default metadata
configuration does not match the provided certificate serial number.

| 12320830
| The certificate common name specified in the default metadata
configuration does not match the provided certificate common name.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#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

|certificate
|link:#certificate[certificate]
a|

|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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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 default metadata configuration

:leveloffset: +1


[[ID0e7241800be7c4db209d8a6fd0397f77]]
= Manage SAML default metadata configuration



== Overview

This API is used to manage relevant information about the SAML default
metadata configuration in the cluster. The POST request creates a SAML
default metadata configuration if there is none present.  The DELETE
request removes the SAML default metadata configuration.  Various
responses are shown in the examples below.
 +

'''

== Examples

=== Retrieving the SAML default metadata configuration in the cluster

The following output shows the SAML default metadata configuration in the
cluster.
 +

'''

----

# The API:
/api/security/authentication/cluster/saml-sp/default-metadata

# The call:
```

```
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/saml-
sp/default-metadata" -H "accept: application/hal+json"

# The response:
{
"host": "172.21.74.181",
"certificate": {
  "ca": "cluster-1",
  "serial_number": "180E3331A0DC5A19",
  "common_name": "cluster-1"
},
"scope": "cluster",
"_links": {
  "self": {
    "href": "/api/security/authentication/cluster/saml-sp/default-
metadata"
  }
}
}
----

'''

=== Creating the SAML default metadata configuration in the cluster

The following output shows how to create the SAML default metadata in the
cluster.
 +

'''

----

# The API:
/api/security/authentication/cluster/saml-sp/default-metadata

# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/saml-
sp/default-metadata?return_records=true" -H "accept: application/hal+json"
-d '{ "host": "172.21.74.181", "certificate": { "ca": "cluster1",
"serial_number": "156F10C3EB4C51C1" }}'
----

'''

=== Deleting the SAML default metadata configuration in the cluster
```

```
'''

----

# The API:
/api/security/authentication/cluster/saml-sp/default-metadata

# The call:
curl -X DELETE "https://<mgmt-
ip>/api/security/authentication/cluster/saml-sp/default-metadata/"
----

'''




[[ID39191a03f5ae55cf5793498502156ce8]]
= Delete the SAML default metadata configuration

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/cluster/saml-sp/default-metadata`#

*Introduced In:* 9.17

Deletes the SAML default metadata configuration.


== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 12320817
| Internal Error. The SAML service provider metadata configuration is
being created, but is taking longer than expected to complete.
```

```
| 12320826
| SAML configuration already exists. Cannot delete the metadata when SAML
configuration is already present.

| 12320832
| Internal Error. Failed to execute the command, web server setup is in
progress. Retry after some time.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID587d05d271b7a35282d317f5310a265b]]
= Retrieve the SAML default metadata configuration

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/saml-sp/default-metadata`#

*Introduced In:* 9.17

Retrieves the SAML default metadata configuration.


== Parameters

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

|Name
|Type
|In
|Required
|Description

|certificate.serial_number
|string
```

```
|query
|False
a|Filter by certificate.serial_number

* maxLength: 40
* minLength: 1


|certificate.common_name
|string
|query
|False
a|Filter by certificate.common_name


|certificate.ca
|string
|query
|False
a|Filter by certificate.ca

* maxLength: 256
* minLength: 1


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


|host
|string
|query
|False
a|Filter by host


|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|

|host
|string
a|The SAML service provider host.


|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"
    }
  },
  "certificate": {
    "ca": "string",
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
```

```
  },
  "host": "string",
  "scope": "string"
}
====

== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDa974b9e3a39b98f64cb92fc1aa30850b]]
= Create the SAML default metadata configuration


[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/cluster/saml-sp/default-metadata`#

*Introduced In:* 9.17

Creates the SAML default metadata configuration. Note that `common_name`
is mutually exclusive with `serial_number` and `ca` in POST requests.
```

```
== Optional properties

* `certificate`
* `host`


== 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: 0
* Max value: 120
* Min value: 0

|===

== Request Body



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

|certificate
|link:#certificate[certificate]
```

```
a|

|host
|string
a|The SAML service provider host.


|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]
{
  "certificate": {
    "ca": "string",
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "host": "string",
  "scope": "string"
}
====

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

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 12320794
| Invalid host parameter for default metadata generation. The host
parameter 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.

| 12320805
| The certificate information provided does not match any installed
certificates.

| 12320806
| The certificate information entered does not match any installed
certificates.

| 12320820
| No certificate is installed with the specified `certificate.ca` and
`certificate.serial`.

| 12320821
| No certificate is installed with the specified
`certificate.common_name`.

| 12320825
| SAML configuration already exists. Cannot create the metadata when SAML
configuration is already present.

| 12320831
| Default metadata configuration already exists.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#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_def_metadata]
[.api-collapsible-fifth-title]
security_saml_def_metadata

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

|certificate
|link:#certificate[certificate]
a|

|host
|string
a|The SAML service provider host.


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


|===


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

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

```
|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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 create Duo groups

:leveloffset: +1


[[IDe7898a381bbc65c1b9cdb879215a48c1]]
= View and create Duo groups



== Overview

This API configures the group to be included in Duo authentication.

== Examples

=== Creating a Duo group

Specify the group name and other necessary information in the body of the
POST request. The owner.uuid or owner.name are not required for a cluster-
```

```
scoped account.

----

# The API:
POST "/api/security/authentication/duo/groups"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/duo/groups --request
POST --data '{"name": "test",  "comment": "test post"}'

# The response:
{
}
----

=== Creating a Duo group for SVM-scoped account

For an 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
group. These parameters indicate the SVM that contains the user group 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/duo/groups"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/duo/groups --request
POST --data '{"name": "test",  "comment": "test post", "owner.name":"vs0"
}'

# The response:
{
}
----

=== Retrieving the configured Duo groups

Retrieves the Duo groups associated with the owners or filtered list (for
a specific SVM and so on).

----

# The API:
```

```
GET "/api/security/authentication/duo/groups"

# The call to retrieve Duo groups with the cluster or SVM:
curl -k https://<mgmt-ip>/api/security/authentication/duo/groups

# the response:
{
"records": [
{
  "owner": {
  "uuid": "5f618c80-d90a-11ed-a6e6-0050568e8ef2",
  "name": "vs0"
}
},
{
"owner": {
"uuid": "f810005a-d908-11ed-a6e6-0050568e8ef2",
"name": "cluster-1"
}
}
],
"num_records": 2
}
----




[[ID555bd99833951febfb034f2bcc88d22c]]
= Retrieve the configured groups

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

*Introduced In:* 9.14

Retrieves the configured groups.

== Related ONTAP commands

* `security login duo group show`

== Learn more

* xref:{relative_path}view_and_create_duo_groups.html[DOC
/security/authentication/duo/groups]
```

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


== Parameters

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

|Name
|Type
|In
|Required
|Description

|owner.name
|string
|query
|False
a|Filter by owner.name


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


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


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


|excluded_users
|string
|query
|False
```

```
a|Filter by excluded_users


|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: 15
* 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:#duogroup[duogroup]]
a|

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
```

```
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "comment": "string",
      "excluded_users": [
        "user1",
        "user2"
      ],
      "name": "AD_Group",
      "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:#returned_error[returned_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

SVM name and UUID for which the Duo group profile is configured.


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

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

```
|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

Group profile to include in Duo authentication.


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

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

|comment
|string
a|Comment for the Duo group.


|excluded_users
|array[string]
a|List of excluded users.


|name
|string
a|Name of the group to be included in Duo authentication.
```

```
|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo group profile 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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDb5f9f0a46f5734424f296b63e94a48bc]]
= Create a Duo group

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/duo/groups`#

*Introduced In:* 9.14

Creates a Duo group.

== Required properties

* `name` - Group name

== Related ONTAP commands

* `security login duo group create`

== Learn more

* xref:{relative_path}view_and_create_duo_groups.html[DOC
/security/authentication/duo/groups]
* xref:{relative_path}manage_security-related_accounts.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

|comment
|string
a|Comment for the Duo group.


|excluded_users
|array[string]
a|List of excluded users.


|name
|string
a|Name of the group to be included in Duo authentication.
```

```
|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo group profile is configured.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "comment": "string",
  "excluded_users": [
    "user1",
    "user2"
  ],
  "name": "AD_Group",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
====

== Response
```

Status: 201, Created

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

|num_records
|integer
a|Number of records.


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

|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "num_records": 1,
  "records": [
    {
      "comment": "string",
      "excluded_users": [
        "user1",
        "user2"
      ],
      "name": "AD_Group",
      "owner": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
====

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Error
```

Status: Default, Error

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

SVM name and UUID for which the Duo group profile is configured.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
```

```
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

Group profile to include in Duo authentication.


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

|comment
|string
a|Comment for the Duo group.


|excluded_users
|array[string]
a|List of excluded users.


|name
|string
a|Name of the group to be included in Duo authentication.


|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo group profile 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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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 Duo groups configured for an SVM or cluster

:leveloffset: +1


[[IDe381430f5fb8461eebfd27b43002ae67]]
= Manage Duo groups configured for an SVM or cluster



== Overview

This API configures the Duo group for an SVM.
Specify the owner UUID. The owner UUID corresponds to the UUID of the SVM
containing the Duo groups and can be obtained from the response body of
the GET request performed on the API "`/api/svm/svms".

== Examples

=== Retrieving the specific configured Duo group(s) of the cluster or SVM

----

# The API:
GET "/api/security/authentication/duo/groups/{owner.uuid}/{group-name}"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/duo/groups/f810005a-
d908-11ed-a6e6-0050568e8ef2/test

# the response:
{
"owner": {
```

```
"uuid": "f810005a-d908-11ed-a6e6-0050568e8ef2",
"name": "cluster-1"
},
"name": "test",
"excluded_users": [
   "tsmith",
   "msmith"
],
"comment": "test group create"
}
----

=== Modifying a Duo group

----

# The API:
PATCH "/api/security/authentication/duo/groups/{owner.uuid}/{group-name}"

# The call:
curl -k "https://<mgmt-
ip>/api/security/authentication/duo/groups/f810005a-d908-11ed-a6e6-
0050568e8ef2/test" --request PATCH --data "{\"comment\": \"Testing\"}"

# the response:
{}
----

=== Deleting a  Duo group

----

# The API:
DELETE "/api/security/authentication/duo/groups/{owner.uuid}/{group-name}"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/duo/groups/f810005a-
d908-11ed-a6e6-0050568e8ef2/test --request DELETE

# the response:
{}
----
```

```
[[ID163c2ea998d0791333c82a96b2a4b66b]]
= Delete a Duo group configured for an SVM or cluster

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

*Introduced In:* 9.14

Deletes a Duo group of the SVM or cluster.

== Related ONTAP commands

* `security login duo group delete`

== Learn more

*
xref:{relative_path}manage_duo_groups_configured_for_an_svm_or_cluster.htm
l[DOC /security/authentication/duo/groups/{owner.uuid}/\{name}]
* xref:{relative_path}manage_security-related_accounts.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|Group name.
```

```
|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID886ef7138650e3e56a3caab808a41e90]]
= Retrieve the Duo group configured for an SVM or cluster

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

*Introduced In:* 9.14

Retrieves the Duo group configured for an SVM or cluster.

== Related ONTAP commands

* `security login duo group show`

== Learn more

*
xref:{relative_path}manage_duo_groups_configured_for_an_svm_or_cluster.htm
l[DOC /security/authentication/duo/groups/{owner.uuid}/\{name}]
* xref:{relative_path}manage_security-related_accounts.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|Group 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|

|comment
|string
a|Comment for the Duo group.
```

```
|excluded_users
|array[string]
a|List of excluded users.


|name
|string
a|Name of the group to be included in Duo authentication.


|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo group profile is configured.


|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "comment": "string",
  "excluded_users": [
    "user1",
    "user2"
  ],
  "name": "AD_Group",
  "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:#returned_error[returned_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

SVM name and UUID for which the Duo group profile is configured.


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

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

```
|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID88ae89f9348801cafd8d860ccf6d39c7]]
= Update a Duo group configured for an SVM or cluster

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

*Introduced In:* 9.14

Updates a configured Duo group for a cluster or SVM.

== Related ONTAP commands

* `security login duo group modify`

== Learn more

*
xref:{relative_path}manage_duo_groups_configured_for_an_svm_or_cluster.htm
```

```
l[DOC /security/authentication/duo/groups/{owner.uuid}/\{name}]
* xref:{relative_path}manage_security-related_accounts.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|Group name.

|===

== Request Body



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

|comment
|string
a|Comment for the Duo group.


|excluded_users
```

```
|array[string]
a|List of excluded users.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "comment": "string",
  "excluded_users": [
    "user1",
    "user2"
  ]
}
====

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

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

SVM name and UUID for which the Duo group profile is configured.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

Group profile to include in Duo authentication.


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

```
|Type
|Description

|comment
|string
a|Comment for the Duo group.


|excluded_users
|array[string]
a|List of excluded users.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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 create a Duo profile

:leveloffset: +1


[[ID0bd8f1423190c0ace6c66cb2810e4572]]
= View and create a Duo profile



== Overview

This API configures the Duo profile for secure shell (SSH).
```

```
== Examples

=== Creating a Duo profile

Specify the integration key, secret key, API host, and other necessary
information in the body of the POST request. The owner.uuid or owner.name
are not required for a cluster-scoped account.

----

# The API:
POST "/api/security/authentication/duo/profiles"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/duo/profiles
--request POST --data '{"api_host": "api-******.duosecurity.com",
"comment": "test post",  "fail_mode": "safe",  "integration_key":
"<INTEGRATION-KEY>", "secret_key": "<SECRET-KEY>"}'

# The response:
{
}
----

=== Creating a Duo profile for an SVM-scoped account

For an 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 Duo
profile. These parameters indicate the SVM that the Duo profile is being
created on 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/duo/profiles"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/duo/profiles
--request POST --data '{"api_host": "api-******.duosecurity.com",
"comment": "test post",  "fail_mode": "safe",  "integration_key":
"<INTEGRATION-KEY>", "secret_key": "<SECRET-KEY>", "owner.name":"vs0" }'

# The response:
{
}
----
```

```
=== Retrieving the configured Duo profile(s)

Retrieves the Duo profiles associated with the owners or filtered list
(for a specific SVM and so on).

----

# The API:
GET "/api/security/authentication/duo/profiles"

# The call to retrieve Duo profiles associated with Duo configured cluster
or SVM:
curl -k https://<mgmt-ip>/api/security/authentication/duo/profiles

# the response:
{
"records": [
{
  "owner": {
  "uuid": "5f618c80-d90a-11ed-a6e6-0050568e8ef2",
  "name": "vs0"
}
},
{
"owner": {
"uuid": "f810005a-d908-11ed-a6e6-0050568e8ef2",
"name": "tsmithcluster-1"
}
}
],
"num_records": 2
}
----




[[ID9c0dbab92480b9acc957e410acdce74f]]
= Retrieve configured Duo profiles

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

*Introduced In:* 9.14
```

```
Retrieves the configured Duo profiles.

== Related ONTAP commands

* `security login duo show`

== Learn more

* xref:{relative_path}view_and_create_a_duo_profile.html[DOC
/security/authentication/duo/profiles]
* xref:{relative_path}manage_security-related_accounts.html[DOC
/security/accounts]


== Parameters

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

|Name
|Type
|In
|Required
|Description

|is_enabled
|boolean
|query
|False
a|Filter by is_enabled


|api_host
|string
|query
|False
a|Filter by api_host


|http_proxy
|string
|query
|False
a|Filter by http_proxy


|comment
```

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


|owner.name
|string
|query
|False
a|Filter by owner.name


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


|max_prompts
|integer
|query
|False
a|Filter by max_prompts

* Max value: 3
* Min value: 1


|integration_key
|string
|query
|False
a|Filter by integration_key


|auto_push
|boolean
|query
|False
a|Filter by auto_push


|status
|string
|query
```

```
|False
a|Filter by status


|fingerprint
|string
|query
|False
a|Filter by fingerprint


|fail_mode
|string
|query
|False
a|Filter by fail_mode


|push_info
|boolean
|query
|False
a|Filter by push_info


|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: 15


|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:#duo[duo]]
```

```
a|

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "api_host": "api-****.duo.com",
      "auto_push": 1,
      "comment": "string",
      "fail_mode": "safe",
      "fingerprint": "string",
      "http_proxy": "IPaddress:port",
      "integration_key": "string",
      "is_enabled": 1,
      "max_prompts": 1,
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "push_info": 1,
      "status": "OK"
```

```
    }
  ]
}
====

== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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

SVM name and UUID for which the Duo profile is configured.


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

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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

Duo profile for the SVM or cluster-management server (Cserver).
```

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

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

|api_host
|string
a|The URL at which the Duo API is hosted.


|auto_push
|boolean
a|Automatically sends a push notification for authentication when using
Duo.


|comment
|string
a|Comment for the Duo profile.


|fail_mode
|string
a|Determines the behavior of the system when it cannot communicate with
the Duo service.


|fingerprint
|string
a|The SHA fingerprint corresponding to the Duo secret key.


|http_proxy
|string
a|Specifies the HTTP proxy server to be used when connecting to the Duo
service.


|integration_key
|string
a|The Integration Key associated with the Duo profile.
```

```
|is_enabled
|boolean
a|Indicates whether the Duo authentication feature is active or inactive.


|max_prompts
|integer
a|The maximum number of authentication attempts allowed for a user before
the process is terminated.


|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo profile is configured.


|push_info
|boolean
a|Additional information sent along with the push notification for Duo
authentication.


|status
|string
a|Information on the reachability status of Duo.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID2eedce2d597476fec2e2a4b388be1f48]]
```

```
= Create a Duo profile

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/duo/profiles`#

*Introduced In:* 9.14

Creates a Duo profile.

== Required properties

* `api_host` - Duo API host
* `integration_key` - Integration key
* `secret_key` - Secret key

== Related ONTAP commands

* `security login duo create`

== Learn more

* xref:{relative_path}view_and_create_a_duo_profile.html[DOC
/security/authentication/duo/profiles]
* xref:{relative_path}manage_security-related_accounts.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

|api_host
|string
a|The URL at which the Duo API is hosted.


|auto_push
|boolean
a|Automatically sends a push notification for authentication when using
Duo.


|comment
|string
a|Comment for the Duo profile.


|fail_mode
|string
a|Determines the behavior of the system when it cannot communicate with
the Duo service.


|fingerprint
|string
a|The SHA fingerprint corresponding to the Duo secret key.


|http_proxy
|string
a|Specifies the HTTP proxy server to be used when connecting to the Duo
service.


|integration_key
|string
a|The Integration Key associated with the Duo profile.
```

```
|is_enabled
|boolean
a|Indicates whether the Duo authentication feature is active or inactive.


|max_prompts
|integer
a|The maximum number of authentication attempts allowed for a user before
the process is terminated.


|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo profile is configured.


|push_info
|boolean
a|Additional information sent along with the push notification for Duo
authentication.


|secret_key
|string
a|The Secret Key associated with the Duo profile.


|status
|string
a|Information on the reachability status of Duo.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "api_host": "api-****.duo.com",
  "auto_push": 1,
  "comment": "string",
  "fail_mode": "safe",
  "fingerprint": "string",
```

```
  "http_proxy": "IPaddress:port",
  "integration_key": "string",
  "is_enabled": 1,
  "max_prompts": 1,
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "push_info": 1,
  "secret_key": "string",
  "status": "OK"
}
====

== Response
```

Status: 201, Created

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

|num_records
|integer
a|Number of records.


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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "num_records": 1,
  "records": [
    {
      "api_host": "api-****.duo.com",
      "auto_push": 1,
```

```
      "comment": "string",
      "fail_mode": "safe",
      "fingerprint": "string",
      "http_proxy": "IPaddress:port",
      "integration_key": "string",
      "is_enabled": 1,
      "max_prompts": 1,
      "owner": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "push_info": 1,
      "secret_key": "string",
      "status": "OK"
    }
  ]
}
====

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Error
```

Status: Default, Error

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

SVM name and UUID for which the Duo profile is configured.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.
```

```
|===


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

Duo profile for the SVM or cluster-management server (Cserver).


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

|api_host
|string
a|The URL at which the Duo API is hosted.


|auto_push
|boolean
a|Automatically sends a push notification for authentication when using
Duo.


|comment
|string
a|Comment for the Duo profile.


|fail_mode
|string
a|Determines the behavior of the system when it cannot communicate with
the Duo service.


|fingerprint
|string
a|The SHA fingerprint corresponding to the Duo secret key.


|http_proxy
|string
a|Specifies the HTTP proxy server to be used when connecting to the Duo
service.
```

```
|integration_key
|string
a|The Integration Key associated with the Duo profile.


|is_enabled
|boolean
a|Indicates whether the Duo authentication feature is active or inactive.


|max_prompts
|integer
a|The maximum number of authentication attempts allowed for a user before
the process is terminated.


|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo profile is configured.


|push_info
|boolean
a|Additional information sent along with the push notification for Duo
authentication.


|secret_key
|string
a|The Secret Key associated with the Duo profile.


|status
|string
a|Information on the reachability status of Duo.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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 Duo profiles for an SVM or cluster

:leveloffset: +1


[[ID89d84f116969df9283c50e04118871d4]]
= Manage Duo profiles for an SVM or cluster



== Overview

This API configures the Duo profile for an SVM.
Specify the owner UUID. The owner UUID corresponds to the UUID of the SVM
containing the Duo profile and can be obtained from the response body of
the GET request performed on the API "`/api/svm/svms".

== Examples

=== Retrieving the specific configured Duo profile of the cluster or SVM

----

# The API:
GET "/api/security/authentication/duo/profiles/{owner.uuid}"

# The call:
curl -k https://<mgmt-
ip>/api/security/authentication/duo/profiles/f810005a-d908-11ed-a6e6-
0050568e8ef2

# the response:
{
"owner": {
"uuid": "f810005a-d908-11ed-a6e6-0050568e8ef2",
```

```
"name": "cluster-1"
},
"integration_key": "<INTEGRATION-KEY>",
"fingerprint": "<FINGERPRINT>",
"api_host": "api-******.duosecurity.com",
"status": "Ok",
"is_enabled": true,
"auto_push": true,
"push_info": true,
"fail_mode": "safe",
"max_prompts": 1,
"comment": "Duo profile for Cserver",
}
----

=== Modifying the Duo profile

----

# The API:
PATCH "/api/security/authentication/duo/profiles/{owner.uuid}"

# The call:
curl -k "https://<mgmt-
ip>/api/security/authentication/duo/profiles/f810005a-d908-11ed-a6e6-
0050568e8ef2" --request PATCH --data "{  \"comment\": \"Testing\",
\"auto_push\": false}"

# the response:
{}
----

=== Deleting the Duo profile

----

# The API:
DELETE "/api/security/authentication/duo/profiles/{owner.uuid}"

# The call:
curl -k https://<mgmt-
ip>/api/security/authentication/duo/profiles/f810005a-d908-11ed-a6e6-
0050568e8ef2 --request DELETE

# the response:
{}
----
```

```
[[IDcda30bd33c20878f3a9fcdf3a9c53c55]]
= Delete a Duo profile for an SVM or cluster

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/duo/profiles/{owner.uuid}`#

*Introduced In:* 9.14

Deletes the Duo profile of the SVM or cluster.

== Related ONTAP commands

* `security login duo delete`

== Learn more

* xref:{relative_path}manage_duo_profiles_for_an_svm_or_cluster.html[DOC
/security/authentication/duo/profiles/{owner.uuid}]
* xref:{relative_path}manage_security-related_accounts.html[DOC
/security/accounts]


== Parameters

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

|Name
|Type
|In
|Required
|Description

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

|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID20346297e755390d553b87ba8a6fcc6b]]
= Retrieve a Duo profile configured for an SVM or cluster

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/duo/profiles/{owner.uuid}`#

*Introduced In:* 9.14

Retrieves the Duo profile configured for the cluster or an SVM.

== Related ONTAP commands

* `security login duo show`

== Learn more

* xref:{relative_path}manage_duo_profiles_for_an_svm_or_cluster.html[DOC
/security/authentication/duo/profiles/{owner.uuid}]
* xref:{relative_path}manage_security-related_accounts.html[DOC
/security/accounts]


== Parameters

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

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

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

|api_host
|string
a|The URL at which the Duo API is hosted.


|auto_push
|boolean
a|Automatically sends a push notification for authentication when using
Duo.


|comment
|string
a|Comment for the Duo profile.


|fail_mode
```

```
|string
a|Determines the behavior of the system when it cannot communicate with
the Duo service.


|fingerprint
|string
a|The SHA fingerprint corresponding to the Duo secret key.


|http_proxy
|string
a|Specifies the HTTP proxy server to be used when connecting to the Duo
service.


|integration_key
|string
a|The Integration Key associated with the Duo profile.


|is_enabled
|boolean
a|Indicates whether the Duo authentication feature is active or inactive.


|max_prompts
|integer
a|The maximum number of authentication attempts allowed for a user before
the process is terminated.


|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo profile is configured.


|push_info
|boolean
a|Additional information sent along with the push notification for Duo
authentication.


|status
|string
a|Information on the reachability status of Duo.
```

```
|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "api_host": "api-****.duo.com",
  "auto_push": 1,
  "comment": "string",
  "fail_mode": "safe",
  "fingerprint": "string",
  "http_proxy": "IPaddress:port",
  "integration_key": "string",
  "is_enabled": 1,
  "max_prompts": 1,
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "push_info": 1,
  "status": "OK"
}
====

== Error
```

Status: Default, Error

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

```
|Description

|error
|link:#returned_error[returned_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

SVM name and UUID for which the Duo profile is configured.


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

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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
```

```
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDbb9e1eae639f894bf442930ee03e67b5]]
= Update a Duo profile configured for an SVM or cluster

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/authentication/duo/profiles/{owner.uuid}`#

*Introduced In:* 9.14

Updates a configured Duo profile for a cluster or an SVM.

== Related ONTAP commands

* `security login duo modify`

== Learn more

* xref:{relative_path}manage_duo_profiles_for_an_svm_or_cluster.html[DOC
/security/authentication/duo/profiles/{owner.uuid}]
* xref:{relative_path}manage_security-related_accounts.html[DOC
/security/accounts]


== Parameters

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

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

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

|===

== Request Body



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

|api_host
|string
a|The URL at which the Duo API is hosted.


|auto_push
|boolean
a|Automatically sends a push notification for authentication when using
Duo.


|comment
|string
a|Comment for the Duo profile.


|fail_mode
|string
a|Determines the behavior of the system when it cannot communicate with
the Duo service.
```

```
|fingerprint
|string
a|The SHA fingerprint corresponding to the Duo secret key.


|http_proxy
|string
a|Specifies the HTTP proxy server to be used when connecting to the Duo
service.


|integration_key
|string
a|The Integration Key associated with the Duo profile.


|is_enabled
|boolean
a|Indicates whether the Duo authentication feature is active or inactive.


|max_prompts
|integer
a|The maximum number of authentication attempts allowed for a user before
the process is terminated.


|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo profile is configured.


|push_info
|boolean
a|Additional information sent along with the push notification for Duo
authentication.


|secret_key
|string
a|The Secret Key associated with the Duo profile.


|status
|string
a|Information on the reachability status of Duo.
```

```
|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "api_host": "api-****.duo.com",
  "auto_push": 1,
  "comment": "string",
  "fail_mode": "safe",
  "fingerprint": "string",
  "http_proxy": "IPaddress:port",
  "integration_key": "string",
  "is_enabled": 1,
  "max_prompts": 1,
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "push_info": 1,
  "secret_key": "string",
  "status": "OK"
}
====

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

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

SVM name and UUID for which the Duo profile is configured.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

```
duo

Duo profile for the SVM or cluster-management server (Cserver).


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

|api_host
|string
a|The URL at which the Duo API is hosted.


|auto_push
|boolean
a|Automatically sends a push notification for authentication when using
Duo.


|comment
|string
a|Comment for the Duo profile.


|fail_mode
|string
a|Determines the behavior of the system when it cannot communicate with
the Duo service.


|fingerprint
|string
a|The SHA fingerprint corresponding to the Duo secret key.


|http_proxy
|string
a|Specifies the HTTP proxy server to be used when connecting to the Duo
service.


|integration_key
|string
a|The Integration Key associated with the Duo profile.
```

```
|is_enabled
|boolean
a|Indicates whether the Duo authentication feature is active or inactive.


|max_prompts
|integer
a|The maximum number of authentication attempts allowed for a user before
the process is terminated.


|owner
|link:#owner[owner]
a|SVM name and UUID for which the Duo profile is configured.


|push_info
|boolean
a|Additional information sent along with the push notification for Duo
authentication.


|secret_key
|string
a|The Secret Key associated with the Duo profile.


|status
|string
a|Information on the reachability status of Duo.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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 the user account password

:leveloffset: +1


[[ID3df75e79fc1da75a9111a49837c774df]]
= Update the user account password



== 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":"<USER-PASSWORD>"}'
----

----

# 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":"<USER-PASSWORD>"}'
----

----

# 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":"<USER-
PASSWORD>","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":"<USER-
PASSWORD>","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":"<USER-PASSWORD>"}'
----

'''
```

```
[[ID3cc402bf9b8def042ad39cb4949b8636]]
= 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}update_the_user_account_password.html[DOC
/security/authentication/password]
* xref:{relative_path}manage_security-related_accounts.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]
{
  "name": "string",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "password": "string",
  "password_hash_algorithm": "sha512"
}
====

== Response
```

Status: 201, Created

```
=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== 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.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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


[[ID5cffbba81842205d0ee5719f291a242b]]
= Manage authentication keys (for admins)



== 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, comment, and optionally
the certificate 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, "certificate": "<CERTIFICATE-CONTENT>",
```

```
"public_key": "<SSH-PUBLIC-KEY>" }'
----

=== 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, "certificate": "<CERTIFICATE-CONTENT>",
"owner.uuid":"513a78c7-8c13-11e9-8f78-
005056bbf6ac","owner.name":"vs0","public_key": "<SSH-PUBLIC-KEY>" }'
----

=== 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
----




[[IDdc91baacf95a2253ddb8dccb4ba593aa]]
= Retrieve 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}manage_authentication_keys_(for_admins).html[DOC
/security/authentication/publickeys]
* xref:{relative_path}manage_security-related_accounts.html[DOC
/security/accounts]


== Parameters

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

|Name
|Type
|In
|Required
|Description

|certificate_details
|string
|query
|False
a|Filter by certificate_details

* Introduced in: 9.13


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


|index
|integer
```

```
|query
|False
a|Filter by index

* Max value: 99
* Min value: 0


|owner.name
|string
|query
|False
a|Filter by owner.name


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


|account.name
|string
|query
|False
a|Filter by account.name


|certificate
|string
|query
|False
a|Filter by certificate

* Introduced in: 9.13


|certificate_revoked
|string
|query
|False
a|Filter by certificate_revoked

* Introduced in: 9.13
```

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


|obfuscated_fingerprint
|string
|query
|False
a|Filter by obfuscated_fingerprint


|sha_fingerprint
|string
|query
|False
a|Filter by sha_fingerprint


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


|certificate_expired
|string
|query
|False
a|Filter by certificate_expired

* Introduced in: 9.13


|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: 15


|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"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "account": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "joe.smith"
      },
```

```
      "certificate": "string",
      "certificate_details": "string",
      "certificate_expired": "string",
      "certificate_revoked": "string",
      "comment": "string",
      "obfuscated_fingerprint": "string",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "public_key": "string",
      "scope": "string",
      "sha_fingerprint": "string"
    }
  ]
}
====

== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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|

|certificate
|string
a|Optional certificate for the public key.


|certificate_details
|string
a|The details present in the certificate (READONLY).


|certificate_expired
|string
a|The expiration details of the certificate (READONLY).


|certificate_revoked
|string
a|The revocation details of the certificate (READONLY).


|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


|===


[#returned_error]
```

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



[[IDdcef5453924839b83e7036839ada97a3]]
= 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 along with an optional certificate 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.

== Optional properties

* `comment` - Comment text for the public key.
* `certificate` - The certificate in PEM format.

== Related ONTAP commands

* `security login publickey create`

== Learn more

* xref:{relative_path}manage_authentication_keys_(for_admins).html[DOC
/security/authentication/publickeys]
* xref:{relative_path}manage_security-related_accounts.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

|account
|link:#account_reference[account_reference]
a|

|certificate
|string
a|Optional certificate for the public key.


|certificate_details
|string
a|The details present in the certificate (READONLY).


|certificate_expired
|string
a|The expiration details of the certificate (READONLY).


|certificate_revoked
|string
a|The revocation details of the certificate (READONLY).


|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]
{
  "account": {
    "name": "joe.smith"
  },
  "certificate": "string",
  "certificate_details": "string",
  "certificate_expired": "string",
  "certificate_revoked": "string",
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "public_key": "string",
```

```
  "scope": "string",
  "sha_fingerprint": "string"
}
====
```

```
== Response
```

Status: 201, Created

```
=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 5832705
| Public key already exists for the given user and application.

| 5832707
| Failed to generate fingerprint for the public key.

| 5832722
| The public key cannot be associated with this user on the SVM because a
login method using the given application and authentication method does
```

```
not exist for this user.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#account_reference]
[.api-collapsible-fifth-title]
account_reference

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

|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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

The public key for the user account (to access SSH).


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

|account
```

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

|certificate
|string
a|Optional certificate for the public key.


|certificate_details
|string
a|The details present in the certificate (READONLY).


|certificate_expired
|string
a|The expiration details of the certificate (READONLY).


|certificate_revoked
|string
a|The revocation details of the certificate (READONLY).


|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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


[[ID0959592ee8c0083e9004fdc4a5880432]]
= Manage authentication keys (end-users)



== 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}/{inde
x}"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/publickeys/513a78c7-
8c13-11e9-8f78-005056bbf6ac/pubuser4/0
----

=== Updating the public key, certificate, and comment for user accounts

----

# The API:
PATCH
"/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 PATCH --data '{
"comment": "Cserver-modification", "certificate": "<CERTIFICATE-CONTENT>"
, "public_key": "<SSH-PUBLIC-KEY>" }'
----

=== 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
----




[[ID969e9afa8a59fa6e5aaea9a3b8551f12]]
= 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}manage_authentication_keys_(end-users).html[DOC
/security/authentication/publickeys/{owner.uuid}/{account.name}/\{index}]
* xref:{relative_path}manage_security-related_accounts.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:#returned_error[returned_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
```

```
|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDc9f275203c8dd1f584a82604c6cbc634]]
= Retrieve 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}manage_authentication_keys_(end-users).html[DOC
/security/authentication/publickeys/{owner.uuid}/{account.name}/\{index}]
* xref:{relative_path}manage_security-related_accounts.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: 15


|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|

|certificate
|string
a|Optional certificate for the public key.


|certificate_details
|string
a|The details present in the certificate (READONLY).


|certificate_expired
|string
a|The expiration details of the certificate (READONLY).


|certificate_revoked
|string
a|The revocation details of the certificate (READONLY).


|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"
  },
  "certificate": "string",
  "certificate_details": "string",
  "certificate_expired": "string",
  "certificate_revoked": "string",
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "public_key": "string",
  "scope": "string",
  "sha_fingerprint": "string"
}
====

== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDb6955b40cf245c56fd9191078beab589]]
= 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 and/or certificate for a user account.

== Related ONTAP commands
```

```
* `security login publickey modify`

== Learn more

* xref:{relative_path}manage_authentication_keys_(end-users).html[DOC
/security/authentication/publickeys/{owner.uuid}/{account.name}/\{index}]
* xref:{relative_path}manage_security-related_accounts.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

|certificate
|string
a|Optional certificate for the public key.


|certificate_details
|string
a|The details present in the certificate (READONLY).


|certificate_expired
|string
a|The expiration details of the certificate (READONLY).


|certificate_revoked
|string
a|The revocation details of the certificate (READONLY).


|comment
|string
a|Optional comment for the public key.


|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).


|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]
{
  "certificate": "string",
  "certificate_details": "string",
  "certificate_expired": "string",
  "certificate_revoked": "string",
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "public_key": "string",
  "scope": "string",
  "sha_fingerprint": "string"
}
====

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 5832707
| Failed to generate fingerprint for the public key.
```

```
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#account_reference]
[.api-collapsible-fifth-title]
account_reference

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

|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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

The public key for the user account (to access SSH).


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

|certificate
|string
```

```
a|Optional certificate for the public key.


|certificate_details
|string
a|The details present in the certificate (READONLY).


|certificate_expired
|string
a|The expiration details of the certificate (READONLY).


|certificate_revoked
|string
a|The revocation details of the certificate (READONLY).


|comment
|string
a|Optional comment for the public key.


|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).


|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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 AWS KMS

:leveloffset: +1


[[ID869d0831c65a9e74348bee511d3be23d]]
= Manage AWS KMS



== Overview

Amazon Web Services Key Management Services (AWS KMS) 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 AWS KMS.
In order to use AWS KMS with ONTAP, you must first create a
Customer Master Key (CMK) in AWS KMS and provide an Access Key ID and
Secret Access Key for a user that has appropriate access to the newly
created CMK in the AWS KMS."

== Examples

=== Enabling AWS KMS for an SVM

The following example shows how to enable AWS KMS 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/aws-kms

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/aws-kms?return_records=true'
-H 'accept: application/hal+json' -d '{"svm":{"uuid":"f36ff553-e713-11ea-
bd56-005056bb4222" }, "region": "us-east-1", "key_id": "kmip-aws",
"access_key_id": "<AWS-ACCESS-KEY-ID>", "secret_access_key": "<AWS-SECRET-
ACCESS-KEY>"}'

# The response:
{
"num_records": 1,
"records": [
    {
    "uuid": "f72098a2-e908-11ea-bd56-005056bb4222",
    "svm": {
        "uuid": "f36ff553-e713-11ea-bd56-005056bb4222",
        "name": "vs0"
    },
    "region": "us-east-1",
    "key_id": "kmip-aws",
    "access_key_id": "<AWS-ACCESS-KEY-ID>",
    "_links": {
        "self": {
        "href": "/api/security/aws-kms/f72098a2-e908-11ea-bd56-
005056bb4222"
            }
        }
    }
]
}
----

'''

=== Retrieving all AWS KMS configurations

The following example shows how to retrieve all AWS KMS configurations.

----

# The API:
GET /api/security/aws-kms

# The call:
```

```
curl -X GET 'https://<mgmt-ip>/api/security/aws-kms?fields=*'

# The response:
{
"records": [
    {
    "uuid": "f72098a2-e908-11ea-bd56-005056bb4222",
    "scope": "svm",
    "svm": {
        "uuid": "f36ff553-e713-11ea-bd56-005056bb4222",
        "name": "vs0"
    },
    "region": "us-east-1",
    "key_id": "kmip-aws",
    "access_key_id": "<AWS-ACCESS-KEY-ID>",
    "service": "KMS",
    "default_domain": "amazonaws.com",
    "polling_period": 60,
    "timeout": 10,
    "_links": {
        "self": {
        "href": "/api/security/aws-kms/f72098a2-e908-11ea-bd56-
005056bb4222"
            }
        }
    }
],
"num_records": 1,
"_links": {
    "self": {
    "href": "/api/security/aws-kms?fields=*"
    }
}
}
----

'''

=== Retrieving a specific AWS KMS configuration

The following example shows how to retrieve information for a specific AWS
KMS configuration.

----

# The API:
```

```
GET /api/security/aws-kms/{uuid}

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/aws-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"
},
"region": "us-east-1",
"key_id": "kmip-aws",
"access_key_id": "<AWS-ACCESS-KEY-ID>",
"service": "KMS",
"default_domain": "amazonaws.com",
"polling_period": 60,
"timeout": 10,
"_links": {
    "self": {
    "href": "/api/security/aws-kms/f72098a2-e908-11ea-bd56-005056bb4222"
    }
}
}
----

'''

=== Retrieving the advanced properties of an AWS configured for a specific
SVM

These values are not retrieved by default with the 'fields=*' option.
The following example retrieves the advanced properties of a configured
AWS for a specific SVM; there is an added computational cost in retrieving
their values. The properties are not populated for either a collection GET
or an instance GET unless they are explicitly requested using the `fields`
query parameter or GET for all advanced properties is enabled.

----

# The API:
GET /api/security/aws-kms
```

```
# The call:
curl -X GET 'https://<mgmt-ip>/api/security/aws-kms/7052c6c0-a503-11ec-
a68f-005056ac75a0/?fields=state,amazon_reachability,ekmip_reachability'

# The response:
{
"uuid": "d70efc34-aa13-11ec-a059-005056ac7c32",
"state": {
  "cluster_state": true,
  "message": "",
  "code": "0"
},
"amazon_reachability": {
  "reachable": true,
  "message": "",
  "code": "0"
},
"ekmip_reachability": [
  {
    "reachable": true,
    "message": "",
    "code": "0",
    "node": {
      "uuid": "817f544f-a98d-11ec-ae20-005056ac7c32",
      "name": "node1",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/817f544f-a98d-11ec-ae20-
005056ac7c32"
        }
      }
    }
  },
  {
    "reachable": true,
    "message": "",
    "code": "0",
    "node": {
      "uuid": "84b3f5f3-a98d-11ec-9ff4-005056acfbfe",
      "name": "node2",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/84b3f5f3-a98d-11ec-9ff4-
005056acfbfe"
        }
      }
```

```
    }
  }
],
"_links": {
  "self": {
    "href": "/api/security/aws-kms/d70efc34-aa13-11ec-a059-005056ac7c32"
  }
}
}
----

'''

=== Updating the "access_key_id" of a specific AWS KMS configuration

The following example shows how to update the "access_key_id" for a
specific AWS KMS configuration.

----

# The API:
PATCH /api/security/aws-kms/{uuid}

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/aws-kms/f72098a2-e908-11ea-
bd56-005056bb4222/' -d '{"access_key_id": "<AWS-ACCESS-KEY-ID>",
"secret_access_key": "<AWS-SECRET-ACCESS-KEY>"}'
----

'''

=== Updating a specific AWS KMS configuration to allow it to use a proxy.

The following example shows how to update a specific AWS KMS configuration
to allow the AWS KMS instance to use a proxy.

----

# The API:
PATCH /api/security/aws-kms/{uuid}

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/aws-kms/f72098a2-e908-11ea-
bd56-005056bb4222/' -d '{"default_domain": "216.9", "host":
"172.20.216.9", "port": 8000, "service": "10", "verify_host": false,
"verify_ip": false}'
----
```

```
'''

=== Deleting a specific AWS KMS configuration

The following example shows how to delete a specific AWS KMS
configuration.

----

# The API:
DELETE /api/security/aws-kms/{uuid}

# The call;
curl -X DELETE 'https://<mgmt-ip>/api/security/aws-kms/f72098a2-e908-11ea-
bd56-005056bb4222'
----

'''

=== Restoring keys from a KMIP server

The following example shows how to restore keys for a AWS KMS
configuration.

----

# The API:
POST /api/security/aws-kms/{uuid}/restore

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/aws-kms/33820b57-ec90-11ea-
875e-005056bbf3f0/restore'
----

'''




[[IDa66df72638c6476025cf397589d6f549]]
= Retrieve all AWS KMS instances configured for all clusters and SVMs

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

```
*Introduced In:* 9.12

Retrieves all AWS KMS instances configured for all clusters and SVMs.

== Related ONTAP commands

* `security key-manager external aws show`
* `security key-manager external aws check`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|proxy_host
|string
|query
|False
a|Filter by proxy_host


|proxy_port
|integer
|query
|False
a|Filter by proxy_port


|polling_period
|integer
|query
|False
a|Filter by polling_period


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

```
|ekmip_reachability.reachable
|boolean
|query
|False
a|Filter by ekmip_reachability.reachable


|ekmip_reachability.code
|string
|query
|False
a|Filter by ekmip_reachability.code


|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


|ekmip_reachability.message
|string
|query
|False
a|Filter by ekmip_reachability.message


|region
|string
|query
|False
a|Filter by region


|verify_host
|boolean
|query
```

```
|False
a|Filter by verify_host


|default_domain
|string
|query
|False
a|Filter by default_domain


|verify_ip
|boolean
|query
|False
a|Filter by verify_ip


|service
|string
|query
|False
a|Filter by service


|amazon_reachability.code
|string
|query
|False
a|Filter by amazon_reachability.code


|amazon_reachability.reachable
|boolean
|query
|False
a|Filter by amazon_reachability.reachable


|amazon_reachability.message
|string
|query
|False
a|Filter by amazon_reachability.message


|encryption_context
```

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


|timeout
|integer
|query
|False
a|Filter by timeout


|verify
|boolean
|query
|False
a|Filter by verify


|svm.name
|string
|query
|False
a|Filter by svm.name


|svm.uuid
|string
|query
|False
a|Filter by svm.uuid


|proxy_type
|string
|query
|False
a|Filter by proxy_type


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

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


|state.message
|string
|query
|False
a|Filter by state.message


|state.code
|string
|query
|False
a|Filter by state.code


|state.cluster_state
|boolean
|query
|False
a|Filter by state.cluster_state


|skip_verify
|boolean
|query
|False
a|Filter by skip_verify


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


|scope
|string
|query
|False
```

```
a|Filter by scope


|access_key_id
|string
|query
|False
a|Filter by access_key_id


|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: 15
* 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:#aws_kms[aws_kms]]
a|

|===


.Example response
[%collapsible%closed]
====
```

```
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access_key_id": "<AWS-ACCESS-KEY-ID>",
      "amazon_reachability": {
        "code": "346758",
        "message": "Amazon KMS is not reachable from all nodes -
<reason>."
      },
      "default_domain": "domainName",
      "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"
          }
        }
      ],
      "encryption_context": "aws:fsx:fs-id=fs-0785c8beceb895999",
      "host": "aws-host.host.com",
      "key_id": "kmip-aws",
      "polling_period": 55,
      "port": 443,
      "proxy_host": "proxy.eng.com",
```

```
      "proxy_port": 1234,
      "proxy_type": "http",
      "proxy_username": "proxyuser",
      "region": "us-east-1",
      "scope": "string",
      "service": "dynamodb.*.amazonaws.com",
      "skip_verify": "",
      "state": {
        "code": "346758",
        "message": "AWS KMS key protection is unavailable on the following
nodes: node1, node2."
      },
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "timeout": 20,
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412",
      "verify": "",
      "verify_host": 1,
      "verify_ip": ""
    }
  ]
}
====

== 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.

| 65537915
| The Amazon Web Service Key Management Service is unreachable from one or
more nodes.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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|

|===


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

Indicates whether or not the Amazon KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational 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
|string
a|Code corresponding to the error message. Returns a 0 if Amazon KMS is
reachable from all nodes in the cluster.


|message
|string
a|Error message returned when 'reachable' is false.


|reachable
|boolean
a|Set to true if the Amazon KMS 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 computational 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
|string
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 Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


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

|cluster_state
|boolean
a|Set to true when AWS KMS key protection is available on all nodes of the
cluster.
```

```
|code
|string
a|Code corresponding to the message. Returns a 0 if AWS KMS key protection
is available on all nodes of the cluster.


|message
|string
a|Error message set when cluster_state is false.


|===


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

SVM, applies only to SVM-scoped objects.


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

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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#aws_kms]
```

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

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

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

|access_key_id
|string
a|AWS Access Key ID of the user that has appropriate access to AWS KMS.


|amazon_reachability
|link:#amazon_reachability[amazon_reachability]
a|Indicates whether or not the Amazon KMS is reachable from all nodes in
the cluster.
This is an advanced property; there is an added computational 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.


|default_domain
|string
a|AWS KMS default domain.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|encryption_context
|string
a|Additional layer of authentication and logging.


|host
|string
a|AWS KMS host's hostname.
```

```
|key_id
|string
a|AWS Key ID.


|polling_period
|integer
a|Polling period in minutes.


|port
|integer
a|AWS KMS port.


|proxy_host
|string
a|Proxy host.


|proxy_port
|integer
a|Proxy port.


|proxy_type
|string
a|Proxy type.


|proxy_username
|string
a|Proxy username.


|region
|string
a|AWS region of the AWS KMS.


|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|service
|string
a|AWS service type.


|skip_verify
|boolean
a|Set to true to bypass verification of the user provided access_key_id
and secret_access_key. An error will be returned if 'skip_verify' is
provided but 'access_key_id' is not.


|state
|link:#state[state]
a|Indicates whether or not the Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


|svm
|link:#svm[svm]
a|SVM, applies only to SVM-scoped objects.


|timeout
|integer
a|AWS Connection timeout, in seconds.


|uuid
|string
a|A unique identifier for the AWS KMS.


|verify
|boolean
a|Set to true to verify the AWS KMS host.


|verify_host
|boolean
a|Set to true to verify the AWS KMS host's hostname.


|verify_ip
|boolean
a|Set to true to verify the AWS KMS host's IP address.
```

```
|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID540559bd3a8092e1e1ca0513c04c7bab]]
= Configure the AWS KMS configuration for an SVM

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/aws-kms`#

*Introduced In:* 9.12

Configures the AWS KMS configuration for the specified SVM.

== Required properties

* `access_key_id` - AWS access key ID of the user who has the appropriate
access to AWS KMS.
* `secret_access_key` - AWS secret access key for the access key ID
provided.
* `svm.uuid` or `svm.name` - Existing SVM in which to create an AWS KMS.
* `region` - AWS region of the AWS KMS.
* `key_id` - AWS Key ID

== Optional properties

* `service` - AWS service type.
* `default_domain` - AWS KMS default domain.
* `host` - AWS KMS host's hostname.
* `port` - AWS KMS port.
* `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.
* `polling_period` - Polling period in minutes.
* `encryption_context` - Additional layer of authentication and logging.

== Related ONTAP commands

* `security key-manager external aws enable`


== 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: 0
* 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

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

|access_key_id
|string
a|AWS Access Key ID of the user that has appropriate access to AWS KMS.


|amazon_reachability
|link:#amazon_reachability[amazon_reachability]
a|Indicates whether or not the Amazon KMS is reachable from all nodes in
the cluster.
This is an advanced property; there is an added computational 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.


|default_domain
|string
a|AWS KMS default domain.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|encryption_context
|string
a|Additional layer of authentication and logging.


|host
```

```
|string
a|AWS KMS host's hostname.


|key_id
|string
a|AWS Key ID.


|polling_period
|integer
a|Polling period in minutes.


|port
|integer
a|AWS KMS port.


|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|Proxy type.


|proxy_username
|string
a|Proxy username.


|region
|string
a|AWS region of the AWS KMS.
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".


|secret_access_key
|string
a|AWS Secret Access Key for the provided access key ID.


|service
|string
a|AWS service type.


|state
|link:#state[state]
a|Indicates whether or not the Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


|svm
|link:#svm[svm]
a|SVM, applies only to SVM-scoped objects.


|uuid
|string
a|A unique identifier for the AWS KMS.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "access_key_id": "<AWS-ACCESS-KEY-ID>",
  "amazon_reachability": {
    "code": "346758",
    "message": "Amazon KMS is not reachable from all nodes - <reason>."
  },
```

```
  "default_domain": "domainName",
  "ekmip_reachability": [
    {
      "code": "346758",
      "message": "embedded KMIP server status unavailable on node.",
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ],
  "encryption_context": "aws:fsx:fs-id=fs-0785c8beceb895999",
  "host": "aws-host.host.com",
  "key_id": "kmip-aws",
  "polling_period": 55,
  "port": 443,
  "proxy_host": "proxy.eng.com",
  "proxy_password": "awskze-Jwjje2-WJJPer",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "region": "us-east-1",
  "scope": "string",
  "secret_access_key": "<AWS-SECRET-ACCESS-KEY>",
  "service": "dynamodb.*.amazonaws.com",
  "skip_verify": "",
  "state": {
    "code": "346758",
    "message": "AWS KMS key protection is unavailable on the following
nodes: node1, node2."
  },
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412",
  "verify": "",
  "verify_host": 1,
  "verify_ip": ""
}
====

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

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 3735622
| Certificate type not supported for create operation.

| 3735645
| You cannot specify a value for serial as it is generated automatically.

| 3735657
| Specifying \"-subtype\" when creating a certificate is not supported.

| 3735664
| Specified key size is not supported in FIPS mode.

| 3735665
| Specified hash function is not supported in FIPS mode.

| 3735700
| Specified key size is not supported.

| 65536600
| Nodes are out of quorum.

| 65537518
| Failed to find a LIF with Cluster role on node. One or more nodes may be
out of quorum.

| 65537900
| Failed to enable the Amazon Web Service Key Management Service for an
SVM due to an invalid secret access key.

| 65537901
| The Amazon Web Service Key Management Service (AWSKMS) cannot be enabled
because all nodes in the cluster are not running a version that supports
the AWSKMS feature.

| 65537906
| Failed to store the secret access key.
```

```
| 65537907
| The Amazon Web Service Key Management Service is disabled on the
cluster. For further assistance, contact technical support.

| 65537908
| The Amazon Web Service Key Management Service is not supported for the
admin SVM.

| 65537910
| Failed to configure Amazon Web Service Key Management Service for an SVM
because a key manager has already been configured for the SVM.

| 65537911
| The Amazon Web Service Key Management Service is not supported in
MetroCluster configurations.

| 65537912
| The Amazon Web Service Key Management Service cannot be configured for
an SVM because one or more volume encryption keys of the SVM are stored on
the admin SVM.

| 65537926
| The Amazon Web Service Key Management Service is not configured for this
SVM.

| 65539704
| The key manager cannot be configured because the SVM has NAE volumes.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#amazon_reachability]
[.api-collapsible-fifth-title]
amazon_reachability

Indicates whether or not the Amazon KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational 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
|string
a|Code corresponding to the error message. Returns a 0 if Amazon KMS is
reachable from all nodes in the cluster.


|message
|string
a|Error message returned when 'reachable' is false.


|reachable
|boolean
```

```
a|Set to true if the Amazon KMS is reachable from all nodes of the
cluster.


|===


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

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

|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 computational 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
|string
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 Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


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

|cluster_state
|boolean
a|Set to true when AWS KMS key protection is available on all nodes of the
cluster.


|code
```

```
|string
a|Code corresponding to the message. Returns a 0 if AWS KMS key protection
is available on all nodes of the cluster.


|message
|string
a|Error message set when cluster_state is false.


|===


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

SVM, applies only to SVM-scoped objects.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

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

```
|Type
|Description

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

|access_key_id
|string
a|AWS Access Key ID of the user that has appropriate access to AWS KMS.


|amazon_reachability
|link:#amazon_reachability[amazon_reachability]
a|Indicates whether or not the Amazon KMS is reachable from all nodes in
the cluster.
This is an advanced property; there is an added computational 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.


|default_domain
|string
a|AWS KMS default domain.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|encryption_context
|string
a|Additional layer of authentication and logging.


|host
|string
a|AWS KMS host's hostname.


|key_id
|string
a|AWS Key ID.
```

```
|polling_period
|integer
a|Polling period in minutes.


|port
|integer
a|AWS KMS port.


|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|Proxy type.


|proxy_username
|string
a|Proxy username.


|region
|string
a|AWS region of the AWS KMS.


|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".


|secret_access_key
```

```
|string
a|AWS Secret Access Key for the provided access key ID.


|service
|string
a|AWS service type.


|state
|link:#state[state]
a|Indicates whether or not the Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


|svm
|link:#svm[svm]
a|SVM, applies only to SVM-scoped objects.


|uuid
|string
a|A unique identifier for the AWS KMS.


|===


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDd839f45e011f215c6ab92075e5f810e7]]
= Re-key or re-version an AWS KMS key encryption key for AWS KMS

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/aws-kms/{aws_kms.uuid}/rekey-external`#

*Introduced In:* 9.12

Rekeys or re-versions the AWS KMS Key Encryption Key (KEK) for the given
AWS KMS.

== Related ONTAP commands

* `security key-manager external aws rekey-external`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|aws_kms.uuid
|string
|path
|True
a|UUID of the existing AWS 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: 0
* 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 AWS KMS key encryption key.


|===


.Example request
```

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "key_id": "key01"
}
====

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

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

```

```

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65537538
| Internal error. Failed to get unwrapped key for a given key ID.

| 65537543
| Internal Error. Missing top-level internal key protection key (KEK) on a
node.

| 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 before running the rekey operation.

| 65537610
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being switched. If a previous attempt to switch the
keystore configuration failed, or was interrupted, the system will
continue to prevent rekeying for the SVM. Use the REST API PATCH method
"/api/security/key-stores/\{uuid}" to re-run and complete the operation.

| 65537919
| External rekey failed on one or more nodes.

| 65537926
| AWS KMS is not configured for the given SVM.

| 65539436
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being initialized. Wait until the keystore is in the
active state, and rerun the rekey operation.

| 65539437
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being disabled.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== Definitions
```

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

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

|key_id
|string
a|Key identifier of the AWS KMS key encryption key.


|===


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

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

|href
|string
a|

|===


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID97aba4a9f8aee0469538210ec9968b3c]]
= Re-key SVM KEK for an AWS KMS

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/aws-kms/{aws_kms.uuid}/rekey-internal`#

*Introduced In:* 9.12

Rekeys SVM KEK for the given AWS KMS.

== Related ONTAP commands

* `security key-manager external aws rekey-internal`


== Parameters
```

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

|Name
|Type
|In
|Required
|Description

|aws_kms.uuid
|string
|path
|True
a|UUID of the existing AWS 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: 0
* 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

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

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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "uuid": "string"
  }
}
====

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== 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.

| 65537556
| Unable to successfully encrypt or decrypt because the configured
external key manager for the given SVM is in a blocked state.

| 65537559
| There are no existing internal keys for the SVM. A rekey operation is
allowed for an SVM with one or more encryption keys.

| 65537566
| Internal error. All nodes in the cluster are not currently online.

| 65537610
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being switched. If a previous attempt to switch the
keystore configuration failed, or was interrupted, the system will
continue to prevent rekeying for the SVM. Use the REST API PATCH method
"/api/security/key-stores/\{uuid}" to re-run and complete the operation.

| 65537926
| AWS KMS is not configured for the given SVM.

| 65539436
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being initialized. Wait until the keystore is in the
active state, and rerun the rekey operation.

| 65539437
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being disabled.
```

```
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDd5e1caca7da1dde1ce8e7ba85f1ef9e7]]
= Restore keys for an SVM from a configured AWS KMS

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/aws-kms/{aws_kms.uuid}/restore`#

*Introduced In:* 9.12

Restores the keys for an SVM from a configured AWS KMS.

== Related ONTAP commands

* `security key-manager external AWS restore`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|aws_kms.uuid
```

```
|string
|path
|True
a|UUID of the existing AWS 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: 0
* 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

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

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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "uuid": "string"
  }
}
====

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65536082
| Unable to restore all keys.

| 65537544
| Missing wrapped top-level internal key protection key (KEK) from
internal database.

| 65537926
| The Amazon Web Service Key Management Service is not configured for the
given SVM.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


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

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

|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
```

```
|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDa62268e1e0a00ea458b8f379d7ba9081]]
= Delete an AWS KMS configuration

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/aws-kms/{uuid}`#
```

```
*Introduced In:* 9.12

Deletes an AWS KMS configuration.

== Related ONTAP commands

* `security key-manager external aws disable`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|AWS 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: 0
* Max value: 120
* Min value: 0

|===

== Response
```

Status: 200, Ok

```
== Response
```

Status: 202, Accepted

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 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.

| 65536883
| Internal error. Volume encryption key is missing for a volume.

| 65536884
| Internal error. Volume encryption key is invalid for a volume.

| 65537106
| Volume encryption keys (VEK) for one or more encrypted volumes are
stored on the key manager configured for the given SVM.

| 65537926
| Amazon Web Service Key Management Service is not configured for 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.

| 196608332
| NAE aggregates found in the cluster.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID7e25c954dec45e9b1278c079caadaaa5]]
= Retrieve an AWS KMS configuration

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/aws-kms/{uuid}`#

*Introduced In:* 9.12

Retrieves the AWS KMS configuration for the SVM specified by the UUID.

== Related ONTAP commands

* `security key-manager external aws show`
* `security key-manager external aws check`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|uuid
```

```
|string
|path
|True
a|AWS 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|

|access_key_id
|string
a|AWS Access Key ID of the user that has appropriate access to AWS KMS.


|amazon_reachability
|link:#amazon_reachability[amazon_reachability]
a|Indicates whether or not the Amazon KMS is reachable from all nodes in
the cluster.
This is an advanced property; there is an added computational 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.


|default_domain
|string
```

```
a|AWS KMS default domain.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|encryption_context
|string
a|Additional layer of authentication and logging.


|host
|string
a|AWS KMS host's hostname.


|key_id
|string
a|AWS Key ID.


|polling_period
|integer
a|Polling period in minutes.


|port
|integer
a|AWS KMS port.


|proxy_host
|string
a|Proxy host.


|proxy_port
|integer
a|Proxy port.


|proxy_type
|string
a|Proxy type.
```

```
|proxy_username
|string
a|Proxy username.


|region
|string
a|AWS region of the AWS KMS.


|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".


|service
|string
a|AWS service type.


|skip_verify
|boolean
a|Set to true to bypass verification of the user provided access_key_id
and secret_access_key. An error will be returned if 'skip_verify' is
provided but 'access_key_id' is not.


|state
|link:#state[state]
a|Indicates whether or not the Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


|svm
|link:#svm[svm]
a|SVM, applies only to SVM-scoped objects.


|timeout
|integer
a|AWS Connection timeout, in seconds.


|uuid
|string
a|A unique identifier for the AWS KMS.
```

```
|verify
|boolean
a|Set to true to verify the AWS KMS host.


|verify_host
|boolean
a|Set to true to verify the AWS KMS host's hostname.


|verify_ip
|boolean
a|Set to true to verify the AWS KMS host's IP address.


|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_key_id": "<AWS-ACCESS-KEY-ID>",
  "amazon_reachability": {
    "code": "346758",
    "message": "Amazon KMS is not reachable from all nodes - <reason>."
  },
  "default_domain": "domainName",
  "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"
      }
    }
  ],
  "encryption_context": "aws:fsx:fs-id=fs-0785c8beceb895999",
  "host": "aws-host.host.com",
  "key_id": "kmip-aws",
  "polling_period": 55,
  "port": 443,
  "proxy_host": "proxy.eng.com",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "region": "us-east-1",
  "scope": "string",
  "service": "dynamodb.*.amazonaws.com",
  "skip_verify": "",
  "state": {
    "code": "346758",
    "message": "AWS KMS key protection is unavailable on the following
nodes: node1, node2."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "timeout": 20,
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412",
  "verify": "",
  "verify_host": 1,
  "verify_ip": ""
}
====

== 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.

| 65537915
| The Amazon Web Service Key Management Service is unreachable from one or
more nodes.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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|

|===
```

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

Indicates whether or not the Amazon KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational 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
|string
a|Code corresponding to the error message. Returns a 0 if Amazon KMS is
reachable from all nodes in the cluster.


|message
|string
a|Error message returned when 'reachable' is false.


|reachable
|boolean
a|Set to true if the Amazon KMS 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 computational 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
|string
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 Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


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

|cluster_state
|boolean
a|Set to true when AWS KMS key protection is available on all nodes of the
cluster.


|code
|string
a|Code corresponding to the message. Returns a 0 if AWS KMS key protection
is available on all nodes of the cluster.


|message
|string
a|Error message set when cluster_state is false.
```

```
|===


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

SVM, applies only to SVM-scoped objects.


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

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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====
```

```
[[ID26a01c5ceee4f81a68edc446b5090d41]]
= Update an AWS KMS configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/aws-kms/{uuid}`#

*Introduced In:* 9.12

Updates the AWS KMS configuration.

== Optional properties

* `region` - AWS region of the AWS KMS.
* `service` - AWS service type.
* `default_domain` - AWS KMS default domain.
* `port` - AWS KMS port.
* `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.
* `polling_period` - Polling period in minutes.
* `timeout` - AWS Connection timeout, in seconds.
* `verify` - Set to true to verify the AWS KMS host.
* `verify_host` - Set to true to verify the AWS KMS host's hostname.
* `verify_ip` - Set to true to verify the AWS KMS host's IP address.
* `host` - AWS KMS host's hostname.
* `secret_access_key` - AWS secret access key for the access key ID
provided.
* `access_key_id` - AWS access key ID of the user with the appropriate
access to AWS KMS.
* `skip_verify` - Set to true to bypass verification of the user provided
access_key_id and secret_access_key.
* `encryption_context` - Additional layer of authentication and logging.

== Related ONTAP commands

* `security key-manager external aws update-config`
* `security key-manager external aws update-credentials`


== Parameters

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

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

|uuid
|string
|path
|True
a|AWS 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: 0
* Max value: 120
* Min value: 0

|===

== Request Body



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

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

|access_key_id
```

```
|string
a|AWS Access Key ID of the user that has appropriate access to AWS KMS.


|amazon_reachability
|link:#amazon_reachability[amazon_reachability]
a|Indicates whether or not the Amazon KMS is reachable from all nodes in
the cluster.
This is an advanced property; there is an added computational 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.


|default_domain
|string
a|AWS KMS default domain.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|encryption_context
|string
a|Additional layer of authentication and logging.


|host
|string
a|AWS KMS host's hostname.


|polling_period
|integer
a|Polling period in minutes.


|port
|integer
a|AWS KMS port.


|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|Proxy type.


|proxy_username
|string
a|Proxy username.


|region
|string
a|AWS region of the AWS KMS.


|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".


|secret_access_key
|string
a|AWS Secret Access Key for the provided access key ID.


|service
|string
a|AWS service type.


|skip_verify
|boolean
a|Set to true to bypass verification of the user provided access_key_id
and secret_access_key. An error will be returned if 'skip_verify' is
```

```
provided but 'access_key_id' is not.


|state
|link:#state[state]
a|Indicates whether or not the Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


|timeout
|integer
a|AWS Connection timeout, in seconds.


|uuid
|string
a|A unique identifier for the AWS KMS.


|verify
|boolean
a|Set to true to verify the AWS KMS host.


|verify_host
|boolean
a|Set to true to verify the AWS KMS host's hostname.


|verify_ip
|boolean
a|Set to true to verify the AWS KMS host's IP address.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "access_key_id": "<AWS-ACCESS-KEY-ID>",
  "amazon_reachability": {
    "code": "346758",
    "message": "Amazon KMS is not reachable from all nodes - <reason>."
  },
```

```
  "default_domain": "domainName",
  "ekmip_reachability": [
    {
      "code": "346758",
      "message": "embedded KMIP server status unavailable on node.",
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ],
  "encryption_context": "aws:fsx:fs-id=fs-0785c8beceb895999",
  "host": "aws-host.host.com",
  "polling_period": 55,
  "port": 443,
  "proxy_host": "proxy.eng.com",
  "proxy_password": "awskze-Jwjje2-WJJPer",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "region": "us-east-1",
  "scope": "string",
  "secret_access_key": "<AWS-SECRET-ACCESS-KEY>",
  "service": "dynamodb.*.amazonaws.com",
  "skip_verify": "",
  "state": {
    "code": "346758",
    "message": "AWS KMS key protection is unavailable on the following
nodes: node1, node2."
  },
  "timeout": 20,
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412",
  "verify": "",
  "verify_host": 1,
  "verify_ip": ""
}
====

== Response
```

Status: 200, Ok

```
== Response
```

Status: 202, Accepted

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65537541
| No inputs provided for the REST API PATCH request.

| 65537906
| Failed to store the secret access key.

| 65537920
| Secret access key cannot be empty.

| 65537921
| Unable to connect to the Amazon Web Service Key Management Service
(AWSKMS) using these credentials.

| 65537924
| Access key ID cannot be empty.

| 65537926
| Amazon Web Service Key Management Service is not configured for SVM.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#amazon_reachability]
[.api-collapsible-fifth-title]
amazon_reachability

Indicates whether or not the Amazon KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational 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
|string
a|Code corresponding to the error message. Returns a 0 if Amazon KMS is
reachable from all nodes in the cluster.


|message
|string
a|Error message returned when 'reachable' is false.


|reachable
```

```
|boolean
a|Set to true if the Amazon KMS is reachable from all nodes of the
cluster.


|===


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

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

|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 computational 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
|string
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 Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


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

|cluster_state
|boolean
a|Set to true when AWS KMS key protection is available on all nodes of the
cluster.
```

```
|code
|string
a|Code corresponding to the message. Returns a 0 if AWS KMS key protection
is available on all nodes of the cluster.


|message
|string
a|Error message set when cluster_state is false.


|===


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

SVM, applies only to SVM-scoped objects.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

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

```
|Name
|Type
|Description

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

|access_key_id
|string
a|AWS Access Key ID of the user that has appropriate access to AWS KMS.


|amazon_reachability
|link:#amazon_reachability[amazon_reachability]
a|Indicates whether or not the Amazon KMS is reachable from all nodes in
the cluster.
This is an advanced property; there is an added computational 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.


|default_domain
|string
a|AWS KMS default domain.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|encryption_context
|string
a|Additional layer of authentication and logging.


|host
|string
a|AWS KMS host's hostname.


|polling_period
|integer
a|Polling period in minutes.
```

```
|port
|integer
a|AWS KMS port.


|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|Proxy type.


|proxy_username
|string
a|Proxy username.


|region
|string
a|AWS region of the AWS KMS.


|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".


|secret_access_key
|string
a|AWS Secret Access Key for the provided access key ID.
```

```
|service
|string
a|AWS service type.


|skip_verify
|boolean
a|Set to true to bypass verification of the user provided access_key_id
and secret_access_key. An error will be returned if 'skip_verify' is
provided but 'access_key_id' is not.


|state
|link:#state[state]
a|Indicates whether or not the Amazon Web Services Key Management Service
(AWS KMS) key protection is available cluster-wide.


|timeout
|integer
a|AWS Connection timeout, in seconds.


|uuid
|string
a|A unique identifier for the AWS KMS.


|verify
|boolean
a|Set to true to verify the AWS KMS host.


|verify_host
|boolean
a|Set to true to verify the AWS KMS host's hostname.


|verify_ip
|boolean
a|Set to true to verify the AWS KMS host's IP address.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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


[[ID5a83369ff80dc91982ac2739fd260e9f]]
= Manage Azure Key Vaults



== 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

=== Enabling an AKV configuration for an SVM using the certificate
authentication method

The example AKV configuration is enabled for a specific SVM. Note the
_return_records=true_ query parameter is used to obtain the newly created
key-manager keystore 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.vault.azure.net/\", \"key_id\": \"https://keyvault-
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74\",
\"client_certificate\" : \"<CERTIFICATE-CONTENT>\" }"

# 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/a8e619fd8f234db3b0b95c59540e2a74",
    "_links": {
      "self": {
        "href": "/api/security/azure-key-vaults/024cd3cf-9a08-11ea-8d52-
005056bbeba5"
      }
    }
  }
]
}
----

'''

=== Creating an inactive AKV configuration for an SVM using the client
secret authentication method
```

```
The example AKV configuration is created for a specific SVM but is not
enabled.
Note the _create_inactive=true_ parameter that is used to indicate that
the configuration should be created but not enabled.
Note the _return_records=true_ query parameter is used to obtain the newly
created key-manager keystore configuration.

----

# The API:
POST /api/security/azure-key-vaults

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/azure-key-
vaults?create_inactive=true&return_records=true' -H 'accept:
application/hal+json' -d "{ \"svm\": { \"uuid\": \"4f7abf4c-9a07-11ea-
8d52-005056bbeba5\" }, \"configuration\": {\"name\": \"myConfiguration\"},
\"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",
    "configuration": {"name": "myConfiguration"},
    "client_id": "client1",
    "tenant_id": "tenant1",
    "name": "https://mykeyvault.azure.vault.net/",
    "key_id": "https://keyvault-
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",
    "_links": {
      "self": {
        "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-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": [
  {
    "configuration": {
      "uuid": "024cd3cf-9a08-11ea-8d52-005056bbeba5",
      "name" : "default"
    },
    "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/a8e619fd8f234db3b0b95c59540e2a74",
    "authentication_method": "client_secret",
    "enabled": true,
    "_links": {
      "self": {
        "href": "/api/security/azure-key-vaults/024cd3cf-9a08-11ea-8d52-
005056bbeba5"
      }
    }
  },
  {
    "configuration": {
      "uuid": "85619643-9a06-11ea-8d52-005056bbeba5",
      "name" : "new-config"
    },
```

```
    "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/a8e619fd8f234db3b0b95c59540e2a74",
    "authentication_method": "certificate",
    "enabled": false,
    "_links": {
      "self": {
        "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-
005056bbeba5"
      }
    }
  }
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/security/azure-key-vaults?fields=*"
  }
}
}
----

'''

=== Retrieving a specific AKV configuration

The following example retrieves a specific AKV configuration.

----

# 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:
{
"configuration": {
  "uuid": "85619643-9a06-11ea-8d52-005056bbeba5",
  "name" : "default"
```

```
},
"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/a8e619fd8f234db3b0b95c59540e2a74",
"authentication_method": "client_secret",
"enabled": true,
"_links": {
  "self": {
    "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-
005056bbeba5"
  }
}
}
----

'''

=== Retrieving the advanced properties of a specific, enabled AKV
configuration

The following example retrieves the advanced properties of a specific
enabled AKV configuration (inactive AKV configurations do not have these
advanced properties).

----

# 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"'
{
"configuration": {
  "uuid": "85619643-9a06-11ea-8d52-005056bbeba5",
  "name" : "default"
},
"uuid": "85619643-9a06-11ea-8d52-005056bbeba5",
"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/85619643-9a06-11ea-8d52-
005056bbeba5"
  }
}
```

```
}
----

'''

=== Updating the client secret of a specific AKV configuration

The following example updates the client secret of a specific AKV
configuration.

----

# 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\": \"<NEW-SECRET>\" }"
----

'''

=== Updating the client certificate and key of a specific AKV
configuration

The following example updates the client certificate and key of a
configured AKV for a specific AKV configuration.

----

# 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\": \"<CERTIFICATE-
CONTENT>\" }"
----

'''

=== Deleting a specific AKV configuration

The following example deletes a specific, enabled AKV.

----
```

```
# 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 AKV configuration

The following example restores all the keys of a specific AKV
configuration.

----

# 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 AKV configuration

The following example rekeys the internal key of a specific AKV
configuration.

----

# 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"
    }
  }
}
}
----

'''




[[ID6306d1dde3766121201af40e571bcac2]]
= 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

|oauth_host
|string
|query
|False
a|Filter by oauth_host

* Introduced in: 9.14


|svm.name
|string
|query
|False
a|Filter by svm.name


|svm.uuid
|string
|query
|False
a|Filter by svm.uuid


|proxy_type
|string
|query
|False
a|Filter by proxy_type


|azure_reachability.message
|string
|query
|False
a|Filter by azure_reachability.message


|azure_reachability.code
|string
|query
|False
a|Filter by azure_reachability.code
```

```
|azure_reachability.reachable
|boolean
|query
|False
a|Filter by azure_reachability.reachable


|client_id
|string
|query
|False
a|Filter by client_id


|proxy_username
|string
|query
|False
a|Filter by proxy_username


|key_id
|string
|query
|False
a|Filter by key_id


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

* Introduced in: 9.14


|state.message
|string
|query
|False
a|Filter by state.message


|state.available
```

```
|boolean
|query
|False
a|Filter by state.available


|state.code
|string
|query
|False
a|Filter by state.code


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


|authentication_method
|string
|query
|False
a|Filter by authentication_method

* Introduced in: 9.10


|uuid
|string
|query
|False
a|Filter by uuid


|proxy_host
|string
|query
|False
a|Filter by proxy_host


|tenant_id
|string
|query
|False
```

```
a|Filter by tenant_id


|vault_host
|string
|query
|False
a|Filter by vault_host

* Introduced in: 9.14


|proxy_port
|integer
|query
|False
a|Filter by proxy_port


|configuration.name
|string
|query
|False
a|Filter by configuration.name

* Introduced in: 9.14


|configuration.uuid
|string
|query
|False
a|Filter by configuration.uuid

* Introduced in: 9.14


|ekmip_reachability.reachable
|boolean
|query
|False
a|Filter by ekmip_reachability.reachable


|ekmip_reachability.code
|string
|query
```

```
|False
a|Filter by ekmip_reachability.code


|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


|ekmip_reachability.message
|string
|query
|False
a|Filter by ekmip_reachability.message


|skip_verification
|boolean
|query
|False
a|Filter by skip_verification

* Introduced in: 9.16


|enabled
|boolean
|query
|False
a|Filter by enabled

* Introduced in: 9.14


|verify_host
|boolean
|query
|False
```

```
a|Filter by verify_host

* Introduced in: 9.14


|verify_ip
|boolean
|query
|False
a|Filter by verify_ip

* Introduced in: 9.14


|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_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: 15
* 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"
    }
  },
  "num_records": 1,
  "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_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
      "configuration": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
      },
      "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/key1/12345678901234567890123456789
012",
      "name": "https://kmip-akv-keyvault.vault.azure.net/",
      "oauth_host": "login.microsoftonline.com",
      "port": 443,
      "proxy_host": "proxy.eng.com",
      "proxy_port": 1234,
      "proxy_type": "http",
      "proxy_username": "proxyuser",
      "scope": "string",
      "skip_verification": "",
      "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",
      "vault_host": "vault.azure.net",
      "verify_host": "",
      "verify_ip": ""
    }
  ]
}
====

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65537549
| The Azure Key Vault Key Management Service is unreachable from one or
more nodes.

| 65537551
| Top-level internal key protection key (KEK) unavailable on one or more
nodes.

| 65537552
| Embedded KMIP server status not available.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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 computational 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
```

```
|string
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.


|===


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

Security keystore object reference.


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

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

|name
|string
a|Name of the configuration.


|uuid
|string
a|Keystore UUID.


|===
```

```
[#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 computational 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
```

```
|string
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 computational 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
|string
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

SVM, applies only to SVM-scoped objects.


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

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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===
```

```
[#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 computational 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_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.


|configuration
|link:#configuration[configuration]
a|Security keystore object reference.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|
```

```
|enabled
|boolean
a|Indicates whether the configuration is enabled.


|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
* x-nullable: true


|oauth_host
|string
a|Open authorization server host name.


|port
|integer
a|Authorization server and vault port number.


|proxy_host
|string
a|Proxy host.


|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".


|skip_verification
|boolean
a|Set to true to skip the verification of the updated user credentials
when updating credentials. The default value is false.


|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 computational 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|SVM, applies only to SVM-scoped objects.


|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).


|vault_host
|string
a|AKV host subdomain.
```

```
|verify_host
|boolean
a|Verify the identity of the AKV host name.


|verify_ip
|boolean
a|Verify the identity of the AKV IP address.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID125b2a8099d9329999079b9a73c0a613]]
= 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` or `client_certificate` - Secret or 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:

* `port` - Authorization server and vault port number.
* `oauth_host` - Open authorization server host name.
* `vault_host` - AKV host subdomain.
* `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.
* `configuration.name` - The configuration name to use when also setting
the `create_inactive` flag.

== Optional parameters:

* `create_inactive` - Create an AKV configuration without enabling it.
This flag is set to "false" by default.

== Related ONTAP commands

* `security key-manager external azure enable`
* `security key-manager external azure create-config`
* `security key-manager external azure update-config`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|create_inactive
|boolean
|query
|False
a|Indicates whether to create an active or inactive configuration.

* Introduced in: 9.16
```

```
|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: 0
* 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

|_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 computational 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.


|configuration
|link:#configuration[configuration]
a|Security keystore object reference.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|enabled
|boolean
a|Indicates whether the configuration is enabled.


|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
* x-nullable: true


|oauth_host
|string
a|Open authorization server host name.


|port
|integer
a|Authorization server and vault port number.


|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".


|skip_verification
|boolean
a|Set to true to skip the verification of the updated user credentials
when updating credentials. The default value is false.


|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 computational 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|SVM, applies only to SVM-scoped objects.


|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).


|vault_host
|string
a|AKV host subdomain.


|===


.Example request
```

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "authentication_method": "client_secret",
  "azure_reachability": {
    "code": "346758",
    "message": "AKV service is not reachable from all nodes - reason."
  },
  "client_certificate": "<CERTIFICATE-CONTENT>",
  "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
  "client_secret": "abcdef",
  "configuration": {
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  },
  "ekmip_reachability": [
    {
      "code": "346758",
      "message": "embedded KMIP server status unavailable on node.",
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ],
  "key_id":
"https://keyvault1.vault.azure.net/keys/key1/12345678901234567890123456789
012",
  "name": "https://kmip-akv-keyvault.vault.azure.net/",
  "oauth_host": "login.microsoftonline.com",
  "port": 443,
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "string",
  "skip_verification": "",
  "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": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzz",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412",
  "vault_host": "vault.azure.net",
  "verify_host": "",
  "verify_ip": ""
}
====

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

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== 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/a8e619fd8f234db3b0b95c59540e
2a74".

| 65537526
| Failed to enable Azure Key Vault feature.

| 65537567
| No authentication method provided.

| 65537573
| Invalid client certificate.

| 65537589
| The specified configuration.name already exists on the given SVM.

| 65537592
| The configuration.name field requires an ECV of 9.14.0 or greater.

| 65537593
| The create_inactive flag requires an effective cluster version of 9.14.0
or greater.

| 65537594
| The configuration.name field is required when the create_inactive flag
is set to true.

| 65537595
| The configuration.name field can only be specified when the
create_inactive flag is set to true.

| 65538902
| The configuration.name is reserved for use by the system.

| 65538903
| The configuration.name field cannot be an empty string.

| 65539704
| The key manager cannot be configured because the SVM has NAE volumes.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.
```

```
== 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
[#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 computational 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
|string
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.


|===


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

Security keystore object reference.


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

|name
|string
a|Name of the configuration.


|uuid
|string
a|Keystore UUID.


|===
```

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

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

|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 computational 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
|string
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 computational 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
|string
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

SVM, applies only to SVM-scoped objects.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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 computational 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.


|configuration
|link:#configuration[configuration]
a|Security keystore object reference.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|
```

```
|enabled
|boolean
a|Indicates whether the configuration is enabled.


|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
* x-nullable: true


|oauth_host
|string
a|Open authorization server host name.


|port
|integer
a|Authorization server and vault port number.


|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".


|skip_verification
|boolean
a|Set to true to skip the verification of the updated user credentials
when updating credentials. The default value is false.


|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 computational 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|SVM, applies only to SVM-scoped objects.


|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).
```

```
|vault_host
|string
a|AKV host subdomain.


|===


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

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

|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
```

```
|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID3f3eac468600c938e9522cb49ac22693]]
= 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: 0
* 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.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "key_id":
"https://keyvault1.vault.azure.net/keys/key1/12345678901234567890123456789
012"
}
====

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

== Response
```

Status: 201, Created

```
== 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.

| 65537610
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being switched. If a previous attempt to switch the
keystore configuration failed, or was interrupted, the system will
continue to prevent rekeying for the SVM. Use the REST API PATCH method
"/api/security/key-stores/\{uuid}" to re-run and complete the operation.

| 65539436
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being initialized. Wait until the keystore is in the
active state, and rerun the rekey operation.

| 65539437
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being disabled.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== Definitions

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

```
|===


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

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

|href
|string
a|

|===


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID29c694d5fdb71104e7919b04e40fdede]]
= 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


|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: 0
* Max value: 120
* Min value: 0

|===

== Response
```

Status: 200, Ok

```
== Response
```

Status: 202, Accepted

```
== 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.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID9d5f224985afe84e1f58714b5de9254c]]
= 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 computational 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_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.


|configuration
|link:#configuration[configuration]
a|Security keystore object reference.


|ekmip_reachability
|array[link:#ekmip_reachability[ekmip_reachability]]
a|

|enabled
|boolean
a|Indicates whether the configuration is enabled.


|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
* x-nullable: true


|oauth_host
|string
a|Open authorization server host name.


|port
|integer
a|Authorization server and vault port number.


|proxy_host
|string
a|Proxy host.


|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".
```

```
|skip_verification
|boolean
a|Set to true to skip the verification of the updated user credentials
when updating credentials. The default value is false.


|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 computational 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|SVM, applies only to SVM-scoped objects.


|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).


|vault_host
|string
a|AKV host subdomain.


|verify_host
|boolean
a|Verify the identity of the AKV host name.


|verify_ip
|boolean
```

```
a|Verify the identity of the AKV IP address.


|===


.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_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
  "configuration": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  },
  "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/key1/123456789012345678901234567890
12",
  "name": "https://kmip-akv-keyvault.vault.azure.net/",
  "oauth_host": "login.microsoftonline.com",
  "port": 443,
  "proxy_host": "proxy.eng.com",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "string",
  "skip_verification": "",
  "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",
  "vault_host": "vault.azure.net",
  "verify_host": "",
  "verify_ip": ""
}
====

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description
```

```
| 65537549
| The Azure Key Vault Key Management Service is unreachable from one or
more nodes.

| 65537551
| Top-level internal key protection key (KEK) unavailable on one or more
nodes.

| 65537552
| Embedded KMIP server status not available.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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 computational 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
|string
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.


|===


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

Security keystore object reference.


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

```
|Description

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

|name
|string
a|Name of the configuration.


|uuid
|string
a|Keystore UUID.


|===


[#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 computational 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
|string
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 computational 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
|string
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

SVM, applies only to SVM-scoped objects.


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

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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDc861b61e83eb8cce055922788f90f3e2]]
= 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` or `client_certificate` - New secret or 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.
* `port` - Authorization server and vault port number.
* `oauth_host` - Open authorization server host name.
* `vault_host` - AKV host subdomain.
* `verify_host` - Verify the identity of the AKV host name.
* `verify_ip ` - Verify the identity of the AKV IP address.
* `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.
* `skip_verification` - Skip the verification of the updated credentials,
set to true to bypass the verification. The default value is false.

== 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: 0
* 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 computational 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|

|enabled
|boolean
a|Indicates whether the configuration is enabled.


|oauth_host
|string
a|Open authorization server host name.


|port
|integer
a|Authorization server and vault port number.


|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".


|skip_verification
|boolean
a|Set to true to skip the verification of the updated user credentials
when updating credentials. The default value is false.


|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 computational 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.


|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).


|vault_host
|string
a|AKV host subdomain.
```

```
|verify_host
|boolean
a|Verify the identity of the AKV host name.


|verify_ip
|boolean
a|Verify the identity of the AKV IP address.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "authentication_method": "client_secret",
  "azure_reachability": {
    "code": "346758",
    "message": "AKV service is not reachable from all nodes - reason."
  },
  "client_certificate": "<CERTIFICATE-CONTENT>",
  "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
  "client_secret": "abcdef",
  "ekmip_reachability": [
    {
      "code": "346758",
      "message": "embedded KMIP server status unavailable on node.",
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ],
  "oauth_host": "login.microsoftonline.com",
  "port": 443,
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "string",
```

```
  "skip_verification": "",
  "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."
  },
  "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzz",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412",
  "vault_host": "vault.azure.net",
  "verify_host": "",
  "verify_ip": ""
}
====

== 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.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#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 computational 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
|string
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.


|===


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

```
Security keystore object reference.


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

|name
|string
a|Name of the configuration.


|uuid
|string
a|Keystore UUID.


|===


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

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

|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 computational 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
|string
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 computational 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
|string
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

SVM, applies only to SVM-scoped objects.


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

```
|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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 computational 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|

|enabled
|boolean
a|Indicates whether the configuration is enabled.


|oauth_host
|string
a|Open authorization server host name.


|port
|integer
a|Authorization server and vault port number.


|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".


|skip_verification
|boolean
a|Set to true to skip the verification of the updated user credentials
when updating credentials. The default value is false.


|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 computational 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.


|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).


|vault_host
|string
```

```
a|AKV host subdomain.


|verify_host
|boolean
a|Verify the identity of the AKV host name.


|verify_ip
|boolean
a|Verify the identity of the AKV IP address.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[IDba5f8e58cc411475b963bdfef9ed2cbb]]
= 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: 0
* 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

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

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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "uuid": "string"
  }
}
====

== Response
```

Status: 201, Created

```
== 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.

| 65537610
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being switched. If a previous attempt to switch the
keystore configuration failed, or was interrupted, the system will
continue to prevent rekeying for the SVM. Use the REST API PATCH method
"/api/security/key-stores/\{uuid}" to re-run and complete the operation.

| 65539436
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being initialized. Wait until the keystore is in the
active state, and rerun the rekey operation.

| 65539437
| Rekey cannot be performed on the SVM while the enabled keystore
configuration is being disabled.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID06d9bc14c1969b9e63f602d1939b9256]]
= 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: 0
* 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

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

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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "uuid": "string"
  }
}
====

== Response
```

Status: 201, Created

```
== 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.

| 65537544
| Missing wrapped top-level internal key protection key (KEK) from
internal database.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


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

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

|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


|===


[#returned_error]
```

```
[.api-collapsible-fifth-title]
returned_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 Barbican KMS configurations

:leveloffset: +1


[[IDc746774b81f55484e22e220828531bd6]]
= Manage Barbican KMS configurations
```

```
== Overview

Barbican Key Management Services (KMS) is a key management service that
provides a secure store for encryption keys. This feature
allows ONTAP to securely protect its encryption keys using Barbican KMS.
Before you can use Barbican KMS with ONTAP, you must provide ONTAP with
the necessary details to allow ONTAP to communicate with the deployed
Barbican application.
These details include the key ID URL, Keystone authentication URL, and the
application credentials ID and secret.
The property `barbican_reachability` is considered an advanced property
and is populated only when explicitly requested.

== Examples

=== Creating an inactive Barbican configuration for an SVM

The example Barbican configuration is created for a specific SVM but is
not enabled.
Note the _return_records=true_ query parameter can be used to return the
newly created key-manager keystore configuration.

----

# The API:
POST /api/security/barbican-kms

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/barbican-kms' -H 'accept:
application/hal+json' -H 'Content-Type: application/json' -d '{ "svm": {
"name": "barbican_svm" }, "configuration": {"name": "myConfiguration"},
"application_cred_id": "app1", "application_cred_secret": "secret1",
"key_id": "https://sample.keyid.com:9311/v1/secrets/5c610a4f-ea97-44b5-
8682-f4daeafa9647/", "keystone_url":
"https://sample.keystone.com:5000/v3/auth/tokens" }'

# The response:
{
"job": {
  "uuid": "5a208fb0-fa58-11ef-8c9f-005056bbeee5",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/5a208fb0-fa58-11ef-8c9f-005056bbeee5"
    }
```

```
  }
}
}
----

'''

=== Listing all Barbican configurations

The following example shows how to retrieve a list of all created Barbican
configurations.

----

# The API:
GET /api/security/barbican-kms

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/barbican-kms'

# The response:
{
"records": [
  {
    "configuration": {
      "name": "myConfiguration",
      "uuid": "5a134975-fa58-11ef-8c9f-005056bbeee5"
    },
    "uuid": "5a134975-fa58-11ef-8c9f-005056bbeee5",
    "_links": {
      "self": {
        "href": "/api/security/barbican-kms/5a134975-fa58-11ef-8c9f-
005056bbeee5"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/security/barbican-kms"
  }
}
}
----
```

```
'''

=== Retrieving a specific Barbican configuration

The following example shows how to retrieve information for a specific
Barbican configuration.

----

# The API:
GET /api/security/barbican-kms/{uuid}

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/barbican-kms/5a134975-fa58-
11ef-8c9f-005056bbeee5?fields=*'

# The response:
{
"configuration": {
  "name": "myConfiguration",
  "uuid": "5a134975-fa58-11ef-8c9f-005056bbeee5"
},
"uuid": "5a134975-fa58-11ef-8c9f-005056bbeee5",
"scope": "svm",
"svm": {
  "uuid": "ec8e0954-fa10-11ef-8c9f-005056bbeee5",
  "name": "barbican_svm"
},
"key_id": "https://sample.keyid.com:9311/v1/secrets/5c610a4f-ea97-44b5-
8682-f4daeafa9647/",
"application_cred_id": "app1",
"keystone_url": "https://sample.keystone.com:5000/v3/auth/tokens",
"proxy_type": "https",
"proxy_host": "",
"proxy_port": 0,
"proxy_username": "",
"verify": true,
"verify_host": true,
"enabled": false,
"timeout": 10,
"_links": {
  "self": {
    "href": "/api/security/barbican-kms/5a134975-fa58-11ef-8c9f-
005056bbeee5"
  }
}
```

```
}
----

'''

=== Retrieving an advanced property for a specific Barbican configuration

The following example shows how to retrieve an advanced property for a
specific Barbican configuration.

----

# The API:
GET /api/security/barbican-kms/{uuid}

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/barbican-kms/f72098a2-e908-
11ea-bd56-005056bb4222?fields=barbican_reachability'

# The response:
{
"configuration": {
  "name": "myConfiguration",
  "uuid": "f72098a2-e908-11ea-bd56-005056bb4222"
},
"uuid": "f72098a2-e908-11ea-bd56-005056bb4222",
"barbican_reachability": {
  "reachable": true,
  "message": "",
  "code": "0"
},
"_links": {
  "self": {
    "href": "/api/security/barbican-kms/f72098a2-e908-11ea-bd56-
005056bb4222"
  }
}
}
----

'''

=== Updating the application credentials ID and secret for a specific
Barbican configuration

The following example shows how to update the application credentials for
a specific Barbican configuration.
```

```
----

# The API:
PATCH /api/security/barbican-kms/{uuid}

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/barbican-kms/f72098a2-e908-
11ea-bd56-005056bb4222/' -d '{"application_cred_id": "app345",
"application_cred_secret" : "secret"}'

# The response:
{
"job": {
  "uuid": "921ee66a-fa5a-11ef-8c9f-005056bbeee5",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/921ee66a-fa5a-11ef-8c9f-005056bbeee5"
    }
  }
}
}
----

'''

=== Enabling a Barbican configuration

The newly created Barbican configuration is inactive by default. Use the
REST API PATCH method "/api/security/key-stores/\{uuid}" to enable the
configuration.

'''

=== Restoring keys

The following example shows how to restore keys for a specific Barbican
configuration.

----

# The API:
POST /api/security/barbican-kms/{uuid}/restore

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/barbican-kms/f72098a2-e908-
11ea-bd56-005056bb4222/restore'
```

```
# The response:
{
"job": {
  "uuid": "e89e7283-2c49-11f0-831c-005056bb33a5",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/e89e7283-2c49-11f0-831c-005056bb33a5"
    }
  }
}
}
----

'''

=== Rekey the internal key

The following example shows how to rekey the internal key based on a
specific Barbican configuration.

----

# The API:
POST /api/security/barbican-kms/{uuid}/rekey-internal

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/barbican-kms/f72098a2-e908-
11ea-bd56-005056bb4222/rekey-internal'

# The response:
{
"job": {
  "uuid": "921ee66a-fa5a-11ef-8c9f-005056bbeee5",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/921ee66a-fa5a-11ef-8c9f-005056bbeee5"
    }
  }
}
}
----

'''
```

```
[[ID85c5fbfe23ff83cde1c1144fb0cbeb90]]
= Retrieve Barbican KMS configurations for all SVMs

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

*Introduced In:* 9.17

Retrieves Barbican KMS configurations for all SVMs.

== Related ONTAP commands

* `security key-manager external barbican show`
* `security key-manager external barbican check`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|application_cred_id
|string
|query
|False
a|Filter by application_cred_id


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


|state.message
|string
|query
|False
```

```
a|Filter by state.message


|state.cluster_state
|boolean
|query
|False
a|Filter by state.cluster_state


|state.code
|string
|query
|False
a|Filter by state.code


|uuid
|string
|query
|False
a|Filter by uuid


|barbican_reachability.code
|string
|query
|False
a|Filter by barbican_reachability.code


|barbican_reachability.reachable
|boolean
|query
|False
a|Filter by barbican_reachability.reachable


|barbican_reachability.message
|string
|query
|False
a|Filter by barbican_reachability.message


|proxy_type
|string
```

```
|query
|False
a|Filter by proxy_type


|svm.name
|string
|query
|False
a|Filter by svm.name


|svm.uuid
|string
|query
|False
a|Filter by svm.uuid


|key_id
|string
|query
|False
a|Filter by key_id


|proxy_username
|string
|query
|False
a|Filter by proxy_username


|verify_host
|boolean
|query
|False
a|Filter by verify_host


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

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


|proxy_host
|string
|query
|False
a|Filter by proxy_host


|keystone_url
|string
|query
|False
a|Filter by keystone_url


|enabled
|boolean
|query
|False
a|Filter by enabled


|configuration.name
|string
|query
|False
a|Filter by configuration.name


|configuration.uuid
|string
|query
|False
a|Filter by configuration.uuid


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

```
|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: 15
* 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:#barbican[barbican]]
a|

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
```

```
          "href": "/api/resourcelink"
        }
      },
      "application_cred_id": "63e3cb77f84f42b7a0395a3efb7636f9",
      "barbican_reachability": {
        "code": "346758",
        "message": "Barbican KMS is not reachable from all nodes -
<reason>.",
        "reachable": ""
      },
      "configuration": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
      },
      "key_id": "https://172.29.58.184:9311/v1/secrets/5c610a4f-ea97-44b5-
8682-f4daeafa9647",
      "keystone_url": "https://keystoneip:5000/v3/auth/tokens",
      "proxy_host": "proxy.eng.com",
      "proxy_port": 1234,
      "proxy_type": "http",
      "proxy_username": "proxyuser",
      "scope": "string",
      "state": {
        "cluster_state": "",
        "code": "346758",
        "message": "Top-level internal key encryption key 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"
      },
      "timeout": 60,
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
```

```
    }
  ]
}
====

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65539801
| The Barbican Key Management Service is unreachable from one or more
nodes.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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|

|===


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

Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


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

|code
```

```
|string
a|Code corresponding to the error message. Returns 0 if Barbican KMS is
reachable from all nodes in the cluster.


|message
|string
a|Set to the appropriate error message when 'reachable' is false.


|reachable
|boolean
a|Set to true if the Barbican KMS is reachable from all nodes of the
cluster.


|===


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

Security keystore object reference.


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

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

|name
|string
a|Name of the configuration.


|uuid
|string
a|Keystore UUID.


|===
```

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

Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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 an SVM-KEK is present on all nodes of the cluster.


|code
|string
a|Code corresponding to the status message. Returns a 0 if the SVM-KEK is
available on all nodes in the cluster.


|message
|string
a|Error message returned when there's no SVM-KEK availability on the
cluster.


|===


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

SVM, applies only to SVM-scoped objects.
```

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

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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

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

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

|application_cred_id
|string
a|Keystone application credentials ID required to access the specified
Barbican KMS.


|barbican_reachability
|link:#barbican_reachability[barbican_reachability]
```

```
a|Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


|configuration
|link:#configuration[configuration]
a|Security keystore object reference.


|enabled
|boolean
a|Indicates whether the configuration is enabled.


|key_id
|string
a|Key Identifier URL of the Barbican KMS key encryption key. Must be an
HTTPS URL.


|keystone_url
|string
a|Keystone URL for the access token. Must be an HTTPS URL.


|proxy_host
|string
a|Proxy host name.


|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|Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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|SVM, applies only to SVM-scoped objects.


|timeout
|integer
a|Connection timeout in seconds.


|uuid
|string
a|A unique identifier of the Barbican KMS.


|verify
|boolean
a|Verify the identity of the Barbican KMS.


|verify_host
|boolean
a|Verify the identity of the Barbican KMS host 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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID9711804443b19517fea50fad21a60b58]]
= Create a Barbican KMS configuration for an SVM

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/barbican-kms`#

*Introduced In:* 9.17

Creates a Barbican KMS configuration for the specified SVM.

== Required properties

* `configuration.name` - Name for the new Barbican configuration.
* `svm.uuid` or `svm.name` - Existing SVM in which to create a Barbican
KMS.
* `key_id` - Barbican key URL.
* `keystone_url` - Keystone authentication URL.
* `application_cred_id` - Keystone authentication application ID with
access to the Barbican KMS.
* `application_cred_secret`- Application credentials secret to
authenticate the application credentials ID with Keystone.

== 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.
* `verify` - Verify the identity of the Barbican KMS?
* `verify_host` - Verify the identity of the Barbican KMS host name?
```

```
* `timeout` - Connection timeout in seconds.

== Related ONTAP commands

* `security key-manager external barbican create-config`


== 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: 0
* 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

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

|application_cred_id
|string
a|Keystone application credentials ID required to access the specified
Barbican KMS.


|application_cred_secret
|string
a|Keystone application credentials secret required to access the specified
Barbican KMS. It is not audited.


|barbican_reachability
|link:#barbican_reachability[barbican_reachability]
a|Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


|configuration
|link:#configuration[configuration]
a|Security keystore object reference.


|enabled
|boolean
a|Indicates whether the configuration is enabled.


|key_id
|string
```

```
a|Key Identifier URL of the Barbican KMS key encryption key. Must be an
HTTPS URL.


|keystone_url
|string
a|Keystone URL for the access token. Must be an HTTPS URL.


|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|Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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|SVM, applies only to SVM-scoped objects.


|timeout
|integer
a|Connection timeout in seconds.


|uuid
|string
a|A unique identifier of the Barbican KMS.


|verify
|boolean
a|Verify the identity of the Barbican KMS.


|verify_host
|boolean
a|Verify the identity of the Barbican KMS host name.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "application_cred_id": "63e3cb77f84f42b7a0395a3efb7636f9",
  "application_cred_secret": "secret",
  "barbican_reachability": {
    "code": "346758",
    "message": "Barbican KMS is not reachable from all nodes - <reason>.",
    "reachable": ""
  },
  "configuration": {
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
```

```
  },
  "key_id": "https://172.29.58.184:9311/v1/secrets/5c610a4f-ea97-44b5-
8682-f4daeafa9647",
  "keystone_url": "https://keystoneip:5000/v3/auth/tokens",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "string",
  "state": {
    "cluster_state": "",
    "code": "346758",
    "message": "Top-level internal key encryption key 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": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "timeout": 60,
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
}
====

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

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 1115127
| Package MT_EK_MGMT is not licensed in the cluster.

| 65539805
| Failed to create a Barbican Key Management Service configuration because
the "application-cred-secret" field is invalid or was not provided.

| 65539806
| Barbican Key Management Service (KMS) cannot be configured because not
all nodes in the cluster are running an effective cluster version of 9.17
or later to support the Barbican KMS feature.

| 65539807
| Barbican Key Management Service is not supported for the admin SVM.

| 65539808
| Failed to create the specified Barbican Key Management Service
configuration because a Barbican Key Management Service configuration with
the same name already exists.

| 65539809
| Barbican Key Management Service is not supported in MetroCluster
configurations.

| 65539810
| Failed to create a Barbican Key Management Service configuration because
the "key-id" field is invalid or was not provided. The URI scheme must be
HTTPS.

| 65539811
| Failed to create a Barbican Key Management Service configuration because
the "keystone-url" field is invalid or was not provided. The URI scheme
must be HTTPS.

| 65539835
| Failed to create a Barbican Key Management Service configuration because
```

```
the "application-cred-id" field cannot be empty.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#barbican_reachability]
[.api-collapsible-fifth-title]
barbican_reachability

Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.
```

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

|code
|string
a|Code corresponding to the error message. Returns 0 if Barbican KMS is
reachable from all nodes in the cluster.


|message
|string
a|Set to the appropriate error message when 'reachable' is false.


|reachable
|boolean
a|Set to true if the Barbican KMS is reachable from all nodes of the
cluster.


|===


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

Security keystore object reference.


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

|name
|string
a|Name of the configuration.


|uuid
|string
```

```
a|Keystore UUID.


|===


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

Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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 an SVM-KEK is present on all nodes of the cluster.


|code
|string
a|Code corresponding to the status message. Returns a 0 if the SVM-KEK is
available on all nodes in the cluster.


|message
|string
a|Error message returned when there's no SVM-KEK availability on the
cluster.


|===


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

```
svm

SVM, applies only to SVM-scoped objects.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


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

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

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

|application_cred_id
|string
a|Keystone application credentials ID required to access the specified
Barbican KMS.


|application_cred_secret
|string
```

```
a|Keystone application credentials secret required to access the specified
Barbican KMS. It is not audited.


|barbican_reachability
|link:#barbican_reachability[barbican_reachability]
a|Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


|configuration
|link:#configuration[configuration]
a|Security keystore object reference.


|enabled
|boolean
a|Indicates whether the configuration is enabled.


|key_id
|string
a|Key Identifier URL of the Barbican KMS key encryption key. Must be an
HTTPS URL.


|keystone_url
|string
a|Keystone URL for the access token. Must be an HTTPS URL.


|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|Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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|SVM, applies only to SVM-scoped objects.


|timeout
|integer
a|Connection timeout in seconds.


|uuid
|string
a|A unique identifier of the Barbican KMS.


|verify
```

```
|boolean
a|Verify the identity of the Barbican KMS.


|verify_host
|boolean
a|Verify the identity of the Barbican KMS host name.


|===


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID39a36bac944029355972b2a4f5429c5c]]
= Retrieve the Barbican KMS configuration for an SVM
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/barbican-kms/{uuid}`#

*Introduced In:* 9.17

Retrieves the Barbican KMS configuration for the SVM specified by the
UUID.

== Related ONTAP commands

* `security key-manager external barbican show`
* `security key-manager external barbican check`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|Barbican 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_cred_id
|string
a|Keystone application credentials ID required to access the specified
Barbican KMS.


|barbican_reachability
|link:#barbican_reachability[barbican_reachability]
a|Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


|configuration
|link:#configuration[configuration]
a|Security keystore object reference.


|enabled
|boolean
a|Indicates whether the configuration is enabled.


|key_id
|string
a|Key Identifier URL of the Barbican KMS key encryption key. Must be an
HTTPS URL.


|keystone_url
|string
a|Keystone URL for the access token. Must be an HTTPS URL.
```

```
|proxy_host
|string
a|Proxy host name.


|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|Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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|SVM, applies only to SVM-scoped objects.


|timeout
|integer
a|Connection timeout in seconds.
```

```
|uuid
|string
a|A unique identifier of the Barbican KMS.


|verify
|boolean
a|Verify the identity of the Barbican KMS.


|verify_host
|boolean
a|Verify the identity of the Barbican KMS host name.


|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "application_cred_id": "63e3cb77f84f42b7a0395a3efb7636f9",
  "barbican_reachability": {
    "code": "346758",
    "message": "Barbican KMS is not reachable from all nodes - <reason>.",
    "reachable": ""
  },
  "configuration": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  },
  "key_id": "https://172.29.58.184:9311/v1/secrets/5c610a4f-ea97-44b5-
8682-f4daeafa9647",
  "keystone_url": "https://keystoneip:5000/v3/auth/tokens",
```

```
  "proxy_host": "proxy.eng.com",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "string",
  "state": {
    "cluster_state": "",
    "code": "346758",
    "message": "Top-level internal key encryption key 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"
  },
  "timeout": 60,
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
}
====

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65539801
| The Barbican Key Management Service is unreachable from one or more
nodes.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.
```

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

|error
|link:#returned_error[returned_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|

|===


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

Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


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

```
|code
|string
a|Code corresponding to the error message. Returns 0 if Barbican KMS is
reachable from all nodes in the cluster.


|message
|string
a|Set to the appropriate error message when 'reachable' is false.


|reachable
|boolean
a|Set to true if the Barbican KMS is reachable from all nodes of the
cluster.


|===


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

Security keystore object reference.


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

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

|name
|string
a|Name of the configuration.


|uuid
|string
a|Keystore UUID.
```

```
|===


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

Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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 an SVM-KEK is present on all nodes of the cluster.


|code
|string
a|Code corresponding to the status message. Returns a 0 if the SVM-KEK is
available on all nodes in the cluster.


|message
|string
a|Error message returned when there's no SVM-KEK availability on the
cluster.


|===


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

SVM, applies only to SVM-scoped objects.
```

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

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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.


|===


[#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


|===
```

```
[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID1802219288f82aebbb9aa2b57ae1cc2d]]
= Update the Barbican KMS configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/barbican-kms/{uuid}`#

*Introduced In:* 9.17
```

```
Updates the Barbican KMS configuration.

== Optional properties

* `application_cred_id` - New credentials used to verify the application's
identity to the Barbican KMS. You must provide both `application_cred_id`
and `application_cred_secret` to update the credentials.
* `application_cred_secret` - New credentials secret used to verify the
application's identity to the Barbican KMS. You must provide both
`application_cred_id` and `application_cred_secret` to update the
credentials.
* `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.
* `verify` - Verify the identity of the Barbican KMS?
* `verify_host` - Verify the identity of the Barbican KMS host name?
* `timeout` - Connection timeout in seconds.

== Related ONTAP commands

* `security key-manager external barbican update-credentials`
* `security key-manager external barbican update-config`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|Barbican 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: 0
* Max value: 120
* Min value: 0

|===

== Request Body



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

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

|application_cred_id
|string
a|Keystone application credentials ID required to access the specified
Barbican KMS.


|application_cred_secret
|string
a|Keystone application credentials secret required to access the specified
Barbican KMS. It is not audited.


|barbican_reachability
|link:#barbican_reachability[barbican_reachability]
a|Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
```

```
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


|enabled
|boolean
a|Indicates whether the configuration is enabled.


|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|Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
```

```
This is an advanced property; there is an added computational 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.


|timeout
|integer
a|Connection timeout in seconds.


|uuid
|string
a|A unique identifier of the Barbican KMS.


|verify
|boolean
a|Verify the identity of the Barbican KMS.


|verify_host
|boolean
a|Verify the identity of the Barbican KMS host name.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "application_cred_id": "63e3cb77f84f42b7a0395a3efb7636f9",
  "application_cred_secret": "secret",
  "barbican_reachability": {
    "code": "346758",
    "message": "Barbican KMS is not reachable from all nodes - <reason>.",
    "reachable": ""
  },
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
```

```
  "scope": "string",
  "state": {
    "cluster_state": "",
    "code": "346758",
    "message": "Top-level internal key encryption key 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."
  },
  "timeout": 60,
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
}
====

== Response
```

Status: 200, Ok

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

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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "uuid": "string"
  }
}
====

== Response
```

Status: 202, Accepted

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65539223
| Failed to check the health of the Barbican Key Management Service.

| 65539814
| Failed to update the Barbican Key Management Service configuration
because the "application-cred-secret" field is invalid or was not
provided.

| 65539815
| Failed to update the Barbican Key Management Service configuration
because the "application-cred-id" field is invalid or was not provided.

| 65539832
| Specified Barbican Key Management Service configuration does not exist.

| 65539841
| Both "application_cred_id" and "application_cred_secret" are required.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#barbican_reachability]
[.api-collapsible-fifth-title]
barbican_reachability

Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


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

|code
|string
a|Code corresponding to the error message. Returns 0 if Barbican KMS is
reachable from all nodes in the cluster.


|message
|string
a|Set to the appropriate error message when 'reachable' is false.


|reachable
|boolean
```

```
a|Set to true if the Barbican KMS is reachable from all nodes of the
cluster.


|===


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

Security keystore object reference.


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

|name
|string
a|Name of the configuration.


|uuid
|string
a|Keystore UUID.


|===


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

Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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 an SVM-KEK is present on all nodes of the cluster.


|code
|string
a|Code corresponding to the status message. Returns a 0 if the SVM-KEK is
available on all nodes in the cluster.


|message
|string
a|Error message returned when there's no SVM-KEK availability on the
cluster.


|===


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

SVM, applies only to SVM-scoped objects.


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

|name
|string
a|The name of the SVM. This field cannot be specified in a PATCH method.


|uuid
|string
a|The unique identifier of the SVM. This field cannot be specified in a
PATCH method.
```

```
|===


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

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

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

|application_cred_id
|string
a|Keystone application credentials ID required to access the specified
Barbican KMS.


|application_cred_secret
|string
a|Keystone application credentials secret required to access the specified
Barbican KMS. It is not audited.


|barbican_reachability
|link:#barbican_reachability[barbican_reachability]
a|Indicates whether the Barbican KMS is reachable from all nodes in the
cluster.
This is an advanced property; there is an added computational cost to
retrieving its value. The property is not populated for either a
collection GET request or an instance GET request unless it is explicitly
requested using the field's query parameter or GET for all advanced
properties is enabled.


|enabled
|boolean
a|Indicates whether the configuration is enabled.
```

```
|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|Indicates whether or not the SVM key encryption key (KEK) is available
cluster wide.
This is an advanced property; there is an added computational 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.


|timeout
|integer
a|Connection timeout in seconds.
```

```
|uuid
|string
a|A unique identifier of the Barbican KMS.


|verify
|boolean
a|Verify the identity of the Barbican KMS.


|verify_host
|boolean
a|Verify the identity of the Barbican KMS host name.


|===


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
```

```
====



[[ID8679d0bad8a801b46047e345d238b056]]
= Rekey the internal key in the key hierarchy for an SVM with a Barbican
KMS configuration

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/barbican-kms/{uuid}/rekey-internal`#

*Introduced In:* 9.17

Rekeys the internal key in the key hierarchy for an SVM with a Barbican
KMS configuration.

== Related ONTAP commands

* `security key-manager external barbican rekey-internal`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|UUID of the existing Barbican 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: 0
* 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

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

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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "uuid": "string"
  }
}
====

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65536205
| Internal error. Failed to generate SVM key in the kernel.

| 65536882
| Internal error. UUID is missing.

| 65536883
```

```
| Internal error. Volume encryption key is missing.

| 65536884
| Internal error. Volume encryption key is invalid.

| 65536889
| Internal error. Volume has invalid encryption blob.

| 65536973
| Internal error. Volume DSID is missing.

| 65537533
| Internal error. Failed to unwrap SVM key encryption key.

| 65537547
| One or more volume encryption keys (VEKs) for this data SVM's encrypted
volumes are stored in the key manager configured for the admin SVM. Use
the REST API POST method "/api/security/key-
managers/{source.svm.uuid}/migrate" to migrate these keys from the admin
SVM's key manager to this data SVM's key manager before running the rekey
operation.

| 65537556
| ONTAP is unable to encrypt or decrypt because the configured external
key manager is in a blocked state. Possible reasons for a blocked state
include the top-level external key protection key is not found, disabled
or has insufficient privileges. Resolve the external key manager key
issues at the key manager's portal before running the rekey operation.

| 65537565
| Internal error. Failed to update the VDEK blob.

| 65537610
| Rekey cannot be performed while the enabled keystore configuration is
being switched. If a previous attempt to switch the keystore configuration
failed, or was interrupted, the system will continue to prevent rekeying.
Use the REST API PATCH method "/api/security/key-stores/\{uuid}" to re-run
and complete the operation.

| 65539200
| The key custodian not provided with an external key value store.

| 65539201
| Failed to encrypt.

| 65539202
| Failed to decrypt.
```

```
| 65539416
| Internal error. Failed to parse the key value store response.

| 65539436
| Rekey cannot be performed while the enabled keystore configuration is
being initialized. Wait until the keystore is in the active state, and
rerun the rekey operation.

| 65539437
| Rekey cannot be performed while the enabled keystore configuration is
being disabled.

| 65539817
| The Barbican Key Management Service is not configured.

| 65539834
| New Key ID not found.

| 65539836
| No Key Management Service configured.

| 65539844
| Failed to import the SVM-KEK.

| 196608088
| Internal error. Failed to get encryption operation status.

| 196608352
| Internal error. The encryption blob was not found in the RDB table.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


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

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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====
```

```
[[ID12d302284feb9c88290d89d4a5dece76]]
= Restore the keys for an SVM from a configured Barbican KMS

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/barbican-kms/{uuid}/restore`#

*Introduced In:* 9.17

Restores the keys for an SVM from a configured Barbican KMS.

== Related ONTAP commands

* `security key-manager external barbican restore`


== Parameters

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

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|UUID of the existing Barbican 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: 0
* 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

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

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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "uuid": "string"
  }
}
====

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65539817
| The Barbican Key Management Service is not configured.

| 65539842
| Failed to restore the SVM-KEK on at least one node.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


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

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

|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


|===


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

```
returned_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


[[ID5a3b5ac1c4cc9cd43b2f61f7aac4492a]]
= 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.

== Required properties

* `subject_name` - Subject details of the certificate, including but not
limited to the common name. Can be omitted if subject_alternatives is
specified.
* `subject_alternatives` - Subject Alternate Name (SAN) extensions. Only
required if a common name is not specified using subject_name.

== Recommended optional properties

* `security_strength` - Key size of the certificate, in bits. Specifying a
stronger security strength in bits is recommended when creating a
certificate. A value of at least 128 is necessary when using EC algorithm
if the certificate is to be used in the context of TLSv1.3.
* `hash_function` -  Hashing function.
* `algorithm` - Asymmetric algorithm. Algorithm used to generate a
public/private key pair when creating a certificate.

== 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

|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]
{
  "algorithm": "string",
  "csr": "string",
  "extended_key_usages": [
    "string"
  ],
  "generated_private_key": "string",
  "hash_function": "string",
  "key_usages": [
    "string"
  ],
  "security_strength": 112,
  "subject_alternatives": {
    "dns": [
      "*.example.com"
    ],
    "email": [
      "abc@example.com"
    ],
```

```
    "ip": [
      "10.225.34.10"
    ],
    "uri": [
      "http://example.com"
    ]
  },
  "subject_name": "C=US,O=NTAP,CN=test.domain.com"
}
====

== Response
```

Status: 200, Ok

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

|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]
{
  "algorithm": "string",
  "csr": "string",
  "extended_key_usages": [
    "string"
  ],
  "generated_private_key": "string",
  "hash_function": "string",
  "key_usages": [
    "string"
  ],
  "security_strength": 112,
  "subject_alternatives": {
    "dns": [
      "*.example.com"
    ],
    "email": [
      "abc@example.com"
```

```
    ],
    "ip": [
      "10.225.34.10"
    ],
    "uri": [
      "http://example.com"
    ]
  },
  "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.

| 3735750
```

```
| Cannot supply "critical" as the only value in a list of extension
values.

| 52560173
| Hash function is not supported for digital signatures.

| 52560423
| Failed to read the relative distinguished names.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


== 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
[#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

|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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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


[[IDbd61fd824537add1007cdff1c06246e8]]
= Manage security certificates



:doctype: book

== 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": "cert_name",
    "_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": "cert_name",
    "_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": "<CERTIFICATE-CONTENT>",
"_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\": \"<CERTIFICATE-CONTENT>\"  }"
----

'''

=== 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\":
\"<CERTIFICATE-CONTENT>\"  }"
----

'''

=== Installing a CA-signed 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\", \"public_certificate\":
\"<CERTIFICATE-CONTENT>\", \"intermediate_certificates\": [\"<CERTIFICATE-
CONTENT>\",\"<CERTIFICATE-CONTENT>\"]}"
----

'''

=== 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\": \"<CERTIFICATE-
CONTENT>\",  \"hash_function\": \"sha256\"}"

# The response:
{
"public_certificate": "<CERTIFICATE-CONTENT>"
}
----

=== 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"
}
----

'''

----

### Download and install a certificate from the Azure Key Vault.
----

= 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\"}, \"name\" : \"vs0-client-cert\", \"type\"
: \"client\", \"azure\": { \"key_vault\" :
\"https://example.vault.azure.net\", \"client_id\" : \"12345678-abcd-1234-
12ad-dfasdffgfdaaa\", \"tenant_id\" : \"12345678-abcd-abcd-test-
720ef604b100\", \"client_secret\" : \"clientSecretString\",
\"verify_host\": false }}" { "job": { "uuid": "be8d45cb-1d41-11ee-9725-
005056ae0f31", "_links": { "self": { "href": "/api/cluster/jobs/be8d45cb-
1d41-11ee-9725-005056ae0f31" } } } }+++</mgmt-ip>+++
```

Retrieve security certificates

GET `/security/certificates`

Introduced In: 9.6

Retrieves security certificates.

Related ONTAP commands

- `security certificate show`

Parameters

Name	Type	In	Required	Description
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
subject_key_identifier	string	query	False	Filter by subject_key_identifier • Introduced in: 9.8
ca	string	query	False	Filter by ca • maxLength: 256 • minLength: 1

Name	Type	In	Required	Description
public_certificate	string	query	False	Filter by public_certificate • Introduced in: 9.8
hash_function	string	query	False	Filter by hash_function
scope	string	query	False	Filter by scope
subject_alternatives.dns	string	query	False	Filter by subject_alternatives.dns • Introduced in: 9.15
subject_alternatives.uri	string	query	False	Filter by subject_alternatives.uri • Introduced in: 9.15
subject_alternatives.email	string	query	False	Filter by subject_alternatives.email • Introduced in: 9.15
subject_alternatives.ip	string	query	False	Filter by subject_alternatives.ip • Introduced in: 9.15
serial_number	string	query	False	Filter by serial_number • maxLength: 40 • minLength: 1

Name	Type	In	Required	Description
uuid	string	query	False	Filter by uuid • Introduced in: 9.8
key_size	integer	query	False	Filter by key_size
authority_key_identifier	string	query	False	Filter by authority_key_identifier • Introduced in: 9.8
common_name	string	query	False	Filter by common_name
type	string	query	False	Filter by type
expiry_time	string	query	False	Filter by expiry_time
name	string	query	False	Filter by name • Introduced in: 9.8
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
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[security_certificate]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "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",
      "azure": {
        "verify_host": true
      },
      "ca": "string",
      "common_name": "test.domain.com",
      "expiry_time": "2030-01-25 06:20:13 -0500",
      "hash_function": "string",
      "key_size": 512,
      "name": "string",
      "public_certificate": "<CERTIFICATE-CONTENT>",
      "scope": "string",
      "serial_number": "string",
      "subject_alternatives": {
        "dns": [
          "*.example.com"
        ],
        "email": [
          "<a href="mailto:abc@example.com">abc@example.com</a>"
        ],
        "ip": [
          "10.225.34.10"
        ],
        "uri": [
          "http://example.com"
        ]
```

```
      },
      "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": "string",
      "uuid": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

proxy

azure

Name	Type	Description
proxy	proxy	

subject_alternatives

Name	Type	Description
dns	array[string]	A list of DNS names for Subject Alternate name extension.
email	array[string]	A list of email addresses for Subject Alternate name extension
ip	array[string]	A list of IP addresses for Subject Alternate name extension.
uri	array[string]	A list of URIs for Subject Alternate name extension.

svm

SVM, applies only to SVM-scoped objects.

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

security_certificate

Name	Type	Description
_links	_links	
authority_key_identifier	string	Provides the key identifier of the issuing CA certificate that signed the SSL certificate.
azure	azure	
ca	string	Certificate authority
common_name	string	FQDN or custom common name. Provide on POST when creating a self-signed certificate.
expiry_time	string	Certificate expiration time, in ISO 8601 duration format or date and time format. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.
hash_function	string	Hashing function. Can be provided on POST when creating a self-signed certificate. Hash functions md5 and sha1 are not allowed on POST.
key_size	integer	Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate with a minimum permissible value of 2048.

Name	Type	Description
name	string	Certificate name or name of the certificate to be downloaded from the Azure Key Vault (AKV). If not provided in POST, a unique name specific to the SVM is automatically generated.
public_certificate	string	Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
serial_number	string	Serial number of certificate.
subject_alternatives	subject_alternatives	
subject_key_identifier	string	Provides the key identifier used to identify the public key in the SSL certificate.
svm	svm	SVM, applies only to SVM-scoped objects.

Name	Type	Description
type	string	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 • x-nullable: true
uuid	string	Unique ID that identifies a certificate.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create or install security certificates

POST `/security/certificates`

Introduced In: 9.6

Creates or installs a certificate or downloads a certificate from Azure Key Vault (AKV) and installs it on the ONTAP cluster.

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 or the name of the certificate in AKV, required for downloading AKV certificates. If one is not provided, it is automatically generated.

AKV required properties for downloading a certificate

- `azure.key_vault` - URI of the Azure Key Vault.
- `azure.client_id` - Application (client) ID of the deployed Azure application with appropriate access to an AKV.
- `azure.tenant_id` - Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV.
- `azure.client_secret` - Secret used by the application to prove its identity to AKV.
- `azure.client_certificate` - PKCS12 certificate used by the application to prove its identity to AKV.

AKV optional properties for downloading a certificate

- `azure.oauth_host` - Open authorization server host name.
- `azure.proxy.type` - Type of proxy (http, https etc.) if proxy configuration is used.
- `azure.proxy.host` - Proxy hostname if proxy configuration is used.
- `azure.proxy.port` - Proxy port number if proxy configuration is used.
- `azure.proxy.username` - Proxy username if proxy configuration is used.
- `azure.proxy.password` - Proxy password if proxy configuration is used.
- `azure.timeout` - AKV connection timeout in seconds.
- `azure.verify_host` - Verify the identity of the AKV host name.

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`
- `security certificate azure-install`

Parameters

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

Request Body

Name	Type	Description
authority_key_identifier	string	Provides the key identifier of the issuing CA certificate that signed the SSL certificate.
azure	azure	

Name	Type	Description
ca	string	Certificate authority
common_name	string	FQDN or custom common name. Provide on POST when creating a self-signed certificate.
expiry_time	string	Certificate expiration time, in ISO 8601 duration format or date and time format. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.
hash_function	string	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]	Chain of intermediate Certificates in PEM format. Only valid in POST when installing a certificate.
key_size	integer	Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate with a minimum permissible value of 2048.
name	string	Certificate name or name of the certificate to be downloaded from the Azure Key Vault (AKV). If not provided in POST, a unique name specific to the SVM is automatically generated.
private_key	string	Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.
public_certificate	string	Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.

Name	Type	Description
serial_number	string	Serial number of certificate.
subject_alternatives	subject_alternatives	
subject_key_identifier	string	Provides the key identifier used to identify the public key in the SSL certificate.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	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 • x-nullable: true
uuid	string	Unique ID that identifies a certificate.

Example request

```
{
  "authority_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D7",
  "azure": {
    "client_certificate": "PEM Cert",
    "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
    "client_secret": "abcdef",
    "key_vault": "https://kmip-akv-keyvault.vault.azure.net/",
    "oauth_host": "login.microsoftonline.com",
    "proxy": {
      "host": "proxy.eng.com",
      "password": "proxypassword",
      "port": 1234,
      "type": "string",
      "username": "proxyuser"
    },
    "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzz",
    "timeout": 25
  },
  "ca": "string",
  "common_name": "test.domain.com",
  "expiry_time": "2030-01-25 06:20:13 -0500",
  "hash_function": "string",
  "intermediate_certificates": [
    "<CERTIFICATE-CONTENT>"
  ],
  "key_size": 512,
  "name": "string",
  "private_key": "-----BEGIN PRIVATE KEY-----\\nprivate-key\\n-----END
PRIVATE KEY-----\\n",
  "public_certificate": "<CERTIFICATE-CONTENT>",
  "serial_number": "string",
  "subject_alternatives": {
    "dns": [
      "*.example.com"
    ],
    "email": [
      "<a href="mailto:abc@example.com">abc@example.com</a>"
    ],
    "ip": [
      "10.225.34.10"
    ],
    "uri": [
      "http://example.com"
```

```
    ]
  },
  "subject_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D8",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "string",
  "uuid": "string"
}
```


Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[security_certificate]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "authority_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D7",
      "azure": {
        "client_certificate": "PEM Cert",
        "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
        "client_secret": "abcdef",
        "key_vault": "https://kmip-akv-keyvault.vault.azure.net/",
        "oauth_host": "login.microsoftonline.com",
        "proxy": {
          "host": "proxy.eng.com",
          "password": "proxypassword",
          "port": 1234,
          "type": "string",
          "username": "proxyuser"
        },
        "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzz",
        "timeout": 25
      },
      "ca": "string",
      "common_name": "test.domain.com",
      "expiry_time": "2030-01-25 06:20:13 -0500",
      "hash_function": "string",
      "intermediate_certificates": [
        "<CERTIFICATE-CONTENT>"
      ],
      "key_size": 512,
      "name": "string",
      "private_key": "-----BEGIN PRIVATE KEY-----\\nprivate-key\\n-----
END PRIVATE KEY-----\\n",
      "public_certificate": "<CERTIFICATE-CONTENT>",
      "serial_number": "string",
      "subject_alternatives": {
        "dns": [
          "*.example.com"
        ],
        "email": [
          "<a href="mailto:abc@example.com">abc@example.com</a>"
        ],
        "ip": [
          "10.225.34.10"
```

```
        ],
        "uri": [
          "http://example.com"
        ]
      },
      "subject_key_identifier":
"26:1F:C5:53:5B:D7:9E:E2:37:74:F4:F4:06:09:03:3D:EB:41:75:D8",
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "type": "string",
      "uuid": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	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.	

Error Code	Description
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.	
3735700	The specified key size is not supported.
	52560173

Error Code	Description
The hash function is not supported for digital signatures.	
3735751	Failed to authenticate and fetch the access token from Azure OAuth host.
	3735752
Failed to extract the private key from the Azure Key Vault certificate.	3735753
Unsupported content_type in the Azure secrets response.	3735754
Internal error. Failed to parse the JSON response from Azure Key Vault.	3735755
REST call to Azure failed.	3735756
Invalid client certificate.	3735757
Internal error. Failed to generate client assertion.	3735762
Provided Azure Key Vault configuration is incorrect.	3735763
Provided Azure Key Vault configuration is incomplete.	3735764

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

proxy

Name	Type	Description
host	string	Proxy host.
password	string	Proxy password. Password is not audited.
port	integer	Proxy port.
type	string	Proxy type.
username	string	Proxy username.

azure

Name	Type	Description
client_certificate	string	PKCS12 certificate used by the application to prove its identity to AKV.
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV.
client_secret	string	Secret used by the application to prove its identity to AKV.

Name	Type	Description
key_vault	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • x-ntap-createOnly: true • Introduced in: 9.14 • x-nullable: true
oauth_host	string	Open authorization server host name.
proxy	proxy	
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV.
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.

subject_alternatives

Name	Type	Description
dns	array[string]	A list of DNS names for Subject Alternate name extension.
email	array[string]	A list of email addresses for Subject Alternate name extension
ip	array[string]	A list of IP addresses for Subject Alternate name extension.
uri	array[string]	A list of URIs for Subject Alternate name extension.

svm

SVM, applies only to SVM-scoped objects.

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

security_certificate

Name	Type	Description
authority_key_identifier	string	Provides the key identifier of the issuing CA certificate that signed the SSL certificate.
azure	azure	
ca	string	Certificate authority
common_name	string	FQDN or custom common name. Provide on POST when creating a self-signed certificate.
expiry_time	string	Certificate expiration time, in ISO 8601 duration format or date and time format. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.
hash_function	string	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]	Chain of intermediate Certificates in PEM format. Only valid in POST when installing a certificate.

Name	Type	Description
key_size	integer	Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate with a minimum permissible value of 2048.
name	string	Certificate name or name of the certificate to be downloaded from the Azure Key Vault (AKV). If not provided in POST, a unique name specific to the SVM is automatically generated.
private_key	string	Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.
public_certificate	string	Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.
serial_number	string	Serial number of certificate.
subject_alternatives	subject_alternatives	
subject_key_identifier	string	Provides the key identifier used to identify the public key in the SSL certificate.
svm	svm	SVM, applies only to SVM-scoped objects.

Name	Type	Description
type	string	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 • x-nullable: true
uuid	string	Unique ID that identifies a certificate.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Sign security certificates

POST `/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

Name	Type	In	Required	Description
ca.uuid	string	path	True	UUID of the existing certificate authority certificate
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
expiry_time	string	Certificate expiration time, in ISO 8601 duration format or date and time format. The allowed expiration time range is between 1 day to 10 years.
hash_function	string	Hashing function
signing_request	string	Certificate signing request to be signed by the given certificate authority. Request should be in X509 PEM format.

Example request

```
{
  "expiry_time": "P1DT2H3M4S or '2030-01-25T11:20:13Z'",
  "hash_function": "string",
  "signing_request": "<CERTIFICATE-CONTENT>"
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
public_certificate	string	CA signed public key Certificate

Example response


```
{
  "public_certificate": "string"
}
```


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.
3735701	Invalid expiration period. The allowed range for expiration time is between 1 and 3652 days.

Definitions

See Definitions

security_certificate_sign

Name	Type	Description
expiry_time	string	Certificate expiration time, in ISO 8601 duration format or date and time format. The allowed expiration time range is between 1 day to 10 years.
hash_function	string	Hashing function
signing_request	string	Certificate signing request to be signed by the given certificate authority. Request should be in X509 PEM format.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete security certificates

DELETE `/security/certificates/{uuid}`

Introduced In: 9.6

Deletes a security certificate.

Related ONTAP commands

- `security certificate delete`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	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.
3735681	Cannot delete preinstalled `server-ca` certificates. Use the CLI to complete the operation.
52560272	The certificate could not be removed due to being in use by one or more subsystems.

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve security certificates

GET `/security/certificates/{uuid}`

Introduced In: 9.6

Retrieves security certificates.

Related ONTAP commands

- `security certificate show`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Certificate UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
authority_key_identifier	string	Provides the key identifier of the issuing CA certificate that signed the SSL certificate.
azure	azure	
ca	string	Certificate authority
common_name	string	FQDN or custom common name. Provide on POST when creating a self-signed certificate.
expiry_time	string	Certificate expiration time, in ISO 8601 duration format or date and time format. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.

Name	Type	Description
hash_function	string	Hashing function. Can be provided on POST when creating a self-signed certificate. Hash functions md5 and sha1 are not allowed on POST.
key_size	integer	Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate with a minimum permissible value of 2048.
name	string	Certificate name or name of the certificate to be downloaded from the Azure Key Vault (AKV). If not provided in POST, a unique name specific to the SVM is automatically generated.
public_certificate	string	Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
serial_number	string	Serial number of certificate.
subject_alternatives	subject_alternatives	
subject_key_identifier	string	Provides the key identifier used to identify the public key in the SSL certificate.
svm	svm	SVM, applies only to SVM-scoped objects.

Name	Type	Description
type	string	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 • x-nullable: true
uuid	string	Unique ID that identifies a certificate.

Example response


```
{
  "_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",
  "azure": {
    "verify_host": true
  },
  "ca": "string",
  "common_name": "test.domain.com",
  "expiry_time": "2030-01-25 06:20:13 -0500",
  "hash_function": "string",
  "key_size": 512,
  "name": "string",
  "public_certificate": "<CERTIFICATE-CONTENT>",
  "scope": "string",
  "serial_number": "string",
  "subject_alternatives": {
    "dns": [
      "*.example.com"
    ],
    "email": [
      "<a href="mailto:abc@example.com">abc@example.com</a>"
    ],
    "ip": [
      "10.225.34.10"
    ],
    "uri": [
      "http://example.com"
    ]
  },
  "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": "string",
  "uuid": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

proxy

azure

Name	Type	Description
proxy	proxy	

subject_alternatives

Name	Type	Description
dns	array[string]	A list of DNS names for Subject Alternate name extension.
email	array[string]	A list of email addresses for Subject Alternate name extension
ip	array[string]	A list of IP addresses for Subject Alternate name extension.
uri	array[string]	A list of URIs for Subject Alternate name extension.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage external-role-mapping entries

Manage external-role-mapping entries

Overview

This API is used to map external identity provider roles to ONTAP roles. The POST request creates an external role to ONTAP role mapping. Various responses are shown in the examples below.

Examples

Creating an external role to ONTAP role mapping entry

The following output shows how to create an external role to ONTAP role mapping entry.

```
# The API
/api/security/external-role-mappings

# The call:
curl -X POST "https://<mgmt-ip>/api/security/external-role-mappings" -d '{
"external_role": "Administrator", "ontap_role": { "name": "admin" },
"provider": "adfs", "comment": "Admin role" }'
```

Retrieving all external role to ONTAP role mapping entries

The following output shows all external role to ONTAP role mapping entries.

```
# The API
/api/security/external-role-mappings

# The call:
curl -X GET "https://<mgmt-ip>/api/security/external-role-mappings"

# The response:
{
 "records": [
 {
   "external_role": "Administrator",
   "provider": "adfs"
 }
 ],
 "num_records": 1
}
```

Retrieve all external-role-mapping entries

GET `/security/external-role-mappings`

Introduced In: 9.16

Retrieves all external-role-mapping entries.

Related ONTAP commands

- `security login external-role-mapping show`

Parameters

Name	Type	In	Required	Description
provider	string	query	False	Filter by provider

Name	Type	In	Required	Description
timestamp	string	query	False	Filter by timestamp
comment	string	query	False	Filter by comment
external_role	string	query	False	Filter by external_role
ontap_role.name	string	query	False	Filter by ontap_role.name
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records.
records	array[security_external_role_mapping]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "comment": "string",
      "external_role": "string",
      "ontap_role": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "admin"
      },
      "provider": "string",
      "timestamp": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

ontap_role

ONTAP role to map with the external identity role.

Name	Type	Description
_links	_links	
name	string	Role name

security_external_role_mapping

Name	Type	Description
_links	self_link	
comment	string	Any comment regarding this external-role-mapping entry.
external_role	string	External Identity provider role.
ontap_role	ontap_role	ONTAP role to map with the external identity role. • Introduced in: 9.16

Name	Type	Description
provider	string	Type of the external identity provider.
timestamp	string	Date and time indicating when this external-role-mapping entry was created.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create an external-role-mapping entry

POST `/security/external-role-mappings`

Introduced In: 9.16

Creates an external-role-mapping entry.

Required properties

- `external_role`
- `provider`
- `ontap_role`

Optional properties

- `comment`

Related ONTAP commands

- `security login external-role-mapping create`

Parameters

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

Request Body

Name	Type	Description
comment	string	Any comment regarding this external-role-mapping entry.
external_role	string	External Identity provider role.
ontap_role	ontap_role	ONTAP role to map with the external identity role. • Introduced in: 9.16
provider	string	Type of the external identity provider.
timestamp	string	Date and time indicating when this external-role-mapping entry was created.

Example request

```
{
  "comment": "string",
  "external_role": "string",
  "ontap_role": {
    "name": "admin"
  },
  "provider": "string",
  "timestamp": "string"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records.
records	array[security_external_role_mapping]	

Example response


```
{
  "records": [
    {
      "comment": "string",
      "external_role": "string",
      "ontap_role": {
        "name": "admin"
      },
      "provider": "string",
      "timestamp": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636243	Provided ONTAP role is not configured.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

_links

ontap_role

ONTAP role to map with the external identity role.

Name	Type	Description
name	string	Role name

security_external_role_mapping

Name	Type	Description
comment	string	Any comment regarding this external-role-mapping entry.
external_role	string	External Identity provider role.
ontap_role	ontap_role	ONTAP role to map with the external identity role. • Introduced in: 9.16
provider	string	Type of the external identity provider.
timestamp	string	Date and time indicating when this external-role-mapping entry was created.

collection_links

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete an external-role-mapping entry

DELETE `/security/external-role-mappings/{external_role}/{provider}`

Introduced In: 9.16

Deletes an external-role-mapping entry.

Related ONTAP commands

- `security login external-role-mapping delete`

Parameters

Name	Type	In	Required	Description
external_role	string	path	True	
provider	string	path	True	

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve an external-role-mapping entry

GET `/security/external-role-mappings/{external_role}/{provider}`

Introduced In: 9.16

Retrieves an external-role-mapping entry.

Related ONTAP commands

- `security login external-role-mapping show`

Parameters

Name	Type	In	Required	Description
external_role	string	path	True	External Identity provider role.
provider	string	path	True	Type of the external identity provider.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	
comment	string	Any comment regarding this external-role-mapping entry.
external_role	string	External Identity provider role.
ontap_role	ontap_role	ONTAP role to map with the external identity role. • Introduced in: 9.16
provider	string	Type of the external identity provider.
timestamp	string	Date and time indicating when this external-role-mapping entry was created.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "comment": "string",
  "external_role": "string",
  "ontap_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "provider": "string",
  "timestamp": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

ontap_role

ONTAP role to map with the external identity role.

Name	Type	Description
_links	_links	
name	string	Role name

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update an external-role-mapping entry

PATCH `/security/external-role-mappings/{external_role}/{provider}`

Introduced In: 9.16

Updates an external-role-mapping entry.

Related ONTAP commands

- `security login external-role-mapping modify`

Parameters

Name	Type	In	Required	Description
external_role	string	path	True	External Identity provider role.
provider	string	path	True	Type of the external identity provider.
fields	array[string]	query	False	Specify the fields to return.

Request Body

Name	Type	Description
comment	string	Any comment regarding this external-role-mapping entry.
ontap_role	ontap_role	ONTAP role to map with the external identity role. • Introduced in: 9.16
timestamp	string	Date and time indicating when this external-role-mapping entry was created.

Example request

```
{
  "comment": "string",
  "ontap_role": {
    "name": "admin"
  },
  "timestamp": "string"
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
comment	string	Any comment regarding this external-role-mapping entry.
ontap_role	ontap_role	ONTAP role to map with the external identity role. • Introduced in: 9.16
timestamp	string	Date and time indicating when this external-role-mapping entry was created.

Example response

```
{
  "comment": "string",
  "ontap_role": {
    "name": "admin"
  },
  "timestamp": "string"
}
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636243	Provided ONTAP role is not configured.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

_links

ontap_role

ONTAP role to map with the external identity role.

Name	Type	Description
name	string	Role name

security_external_role_mapping

Name	Type	Description
comment	string	Any comment regarding this external-role-mapping entry.
ontap_role	ontap_role	ONTAP role to map with the external identity role. • Introduced in: 9.16
timestamp	string	Date and time indicating when this external-role-mapping entry was created.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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.

Manage Google Cloud KMS

Manage Google Cloud KMS

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 protect 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": "{\"client_email\":
\"my@account.email.com\", \"private_key\": \"ValidPrivateKey\"}"}'

# 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": "{\"client_email\":
\"new@account.com\", \"private_key\": \"ValidPrivateKey\"}"}'
```

Updating the application credentials and applying a privileged account for impersonation.

The following example shows how to set a privileged account on an existing 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": "{\"client_email\":
\"unprivileged@account.com\", \"private_key\":
\"ValidPrivateKeyforUnprivilegedAccount\"}", "privileged_account":
"privileged@account.com"}'
```

Updating the authentication method to use GCE metadata server for retrieving short lived authentication tokens.

The following example shows how to change the authentication method on an existing 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 '{"authentication_method":
"sa_credentials_attachment"}'
```

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 a 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'
```

Retrieve a Google Cloud KMS configurations for all clusters and SVMs

GET `/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

Name	Type	In	Required	Description
oauth_host	string	query	False	Filter by oauth_host • Introduced in: 9.14

Name	Type	In	Required	Description
proxy_type	string	query	False	Filter by proxy_type
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
google_reachability.code	string	query	False	Filter by google_reachability.code
google_reachability.reachable	boolean	query	False	Filter by google_reachability.reachable
google_reachability.message	string	query	False	Filter by google_reachability.message
proxy_username	string	query	False	Filter by proxy_username
scope	string	query	False	Filter by scope
port	integer	query	False	Filter by port • Introduced in: 9.14
project_id	string	query	False	Filter by project_id
key_ring_name	string	query	False	Filter by key_ring_name
state.message	string	query	False	Filter by state.message
state.cluster_state	boolean	query	False	Filter by state.cluster_state
state.code	string	query	False	Filter by state.code
privileged_account	string	query	False	Filter by privileged_account • Introduced in: 9.14

Name	Type	In	Required	Description
uuid	string	query	False	Filter by uuid
key_ring_location	string	query	False	Filter by key_ring_location
key_name	string	query	False	Filter by key_name
caller_account	string	query	False	Filter by caller_account • Introduced in: 9.14
authentication_method	string	query	False	Filter by authentication_method • Introduced in: 9.17
gce_metadata_server	string	query	False	Filter by gce_metadata_server • Introduced in: 9.17
cloudkms_host	string	query	False	Filter by cloudkms_host • Introduced in: 9.14
proxy_host	string	query	False	Filter by proxy_host
oauth_url	string	query	False	Filter by oauth_url • Introduced in: 9.14
ekmip_reachability.reachable	boolean	query	False	Filter by ekmip_reachability.reachable
ekmip_reachability.code	string	query	False	Filter by ekmip_reachability.code

Name	Type	In	Required	Description
ekmip_reachability.node.uuid	string	query	False	Filter by ekmip_reachability.node.uuid
ekmip_reachability.node.name	string	query	False	Filter by ekmip_reachability.node.name
ekmip_reachability.message	string	query	False	Filter by ekmip_reachability.message
proxy_port	integer	query	False	Filter by proxy_port
verify_host	boolean	query	False	Filter by verify_host • Introduced in: 9.14
verify_ip	boolean	query	False	Filter by verify_ip • Introduced in: 9.14
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
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[gcp_kms]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "authentication_method": "application_credentials_key",
      "caller_account": "<a href="
mailto:myaccount@myproject.com">myaccount@myproject.com</a>",
      "cloudkms_host": "cloudkms.googleapis.com",
      "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"
          }
        }
      ],
      "gce_metadata_server":
"http://169.254.169.254/computeMetadata/v1/instance/service-
accounts/default/token",
      "google_reachability": {
        "code": "346758",
        "message": "Google Cloud KMS is not reachable from all nodes -
<reason>."
```

```
      },
      "key_name": "cryptokey1",
      "key_ring_location": "global",
      "key_ring_name": "gcpapp1-keyring",
      "oauth_host": "oauth2.googleapis.com",
      "oauth_url": "https://oauth2.googleapis.com/token",
      "port": 443,
      "privileged_account": "<a
href="mailto:myserviceaccount@myproject.iam.gserviceaccount.com">myserv
iceaccount@myproject.iam.gserviceaccount.com</a>",
      "project_id": "gcpapp1",
      "proxy_host": "proxy.eng.com",
      "proxy_port": 1234,
      "proxy_type": "http",
      "proxy_username": "proxyuser",
      "scope": "string",
      "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.

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

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

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 computational 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.

Name	Type	Description
code	string	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	Error message set when cluster-wide EKMIP server availability from the given SVM and node is false.
node	node	

Name	Type	Description
reachable	boolean	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

Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
code	string	Code corresponding to the error message. Returns a 0 if Google Cloud KMS is reachable from all nodes in the cluster.
message	string	Set to the error message when 'reachable' is false.
reachable	boolean	Set to true if the Google Cloud KMS is reachable from all nodes of the cluster.

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 computational 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.

Name	Type	Description
cluster_state	boolean	Set to true when Google Cloud KMS key protection is available on all nodes of the cluster.
code	string	Error code corresponding to the status message. Returns 0 if Google Cloud KMS key protection is available in all nodes of the cluster.

Name	Type	Description
message	string	Error message set when top-level internal key protection key (KEK) availability on cluster is false.

svm

SVM, applies only to SVM-scoped objects.

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

gcp_kms

Name	Type	Description
_links	_links	
authentication_method	string	Google Cloud KMS authentication method.
caller_account	string	Google Cloud KMS caller account email
cloudkms_host	string	Google Cloud KMS host subdomain.
ekmip_reachability	array[ekmip_reachability]	
gce_metadata_server	string	A custom metadata server URL used for retrieving short lived authentication tokens if the default service account is not used. This is only applicable when the `authentication_method` is set to `sa_credentials_attachment`.

Name	Type	Description
google_reachability	google_reachability	Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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	Key Identifier of Google Cloud KMS key encryption key.
key_ring_location	string	Google Cloud KMS key ring location.
key_ring_name	string	Google Cloud KMS key ring name of the deployed Google Cloud application.
oauth_host	string	Open authorization server host name.
oauth_url	string	Open authorization URL for the access token.
port	integer	Authorization server and Google Cloud KMS port number.
privileged_account	string	Google Cloud KMS account to impersonate.
project_id	string	Google Cloud project (application) ID of the deployed Google Cloud application that has appropriate access to the Google Cloud KMS.
proxy_host	string	Proxy host name.
proxy_port	integer	Proxy port number.
proxy_type	string	Type of proxy.

Name	Type	Description
proxy_username	string	Proxy username.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
state	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 computational 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	svm	SVM, applies only to SVM-scoped objects.
uuid	string	A unique identifier for the Google Cloud KMS.
verify_host	boolean	Verify the identity of the Google Cloud KMS host name.
verify_ip	boolean	Verify the identity of the Google Cloud KMS IP address.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a Google Cloud KMS configuration for an SVM

POST `/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` - The Google Cloud application's service account credentials required to access the specified KMS. This is a JSON file containing an email address and the private key of the service account holder. The field is required if the `authentication_method` is set to `application_credentials_key`.

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.
- `port` - Authorization server and Google Cloud KMS port number.
- `cloudkms_host` - Google Cloud KMS host subdomain.
- `oauth_host` - Open authorization server host name.

- `oauth_url` - Open authorization URL for the access token.
- `privileged_account` - Account used to impersonate Google Cloud KMS requests.
- `verify_ip` - Verify identity of Google Cloud KMS IP address.
- `verify_host` - Verify the identity of the Google Cloud KMS host name.
- `authentication_method` - The authentication method to use for retrieving short lived authentication tokens.
- `gce_metadata_server` - A custom metadata server URL used for retrieving short lived authentication tokens if the default service account is not used. This is only applicable when the `authentication_method` is set to `sa_credentials_attachment`.

Related ONTAP commands

- `security key-manager external gcp enable`

Parameters

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
_links	_links	

Name	Type	Description
application_credentials	string	The Google Cloud application's service account credentials required to access the specified KMS. The client_email and private_key fields of the service account holder are required. The credentials are required if the `authentication_method` is set to `application_credentials_key`.
authentication_method	string	Google Cloud KMS authentication method.
caller_account	string	Google Cloud KMS caller account email
cloudkms_host	string	Google Cloud KMS host subdomain.
ekmip_reachability	array[ekmip_reachability]	
gce_metadata_server	string	A custom metadata server URL used for retrieving short lived authentication tokens if the default service account is not used. This is only applicable when the `authentication_method` is set to `sa_credentials_attachment`.
google_reachability	google_reachability	Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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	Key Identifier of Google Cloud KMS key encryption key.

Name	Type	Description
key_ring_location	string	Google Cloud KMS key ring location.
key_ring_name	string	Google Cloud KMS key ring name of the deployed Google Cloud application.
oauth_host	string	Open authorization server host name.
oauth_url	string	Open authorization URL for the access token.
port	integer	Authorization server and Google Cloud KMS port number.
privileged_account	string	Google Cloud KMS account to impersonate.
project_id	string	Google Cloud project (application) ID of the deployed Google Cloud application that has appropriate access to the Google Cloud KMS.
proxy_host	string	Proxy host name.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port number.
proxy_type	string	Type of proxy.
proxy_username	string	Proxy username.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

Name	Type	Description
state	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 computational 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	svm	SVM, applies only to SVM-scoped objects.
uuid	string	A unique identifier for the Google Cloud KMS.
verify_host	boolean	Verify the identity of the Google Cloud KMS host name.
verify_ip	boolean	Verify the identity of the Google Cloud KMS IP address.

Example request


```
{
  "application_credentials": "{\"private_key\":\"ValidPrivateKey\",
\"client_email\":\"<a href="
mailto:my@account.email.com">my@account.email.com</a>\"}",
  "authentication_method": "application_credentials_key",
  "caller_account": "<a href="
mailto:myaccount@myproject.com">myaccount@myproject.com</a>",
  "cloudkms_host": "cloudkms.googleapis.com",
  "ekmip_reachability": [
    {
      "code": "346758",
      "message": "embedded KMIP server status unavailable on node.",
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ],
  "gce_metadata_server":
"http://169.254.169.254/computeMetadata/v1/instance/service-
accounts/default/token",
  "google_reachability": {
    "code": "346758",
    "message": "Google Cloud KMS is not reachable from all nodes -
<reason>."
  },
  "key_name": "cryptokey1",
  "key_ring_location": "global",
  "key_ring_name": "gcpapp1-keyring",
  "oauth_host": "oauth2.googleapis.com",
  "oauth_url": "https://oauth2.googleapis.com/token",
  "port": 443,
  "privileged_account": "<a
href="mailto:myserviceaccount@myproject.iam.gserviceaccount.com">myserv
iceaccount@myproject.iam.gserviceaccount.com</a>",
  "project_id": "gcpapp1",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "string",
  "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": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
```


Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "uuid": "string"
  }
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

```
Status: 201, Created
```

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/gcp-kms\" to view all of the configured key managers.</svm-name>
65537740	The privileged account must be an email address or an empty string.
65537749	The application credentials field must be in valid JSON format.
65539704	The key manager cannot be configured because the SVM has NAE volumes.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

node

Name	Type	Description
name	string	
uuid	string	

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 computational 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.

Name	Type	Description
code	string	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	Error message set when cluster-wide EKMIP server availability from the given SVM and node is false.
node	node	
reachable	boolean	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

Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
code	string	Code corresponding to the error message. Returns a 0 if Google Cloud KMS is reachable from all nodes in the cluster.
message	string	Set to the error message when 'reachable' is false.
reachable	boolean	Set to true if the Google Cloud KMS is reachable from all nodes of the cluster.

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 computational 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.

Name	Type	Description
cluster_state	boolean	Set to true when Google Cloud KMS key protection is available on all nodes of the cluster.
code	string	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	Error message set when top-level internal key protection key (KEK) availability on cluster is false.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

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

gcp_kms

Name	Type	Description
_links	_links	
application_credentials	string	The Google Cloud application's service account credentials required to access the specified KMS. The client_email and private_key fields of the service account holder are required. The credentials are required if the `authentication_method` is set to `application_credentials_key`.
authentication_method	string	Google Cloud KMS authentication method.
caller_account	string	Google Cloud KMS caller account email
cloudkms_host	string	Google Cloud KMS host subdomain.
ekmip_reachability	array[ekmip_reachability]	
gce_metadata_server	string	A custom metadata server URL used for retrieving short lived authentication tokens if the default service account is not used. This is only applicable when the `authentication_method` is set to `sa_credentials_attachment`.

Name	Type	Description
google_reachability	google_reachability	Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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	Key Identifier of Google Cloud KMS key encryption key.
key_ring_location	string	Google Cloud KMS key ring location.
key_ring_name	string	Google Cloud KMS key ring name of the deployed Google Cloud application.
oauth_host	string	Open authorization server host name.
oauth_url	string	Open authorization URL for the access token.
port	integer	Authorization server and Google Cloud KMS port number.
privileged_account	string	Google Cloud KMS account to impersonate.
project_id	string	Google Cloud project (application) ID of the deployed Google Cloud application that has appropriate access to the Google Cloud KMS.
proxy_host	string	Proxy host name.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port number.

Name	Type	Description
proxy_type	string	Type of proxy.
proxy_username	string	Proxy username.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
state	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 computational 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	svm	SVM, applies only to SVM-scoped objects.
uuid	string	A unique identifier for the Google Cloud KMS.
verify_host	boolean	Verify the identity of the Google Cloud KMS host name.
verify_ip	boolean	Verify the identity of the Google Cloud KMS IP address.

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Re-key the external key in the key hierarchy for an SVM

POST `/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

Name	Type	In	Required	Description
gcp_kms.uuid	string	path	True	UUID of the existing Google Cloud KMS configuration.

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
key_name	string	Key identifier of the Google Cloud KMS key encryption key.

Example request

```
{
  "key_name": "cryptokey1"
}
```

Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Response

```
Status: 201, Created
```

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.

Error Code	Description
65537556	ONTAP is not able to successfully encrypt or decrypt because the configured external key manager for this SVM is in a blocked state. Possible reasons for a blocked state include the top-level external key protection key not found, disabled or having insufficient privileges.
65537610	Rekey cannot be performed on the SVM while the enabled keystore configuration is being switched. If a previous attempt to switch the keystore configuration failed, or was interrupted, the system will continue to prevent rekeying for the SVM. Use the REST API PATCH method "/api/security/key-stores/{uuid}" to re-run and complete the 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.
65539436	Rekey cannot be performed on the SVM while the enabled keystore configuration is being initialized. Wait until the keystore is in the active state, and rerun the rekey operation.
65539437	Rekey cannot be performed on the SVM while the enabled keystore configuration is being disabled.

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

Definitions

See Definitions

gcp_kms_key

Name	Type	Description
key_name	string	Key identifier of the Google Cloud KMS key encryption key.

href

Name	Type	Description
href	string	

_links

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete a Google Cloud KMS configuration

DELETE `/security/gcp-kms/{uuid}`

Introduced In: 9.9

Deletes a Google Cloud KMS configuration.

Related ONTAP commands

- `security key-manager external gcp disable`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Google Cloud KMS UUID
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0

Response

```
Status: 200, Ok
```

Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
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.
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.

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

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the Google Cloud KMS configuration

GET `/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

Name	Type	In	Required	Description
uuid	string	path	True	Google Cloud KMS UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
authentication_method	string	Google Cloud KMS authentication method.
caller_account	string	Google Cloud KMS caller account email
cloudkms_host	string	Google Cloud KMS host subdomain.
ekmip_reachability	array[ekmip_reachability]	
gce_metadata_server	string	A custom metadata server URL used for retrieving short lived authentication tokens if the default service account is not used. This is only applicable when the `authentication_method` is set to `sa_credentials_attachment`.

Name	Type	Description
google_reachability	google_reachability	Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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	Key Identifier of Google Cloud KMS key encryption key.
key_ring_location	string	Google Cloud KMS key ring location.
key_ring_name	string	Google Cloud KMS key ring name of the deployed Google Cloud application.
oauth_host	string	Open authorization server host name.
oauth_url	string	Open authorization URL for the access token.
port	integer	Authorization server and Google Cloud KMS port number.
privileged_account	string	Google Cloud KMS account to impersonate.
project_id	string	Google Cloud project (application) ID of the deployed Google Cloud application that has appropriate access to the Google Cloud KMS.
proxy_host	string	Proxy host name.
proxy_port	integer	Proxy port number.
proxy_type	string	Type of proxy.
proxy_username	string	Proxy username.

Name	Type	Description
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
state	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 computational 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	svm	SVM, applies only to SVM-scoped objects.
uuid	string	A unique identifier for the Google Cloud KMS.
verify_host	boolean	Verify the identity of the Google Cloud KMS host name.
verify_ip	boolean	Verify the identity of the Google Cloud KMS IP address.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "authentication_method": "application_credentials_key",
  "caller_account": "<a href="
mailto:myaccount@myproject.com">myaccount@myproject.com</a>",
  "cloudkms_host": "cloudkms.googleapis.com",
  "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"
      }
    }
  ],
  "gce_metadata_server":
"http://169.254.169.254/computeMetadata/v1/instance/service-
accounts/default/token",
  "google_reachability": {
    "code": "346758",
    "message": "Google Cloud KMS is not reachable from all nodes -
<reason>."
  },
  "key_name": "cryptokey1",
  "key_ring_location": "global",
  "key_ring_name": "gcpapp1-keyring",
  "oauth_host": "oauth2.googleapis.com",
  "oauth_url": "https://oauth2.googleapis.com/token",
  "port": 443,
  "privileged_account": "<a
href="mailto:myserviceaccount@myproject.iam.gserviceaccount.com">myserv
iceaccount@myproject.iam.gserviceaccount.com</a>",
  "project_id": "gcpapp1",
  "proxy_host": "proxy.eng.com",
```

```
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "string",
  "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.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

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 computational 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.

Name	Type	Description
code	string	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	Error message set when cluster-wide EKMIP server availability from the given SVM and node is false.
node	node	
reachable	boolean	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

Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
code	string	Code corresponding to the error message. Returns a 0 if Google Cloud KMS is reachable from all nodes in the cluster.
message	string	Set to the error message when 'reachable' is false.
reachable	boolean	Set to true if the Google Cloud KMS is reachable from all nodes of the cluster.

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 computational 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.

Name	Type	Description
cluster_state	boolean	Set to true when Google Cloud KMS key protection is available on all nodes of the cluster.
code	string	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	Error message set when top-level internal key protection key (KEK) availability on cluster is false.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the Google Cloud KMS configuration

PATCH `/security/gcp-kms/{uuid}`

Introduced In: 9.9

Updates the Google Cloud KMS configuration.

Optional properties

- `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.

- `port` - Authorization server and Google Cloud KMS port number.
- `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.
- `cloudkms_host` - Google Cloud KMS host subdomain.
- `oauth_host` - Open authorization server host name.
- `oauth_url` - Open authorization URL for the access token.
- `verify_host` - Verify the identity of the Google Cloud KMS host name.
- `verify_ip ` - Verify identity of Google Cloud KMS IP address.
- `privileged_account` - Account used to impersonate Google Cloud KMS requests.
- `authentication_method` - The authentication method to use for retrieving short lived authentication tokens.
- `gce_metadata_server` - A custom metadata server URL used for retrieving short lived authentication tokens if the default service account is not used. This is only applicable when the `authentication_method` is set to `sa_credentials_attachment`.

Related ONTAP commands

- `security key-manager external gcp update-credentials`
- `security key-manager external gcp update-config`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Google Cloud KMS UUID

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
_links	_links	
application_credentials	string	The Google Cloud application's service account credentials required to access the specified KMS. The client_email and private_key fields of the service account holder are required. The credentials are required if the `authentication_method` is set to `application_credentials_key`.

Name	Type	Description
authentication_method	string	Google Cloud KMS authentication method.
caller_account	string	Google Cloud KMS caller account email
cloudkms_host	string	Google Cloud KMS host subdomain.
ekmip_reachability	array[ekmip_reachability]	
gce_metadata_server	string	A custom metadata server URL used for retrieving short lived authentication tokens if the default service account is not used. This is only applicable when the `authentication_method` is set to `sa_credentials_attachment`.
google_reachability	google_reachability	Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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.
oauth_host	string	Open authorization server host name.
oauth_url	string	Open authorization URL for the access token.
port	integer	Authorization server and Google Cloud KMS port number.
privileged_account	string	Google Cloud KMS account to impersonate.
proxy_host	string	Proxy host name.

Name	Type	Description
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port number.
proxy_type	string	Type of proxy.
proxy_username	string	Proxy username.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
state	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 computational 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.
uuid	string	A unique identifier for the Google Cloud KMS.
verify_host	boolean	Verify the identity of the Google Cloud KMS host name.
verify_ip	boolean	Verify the identity of the Google Cloud KMS IP address.

Example request


```
{
  "application_credentials": "{\"private_key\":\"ValidPrivateKey\",
\"client_email\":\"<a href="
mailto:my@account.email.com">my@account.email.com</a>\"}",
  "authentication_method": "application_credentials_key",
  "caller_account": "<a href="
mailto:myaccount@myproject.com">myaccount@myproject.com</a>",
  "cloudkms_host": "cloudkms.googleapis.com",
  "ekmip_reachability": [
    {
      "code": "346758",
      "message": "embedded KMIP server status unavailable on node.",
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ],
  "gce_metadata_server":
"http://169.254.169.254/computeMetadata/v1/instance/service-
accounts/default/token",
  "google_reachability": {
    "code": "346758",
    "message": "Google Cloud KMS is not reachable from all nodes -
<reason>."
  },
  "oauth_host": "oauth2.googleapis.com",
  "oauth_url": "https://oauth2.googleapis.com/token",
  "port": 443,
  "privileged_account": "<a
href="mailto:myserviceaccount@myproject.iam.gserviceaccount.com">myserv
iceaccount@myproject.iam.gserviceaccount.com</a>",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "scope": "string",
  "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."
```

```
  },
  "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.
65537605	Failed to establish connectivity with the cloud key management service.
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".

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

node

Name	Type	Description
name	string	
uuid	string	

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 computational 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.

Name	Type	Description
code	string	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	Error message set when cluster-wide EKMIP server availability from the given SVM and node is false.
node	node	
reachable	boolean	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

Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
code	string	Code corresponding to the error message. Returns a 0 if Google Cloud KMS is reachable from all nodes in the cluster.
message	string	Set to the error message when 'reachable' is false.
reachable	boolean	Set to true if the Google Cloud KMS is reachable from all nodes of the cluster.

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 computational 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.

Name	Type	Description
cluster_state	boolean	Set to true when Google Cloud KMS key protection is available on all nodes of the cluster.
code	string	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	Error message set when top-level internal key protection key (KEK) availability on cluster is false.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

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

gcp_kms

Name	Type	Description
_links	_links	
application_credentials	string	The Google Cloud application's service account credentials required to access the specified KMS. The client_email and private_key fields of the service account holder are required. The credentials are required if the `authentication_method` is set to `application_credentials_key`.
authentication_method	string	Google Cloud KMS authentication method.
caller_account	string	Google Cloud KMS caller account email
cloudkms_host	string	Google Cloud KMS host subdomain.
ekmip_reachability	array[ekmip_reachability]	
gce_metadata_server	string	A custom metadata server URL used for retrieving short lived authentication tokens if the default service account is not used. This is only applicable when the `authentication_method` is set to `sa_credentials_attachment`.

Name	Type	Description
google_reachability	google_reachability	Indicates whether or not the Google Cloud KMS is reachable from all nodes in the cluster. This is an advanced property; there is an added computational 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.
oauth_host	string	Open authorization server host name.
oauth_url	string	Open authorization URL for the access token.
port	integer	Authorization server and Google Cloud KMS port number.
privileged_account	string	Google Cloud KMS account to impersonate.
proxy_host	string	Proxy host name.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port number.
proxy_type	string	Type of proxy.
proxy_username	string	Proxy username.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

Name	Type	Description
state	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 computational 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.
uuid	string	A unique identifier for the Google Cloud KMS.
verify_host	boolean	Verify the identity of the Google Cloud KMS host name.
verify_ip	boolean	Verify the identity of the Google Cloud KMS IP address.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message

Name	Type	Description
target	string	The target parameter that caused the error.

Re-key the internal key in the key hierarchy for an SVM

POST `/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

Name	Type	In	Required	Description
uuid	string	path	True	UUID of the existing Google Cloud KMS configuration.

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "uuid": "string"
  }
}
```


Response

```
Status: 201, Created
```

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.
65537556	ONTAP is not able to successfully encrypt or decrypt because the configured external key manager for this SVM is in a blocked state. Possible reasons for a blocked state include the top-level external key protection key not found, disabled or having insufficient privileges.
65537559	There are no existing internal keys for the SVM. A rekey operation is allowed for an SVM with one or more encryption keys.
65537610	Rekey cannot be performed on the SVM while the enabled keystore configuration is being switched. If a previous attempt to switch the keystore configuration failed, or was interrupted, the system will continue to prevent rekeying for the SVM. Use the REST API PATCH method "/api/security/key-stores/{uuid}" to re-run and complete the operation.

Error Code	Description
65537721	Google Cloud KMS is not configured for the given SVM.
65539436	Rekey cannot be performed on the SVM while the enabled keystore configuration is being initialized. Wait until the keystore is in the active state, and rerun the rekey operation.
65539437	Rekey cannot be performed on the SVM while the enabled keystore configuration is being disabled.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Restore keys for an SVM from a Google Cloud KMS

POST `/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

Name	Type	In	Required	Description
uuid	string	path	True	UUID of the existing Google Cloud KMS configuration.
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "uuid": "string"
  }
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
65537544	Missing wrapped top-level internal key protection key (KEK) from internal database.
65537721	The Google Cloud Key Management Service is not configured for the given SVM.
65537722	Failed to restore keys on the following nodes.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage group-to-role mapping entries

Manage group-to-role mapping entries

Overview

This API is used to manage and map groups to ONTAP roles. The POST request creates a group to role

mapping. Various responses are shown in the examples below.

Examples

Creating a group to role mapping entry

The following output shows how to create a group to role mapping entry.

```
# The API:
/api/security/group/role-mappings

# The call:
curl -X POST "https://<mgmt-ip>/api/security/group/role-mappings" -d '{
"group_id": 1, "ontap_role": { "name": "admin" }, "comment": "Group1 admin
role"}'
```

Retrieving all group to role mapping entries

The following output shows all group to role mapping entries.

```
# The API:
/api/security/group/role-mappings

# The call:
curl -X GET "https://<mgmt-ip>/api/security/group/role-mappings"

# The response:
{
 "records": [
 {
   "group_id": 1,
   "ontap_role": {
     "name": "admin"
   }
 }
 ],
 "num_records": 1
}
```

Retrieve all group-to-role mapping entries

GET `/security/group/role-mappings`

Introduced In: 9.16

Retrieves all the group to role mapping entries.

Related ONTAP commands

- `security login group role-mapping show`

Parameters

Name	Type	In	Required	Description
scope	string	query	False	Filter by scope
comment	string	query	False	Filter by comment
ontap_role.name	string	query	False	Filter by ontap_role.name
group_id	integer	query	False	Filter by group_id • Max value: 4294967295 • Min value: 1
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 15
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[group_role_mappings]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "comment": "string",
      "group_id": 1,
      "ontap_role": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "admin"
      },
      "scope": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

ontap_role

Role name.

Name	Type	Description
_links	_links	
name	string	Role name

group_role_mappings

Name	Type	Description
_links	_links	
comment	string	Any comment regarding this group entry.
group_id	integer	Group ID.
ontap_role	ontap_role	Role name.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a group-to-role mapping entry

POST `/security/group/role-mappings`

Introduced In: 9.16

Creates a group to role mapping entry.

Required properties

- `group_id`
- `ontap_role`

Optional properties

- `comment`

Related ONTAP commands

- `security login group role-mapping create`

Parameters

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

Request Body

Name	Type	Description
comment	string	Any comment regarding this group entry.
group_id	integer	Group ID.
ontap_role	ontap_role	Role name.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example request

```
{
  "comment": "string",
  "group_id": 1,
  "ontap_role": {
    "name": "admin"
  },
  "scope": "string"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records.
records	array[group_role_mappings]	

Example response


```
{
  "records": [
    {
      "comment": "string",
      "group_id": 1,
      "ontap_role": {
        "name": "admin"
      },
      "scope": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636242	The configured group ID does not exist in the group configuration.
5636243	The configured role name does not exist in the SVM where the group ID is configured.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ontap_role

Role name.

Name	Type	Description
name	string	Role name

group_role_mappings

Name	Type	Description
comment	string	Any comment regarding this group entry.
group_id	integer	Group ID.
ontap_role	ontap_role	Role name.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Delete a group-to-role mapping entry

DELETE `/security/group/role-mappings/{group_id}/{ontap_role.name}`

Introduced In: 9.16

Deletes a group to role mapping entry.

Related ONTAP commands

- `security login group role-mapping delete`

Parameters

Name	Type	In	Required	Description
group_id	integer	path	True	Group ID. • format: int64 • Max value: 4294967295 • Min value: 1
ontap_role.name	string	path	True	Role name.

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a group-to-role mapping entry

GET `/security/group/role-mappings/{group_id}/{ontap_role.name}`

Introduced In: 9.16

Retrieves a group to role mapping entry.

Related ONTAP commands

- `security login group role-mapping show`

Parameters

Name	Type	In	Required	Description
group_id	integer	path	True	Group ID. • format: int64 • Max value: 4294967295 • Min value: 1
ontap_role.name	string	path	True	Role name.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
comment	string	Any comment regarding this group entry.
group_id	integer	Group ID.
ontap_role	ontap_role	Role name.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "comment": "string",
  "group_id": 1,
  "ontap_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

ontap_role

Role name.

Name	Type	Description
_links	_links	
name	string	Role name

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message

Name	Type	Description
target	string	The target parameter that caused the error.

Update a configured group role-mapping entry

PATCH `/security/group/role-mappings/{group_id}/{ontap_role.name}`

Introduced In: 9.16

Updates a configured group role-mapping.

Related ONTAP commands

- `security login group role-mapping modify`

Parameters

Name	Type	In	Required	Description
group_id	integer	path	True	Group ID. • format: int64 • Max value: 4294967295 • Min value: 1
ontap_role.name	string	path	True	Role name.

Request Body

Name	Type	Description
comment	string	Any comment regarding this group entry.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example request

```
{
  "comment": "string",
  "scope": "string"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ontap_role

Role name.

Name	Type	Description
name	string	Role name

group_role_mappings

Name	Type	Description
comment	string	Any comment regarding this group entry.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message

Name	Type	Description
target	string	The target parameter that caused the error.

Manage group configurations

Manage group configurations

Overview

This API is used to manage group configurations in ONTAP. The POST request creates a group configuration. Various responses are shown in the examples below.

Examples

Creating a group configuration

The following output shows how to create a group configuration.

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/groups"  -d '{ "name":
"AzureGroup1", "owner": { "name": "C1_sti213-vsim-sr023a_1718680001",
"uuid": "116127b1-2d21-11ef-a5e1-005056ae1bc2" }, "type": "entra", "uuid":
"3fa85f64-5717-4562-b3fc-2c963f66afa6", "comment": "Azure Group"}'
```

Retrieving all group configurations

The following output shows all group configurations.

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

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

# The response:
{
"records": [
  {
    "owner": {
      "uuid": "116127b1-2d21-11ef-a5e1-005056ae1bc2",
      "name": "C1_sti213-vsim-sr023a_1718680001"
    },
    "name": "AzureGroup1",
    "type": "entra",
    "id": 1,
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
],
"num_records": 1
}
```

Retrieve all group entries

GET `/security/groups`

Introduced In: 9.16

Retrieves all group entries.

Related ONTAP commands

- `security login group show`

Parameters

Name	Type	In	Required	Description
type	string	query	False	Filter by type
scope	string	query	False	Filter by scope
create_time	string	query	False	Filter by create_time

Name	Type	In	Required	Description
name	string	query	False	Filter by name • maxLength: 64 • minLength: 1
uuid	string	query	False	Filter by uuid
id	integer	query	False	Filter by id
owner.name	string	query	False	Filter by owner.name
owner.uuid	string	query	False	Filter by owner.uuid
comment	string	query	False	Filter by comment
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0

Name	Type	In	Required	Description
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records.
records	array[security_group]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "comment": "Azure Group",
      "create_time": "string",
      "id": 0,
      "name": "AzureGroup1",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "scope": "string",
      "type": "entra",
      "uuid": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

owner

Group owner. Used to identify a cluster or an SVM.

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

security_group

Name	Type	Description
_links	self_link	
comment	string	Any comment regarding this group entry.

Name	Type	Description
create_time	string	Date and time indicating when this group entry was created.
id	integer	Group ID which is unique per group across the system. It is a read-only field and it automatically assigns the next available unique number.
name	string	Group name.
owner	owner	Group owner. Used to identify a cluster or an SVM.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
type	string	Group type.
uuid	string	Group UUID from external Active Directory.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a group entry

POST `/security/groups`

Introduced In: 9.16

Creates a group entry.

Required properties

- `name`

Optional properties

- `owner`
- `type`
- `uuid`
- `comment`

Related ONTAP commands

- `security login group create`

Parameters

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

Request Body

Name	Type	Description
comment	string	Any comment regarding this group entry.
create_time	string	Date and time indicating when this group entry was created.
id	integer	Group ID which is unique per group across the system. It is a read-only field and it automatically assigns the next available unique number.

Name	Type	Description
name	string	Group name.
owner	owner	Group owner. Used to identify a cluster or an SVM.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
type	string	Group type.
uuid	string	Group UUID from external Active Directory.

Example request

```
{
  "comment": "Azure Group",
  "create_time": "string",
  "id": 0,
  "name": "AzureGroup1",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "string",
  "type": "entra",
  "uuid": "string"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records.
records	array[security_group]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "comment": "Azure Group",
      "create_time": "string",
      "id": 0,
      "name": "AzureGroup1",
      "owner": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "scope": "string",
      "type": "entra",
      "uuid": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636231	Failed to create the group because the maximum number of allowed group IDs has been reached.
5636232	The group name does not satisfy the length requirement.
5636235	Duplicate UUID.
5636244	Failed to delete the group because it is part of the group role mapping configuration.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

_links

owner

Group owner. Used to identify a cluster or an SVM.

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

security_group

Name	Type	Description
comment	string	Any comment regarding this group entry.
create_time	string	Date and time indicating when this group entry was created.
id	integer	Group ID which is unique per group across the system. It is a read-only field and it automatically assigns the next available unique number.
name	string	Group name.
owner	owner	Group owner. Used to identify a cluster or an SVM.

Name	Type	Description
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
type	string	Group type.
uuid	string	Group UUID from external Active Directory.

collection_links

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete a group entry

DELETE `/security/groups/{owner.uuid}/{name}/{type}`

Introduced In: 9.16

Deletes a group entry.

Related ONTAP commands

- `security login group delete`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	
name	string	path	True	
type	string	path	True	

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636244	The group is part of the role mapping configuration. Delete the mapping first and then delete the group.

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

Name	Type	Description
error	returned_error	

Example error


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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a group entry

GET `/security/groups/{owner.uuid}/{name}/{type}`

Introduced In: 9.16

Retrieves a group entry.

Related ONTAP commands

- `security login group show`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Group owner. Used to identify a cluster or an SVM.
name	string	path	True	Group name.
type	string	path	True	Group type.

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	
comment	string	Any comment regarding this group entry.
create_time	string	Date and time indicating when this group entry was created.
id	integer	Group ID which is unique per group across the system. It is a read-only field and it automatically assigns the next available unique number.
name	string	Group name.
owner	owner	Group owner. Used to identify a cluster or an SVM.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
type	string	Group type.
uuid	string	Group UUID from external Active Directory.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "comment": "Azure Group",
  "create_time": "string",
  "id": 0,
  "name": "AzureGroup1",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "string",
  "type": "entra",
  "uuid": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

owner

Group owner. Used to identify a cluster or an SVM.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Update configured group information

PATCH `/security/groups/{owner.uuid}/{name}/{type}`

Introduced In: 9.16

Updates configured group information.

Related ONTAP commands

- `security login group modify`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Group owner. Used to identify a cluster or an SVM.
name	string	path	True	Group name.
type	string	path	True	Group type.

Request Body

Name	Type	Description
comment	string	Any comment regarding this group entry.
create_time	string	Date and time indicating when this group entry was created.
id	integer	Group ID which is unique per group across the system. It is a read-only field and it automatically assigns the next available unique number.

Name	Type	Description
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
uuid	string	Group UUID from external Active Directory.

Example request

```
{
  "comment": "Azure Group",
  "create_time": "string",
  "id": 0,
  "scope": "string",
  "uuid": "string"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636235	Duplicate UUID.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

_links

owner

Group owner. Used to identify a cluster or an SVM.

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

security_group

Name	Type	Description
comment	string	Any comment regarding this group entry.
create_time	string	Date and time indicating when this group entry was created.
id	integer	Group ID which is unique per group across the system. It is a read-only field and it automatically assigns the next available unique number.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
uuid	string	Group UUID from external Active Directory.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View and update IPsec configuration

View and update IPsec configuration

Overview

The following operations are supported:

- GET to retrieve the IPsec status: GET security/ipsec
- Patch to update IPsec status: PATCH security/ipsec

Retrieve an IPsec configuration

GET `/security/ipsec`

Introduced In: 9.8

Retrieves IPsec configuration via REST APIs.

Related ONTAP commands

- 'security ipsec config show'

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	
enabled	boolean	Indicates whether or not IPsec is enabled.
offload_enabled	boolean	Indicates whether or not IPsec hardware offload is enabled.
replay_window	integer	Replay window size in packets, where 0 indicates that the relay window is disabled.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "replay_window": 0
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update an IPsec configuration

PATCH `/security/ipsec`

Introduced In: 9.8

Updates IPsec configuration via REST APIs.

Optional properties

- 'enabled' - Enable IPsec.
- 'replay_window' - Replay window size in packets.
- 'offload_enabled' - Enable IPsec hardware offload.

Related ONTAP commands

- 'security ipsec config modify'

Request Body

Name	Type	Description
enabled	boolean	Indicates whether or not IPsec is enabled.
offload_enabled	boolean	Indicates whether or not IPsec hardware offload is enabled.
replay_window	integer	Replay window size in packets, where 0 indicates that the relay window is disabled.

Example request

```
{
  "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.
66256913	Offload setting changes are not allowed when IPsec is enabled.
66256915	Anti-replay protection and IPsec offload cannot be operational at the same time.
66257007	Failed to update replay window size.

Error Code	Description
66257199	IPsec is not supported in the current cluster version.
66257496	IPsec must be enabled to support BGP peer groups with MD5. Disable MD5 first in the BGP peer group.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

ipsec

Manages IPsec configuration via REST APIs.

Name	Type	Description
enabled	boolean	Indicates whether or not IPsec is enabled.
offload_enabled	boolean	Indicates whether or not IPsec hardware offload is enabled.
replay_window	integer	Replay window size in packets, where 0 indicates that the relay window is disabled.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage IPsec security certificates

Manage IPsec security certificates

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}

Retrieve IPsec CA certificates configured for the cluster and all SVMs

GET `/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

Name	Type	In	Required	Description
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
scope	string	query	False	Filter by scope
certificate.uuid	string	query	False	Filter by certificate.uuid
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[ipsec_ca_certificate]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "certificate": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "scope": "string",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

certificate

IPsec CA certificate UUID

Name	Type	Description
_links	_links	
uuid	string	Certificate UUID

svm

SVM, applies only to SVM-scoped objects.

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

ipsec_ca_certificate

Name	Type	Description
certificate	certificate	IPsec CA certificate UUID
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Add a CA certificate to IPsec

POST `/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

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

Request Body

Name	Type	Description
certificate	certificate	IPsec CA certificate UUID
svm	svm	SVM, applies only to SVM-scoped objects.

Example request

```
{
  "certificate": {
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[ipsec_ca_certificate]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "certificate": {
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
66257304	CA certificate is not installed.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

certificate

IPsec CA certificate UUID

Name	Type	Description
uuid	string	Certificate UUID

svm

SVM, applies only to SVM-scoped objects.

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

ipsec_ca_certificate

Name	Type	Description
certificate	certificate	IPsec CA certificate UUID
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete a CA certificate with the specified UUID from IPsec

DELETE `/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

Name	Type	In	Required	Description
certificate.uuid	string	path	True	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.

Error Code	Description
66257303	The CA certificate cannot be removed from IPsec because it is not installed.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a CA certificate configured for IPpsec

GET `/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

Name	Type	In	Required	Description
certificate.uuid	string	path	True	UUID of the IPsec CA certificate.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
certificate	certificate	IPsec CA certificate UUID
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	svm	SVM, applies only to SVM-scoped objects.

Example response


```
{
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "scope": "string",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

certificate

IPsec CA certificate UUID

Name	Type	Description
_links	_links	
uuid	string	Certificate UUID

svm

SVM, applies only to SVM-scoped objects.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage IPsec policies

Manage IPsec policies

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

Retrieve IPsec policies

GET `/security/ipsec/policies`

Introduced In: 9.8

Retrieves the collection of IPsec policies.

Related ONTAP commands

- `security ipsec policy show`

Parameters

Name	Type	In	Required	Description
remote_endpoint.family	string	query	False	Filter by remote_endpoint.family

Name	Type	In	Required	Description
remote_endpoint.port	string	query	False	Filter by remote_endpoint.port
remote_endpoint.netmask	string	query	False	Filter by remote_endpoint.netmask
remote_endpoint.address	string	query	False	Filter by remote_endpoint.address
enabled	boolean	query	False	Filter by enabled
local_identity	string	query	False	Filter by local_identity
ipspace.name	string	query	False	Filter by ipspace.name
ipspace.uuid	string	query	False	Filter by ipspace.uuid
name	string	query	False	Filter by name • maxLength: 64 • minLength: 1
action	string	query	False	Filter by action • Introduced in: 9.15
protocol	string	query	False	Filter by protocol
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
certificate.name	string	query	False	Filter by certificate.name • Introduced in: 9.10

Name	Type	In	Required	Description
certificate.uuid	string	query	False	Filter by certificate.uuid • Introduced in: 9.10
authentication_method	string	query	False	Filter by authentication_method • Introduced in: 9.10
uuid	string	query	False	Filter by uuid
remote_identity	string	query	False	Filter by remote_identity
ppk.identity	string	query	False	Filter by ppk.identity • Introduced in: 9.17 • maxLength: 64 • minLength: 6
local_endpoint.family	string	query	False	Filter by local_endpoint.family
local_endpoint.port	string	query	False	Filter by local_endpoint.port
local_endpoint.netmask	string	query	False	Filter by local_endpoint.netmask
local_endpoint.address	string	query	False	Filter by local_endpoint.address
scope	string	query	False	Filter by scope
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_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
error	error	
num_records	integer	Number of records
records	array[records]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist"
  },
  "num_records": 1,
  "records": [
    {
      "action": "string",
      "authentication_method": "string",
      "certificate": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "string",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "ipspace": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "Default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "local_endpoint": {
        "address": "10.10.10.7",
```

```
        "family": "string",
        "netmask": "24",
        "port": "23"
      },
      "local_identity": "string",
      "name": "string",
      "ppk": {
        "identity": "string"
      },
      "protocol": "17",
      "remote_endpoint": {
        "address": "10.10.10.7",
        "family": "string",
        "netmask": "24",
        "port": "23"
      },
      "remote_identity": "string",
      "scope": "string",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

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

_links

Name	Type	Description
self	href	

certificate

Certificate for the IPsec policy.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

ipspace

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

Name	Type	Description
_links	_links	
name	string	IPspace name
uuid	string	IPspace UUID

local_endpoint

Local endpoint for the IPsec policy.

Name	Type	Description
address	string	IPv4 or IPv6 address
family	string	IPv4 or IPv6
netmask	string	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 the netmask length.
port	string	Application port to be covered by the IPsec policy

ppk

Post-quantum pre-shared key information.

Name	Type	Description
identity	string	Post-quantum pre-shared key identity.

remote_endpoint

Remote endpoint for the IPsec policy.

Name	Type	Description
address	string	IPv4 or IPv6 address
family	string	IPv4 or IPv6

Name	Type	Description
netmask	string	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 the netmask length.
port	string	Application port to be covered by the IPsec policy

svm

SVM, applies only to SVM-scoped objects.

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

records

IPsec policy object.

Name	Type	Description
action	string	Action for the IPsec policy.
authentication_method	string	Authentication method for the IPsec policy.
certificate	certificate	Certificate for the IPsec policy.
enabled	boolean	Indicates whether or not the policy is enabled.
ipspace	ipspace	Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

Name	Type	Description
local_endpoint	local_endpoint	Local endpoint for the IPsec policy.
local_identity	string	Local Identity
name	string	IPsec policy name.
ppk	ppk	Post-quantum pre-shared key information.
protocol	string	Lower layer protocol to be covered by the IPsec policy.
remote_endpoint	remote_endpoint	Remote endpoint for the IPsec policy.
remote_identity	string	Remote Identity
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	Unique identifier of the IPsec policy.

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create an IPsec policy

POST `/security/ipsec/policies`

Introduced In: 9.8

Creates an IPsec policy.

Related ONTAP commands

- `security ipsec policy create`

Parameters

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

Request Body

Name	Type	Description
action	string	Action for the IPsec policy.
authentication_method	string	Authentication method for the IPsec policy.
certificate	certificate	Certificate for the IPsec policy.
enabled	boolean	Indicates whether or not the policy is enabled.
ipspace	ipspace	Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.
local_endpoint	local_endpoint	Local endpoint for the IPsec policy.
local_identity	string	Local Identity
name	string	IPsec policy name.
ppk	ppk	Post-quantum pre-shared key information.
protocol	string	Lower layer protocol to be covered by the IPsec policy.

Name	Type	Description
remote_endpoint	remote_endpoint	Remote endpoint for the IPsec policy.
remote_identity	string	Remote Identity
secret_key	string	Pre-shared key for IKE negotiation.
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	Unique identifier of the IPsec policy.

Example request


```
{
  "action": "string",
  "authentication_method": "string",
  "certificate": {
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "ipspace": {
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "netmask": "24",
    "port": "23"
  },
  "local_identity": "string",
  "name": "string",
  "ppk": {
    "identity": "string",
    "shared_key": "string"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "netmask": "24",
    "port": "23"
  },
  "remote_identity": "string",
  "secret_key": "string",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
```


Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[records]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "action": "string",
      "authentication_method": "string",
      "certificate": {
        "name": "string",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "ipspace": {
        "name": "Default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "local_endpoint": {
        "address": "10.10.10.7",
        "netmask": "24",
        "port": "23"
      },
      "local_identity": "string",
      "name": "string",
      "ppk": {
        "identity": "string",
        "shared_key": "string"
      },
      "protocol": "17",
      "remote_endpoint": {
        "address": "10.10.10.7",
        "netmask": "24",
        "port": "23"
      },
      "remote_identity": "string",
      "secret_key": "string",
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ]
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

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.
66257102	Internet Key Exchange version 1 (IKEv1) is not supported.
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.
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 been reached for the specified SVM.
66257125	The local_endpoint.address must be specified with local_endpoint.netmask.

Error Code	Description
66257126	The remote_endpoint.address must be specified with remote_endpoint.netmask.
66257127	The local subnet must be configured as a non-zero subnet.
66257128	Invalid ANY wildcard subnet.
66257129	A specific local or remote port number is required when the remote subnet is configured as an ANY wildcard subnet.
66257130	The maximum limit of IPsec policies has been reached for the cluster.
66257131	ESP in UDPv6 Encapsulation is not supported.
66257132	Invalid value for port field. Value should be in range <0-65535>.
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.
66257135	The specified certificate is not found on the SVM.
66257136	A certificate is not needed for the PSK authentication method.
66257137	A pre-shared key is not needed for the PKI authentication method.
66257138	Remote identity is required when using certificate verification.
66257139	Certificate with the specified UUID was not found.
66257140	Only certificates with a client or server type are supported.
66257142	Failed to create IPsec policy because the specified SVM is being migrated.
66257143	Invalid IPsec policy provided. The subnet must be non-empty.
66257144	The IPsec policy actions ESP TRANSPORT and ESP UDP each provide packet protection and requires a secret key or certificate for authentication.
66257148	The policy name does not meet required ASCII-range characters length.
66257153	The policy requires a post-quantum pre-shared key because ppk-identity is specified for this policy.

Error Code	Description
66257154	The policy requires a post-quantum pre-shared identity because ppk-shared-key is specified for this policy.
66257199	Not all of the nodes in the cluster are running a version that supports the IPsec feature.
66257200	The shared key does not meet required ASCII-range characters length.
66257201	Support for the feature available with effective cluster version or later.
66257202	The specified SVM name is invalid.
66257203	The specified SVM UUID is invalid.
66257204	The specified IPspace UUID and IPspace name refer to different IPspaces.
66257205	The specified SVM must exist in the specified IPspace.
66257305	The certificate UUID does not match the provided certificate name.
66257396	IPsec is not supported for the admin SVM in a MetroCluster configuration.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

certificate

Certificate for the IPsec policy.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

ipspace

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

Name	Type	Description
name	string	IPspace name
uuid	string	IPspace UUID

local_endpoint

Local endpoint for the IPsec policy.

Name	Type	Description
address	string	IPv4 or IPv6 address
netmask	string	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 the netmask length.
port	string	Application port to be covered by the IPsec policy

ppk

Post-quantum pre-shared key information.

Name	Type	Description
identity	string	Post-quantum pre-shared key identity.
shared_key	string	Post-quantum pre-shared key.

remote_endpoint

Remote endpoint for the IPsec policy.

Name	Type	Description
address	string	IPv4 or IPv6 address
netmask	string	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 the netmask length.
port	string	Application port to be covered by the IPsec policy

svm

SVM, applies only to SVM-scoped objects.

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

ipsec_policy

IPsec policy object.

Name	Type	Description
action	string	Action for the IPsec policy.
authentication_method	string	Authentication method for the IPsec policy.

Name	Type	Description
certificate	certificate	Certificate for the IPsec policy.
enabled	boolean	Indicates whether or not the policy is enabled.
ipspace	ipspace	Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.
local_endpoint	local_endpoint	Local endpoint for the IPsec policy.
local_identity	string	Local Identity
name	string	IPsec policy name.
ppk	ppk	Post-quantum pre-shared key information.
protocol	string	Lower layer protocol to be covered by the IPsec policy.
remote_endpoint	remote_endpoint	Remote endpoint for the IPsec policy.
remote_identity	string	Remote Identity
secret_key	string	Pre-shared key for IKE negotiation.
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	Unique identifier of the IPsec policy.

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

records

IPsec policy object.

Name	Type	Description
action	string	Action for the IPsec policy.
authentication_method	string	Authentication method for the IPsec policy.
certificate	certificate	Certificate for the IPsec policy.
enabled	boolean	Indicates whether or not the policy is enabled.
ipspace	ipspace	Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.
local_endpoint	local_endpoint	Local endpoint for the IPsec policy.
local_identity	string	Local Identity
name	string	IPsec policy name.
ppk	ppk	Post-quantum pre-shared key information.
protocol	string	Lower layer protocol to be covered by the IPsec policy.
remote_endpoint	remote_endpoint	Remote endpoint for the IPsec policy.
remote_identity	string	Remote Identity

Name	Type	Description
secret_key	string	Pre-shared key for IKE negotiation.
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	Unique identifier of the IPsec policy.

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete an IPsec policy

DELETE `/security/ipsec/policies/{uuid}`

Introduced In: 9.8

Deletes a specific IPsec policy.

Related ONTAP commands

- `security ipsec policy delete`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	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.

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

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve an IPsec policy

GET `/security/ipsec/policies/{uuid}`

Introduced In: 9.8

Retrieves a specific IPsec policy.

Related ONTAP commands

- `security ipsec policy show`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	IPsec policy UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
action	string	Action for the IPsec policy.
authentication_method	string	Authentication method for the IPsec policy.
certificate	certificate	Certificate for the IPsec policy.
enabled	boolean	Indicates whether or not the policy is enabled.
ipspace	ipspace	Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.
local_endpoint	local_endpoint	Local endpoint for the IPsec policy.
local_identity	string	Local Identity
name	string	IPsec policy name.
ppk	ppk	Post-quantum pre-shared key information.
protocol	string	Lower layer protocol to be covered by the IPsec policy.
remote_endpoint	remote_endpoint	Remote endpoint for the IPsec policy.
remote_identity	string	Remote Identity
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	Unique identifier of the IPsec policy.

Example response


```
{
  "action": "string",
  "authentication_method": "string",
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "string",
    "netmask": "24",
    "port": "23"
  },
  "local_identity": "string",
  "name": "string",
  "ppk": {
    "identity": "string"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "string",
    "netmask": "24",
    "port": "23"
  },
  "remote_identity": "string",
  "scope": "string",
  "svm": {
    "_links": {
      "self": {
```

```
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

certificate

Certificate for the IPsec policy.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

ipspace

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

Name	Type	Description
_links	_links	
name	string	IPspace name
uuid	string	IPspace UUID

local_endpoint

Local endpoint for the IPsec policy.

Name	Type	Description
address	string	IPv4 or IPv6 address
family	string	IPv4 or IPv6

Name	Type	Description
netmask	string	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 the netmask length.
port	string	Application port to be covered by the IPsec policy

ppk

Post-quantum pre-shared key information.

Name	Type	Description
identity	string	Post-quantum pre-shared key identity.

remote_endpoint

Remote endpoint for the IPsec policy.

Name	Type	Description
address	string	IPv4 or IPv6 address
family	string	IPv4 or IPv6
netmask	string	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 the netmask length.
port	string	Application port to be covered by the IPsec policy

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update an IPsec policy

PATCH `/security/ipsec/policies/{uuid}`

Introduced In: 9.8

Updates a specific IPsec policy.

Related ONTAP commands

- `security ipsec policy modify`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	IPsec policy UUID

Request Body

Name	Type	Description
certificate	certificate	Certificate for the IPsec policy.
enabled	boolean	Indicates whether or not the policy is enabled.
local_endpoint	local_endpoint	Local endpoint for the IPsec policy.
local_identity	string	Local Identity
ppk	ppk	Post-quantum pre-shared key information.
protocol	string	Lower layer protocol to be covered by the IPsec policy.
remote_endpoint	remote_endpoint	Remote endpoint for the IPsec policy.
remote_identity	string	Remote Identity
uuid	string	Unique identifier of the IPsec policy.

Example request

```
{
  "certificate": {
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "netmask": "24",
    "port": "23"
  },
  "local_identity": "string",
  "ppk": {
    "identity": "string"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "netmask": "24",
    "port": "23"
  },
  "remote_identity": "string",
  "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.

Error Code	Description
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.
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).
66257125	The local_endpoint.address must be specified with local_endpoint.netmask.
66257126	The remote_endpoint.address must be specified with remote_endpoint.netmask.
66257127	The local subnet must be configured as a non-zero subnet.
66257128	Invalid ANY wildcard subnet.
66257129	A specific local or remote port number is required when the remote subnet is configured as an ANY wildcard subnet.
66257131	ESP in UDPv6 Encapsulation is not supported.
66257135	The specified certificate is not found on the SVM.
66257136	A certificate is not needed for the PSK authentication method.
66257138	Remote identity is required when using certificate verification.
66257139	Certificate with the specified UUID was not found.
66257140	Only certificates with a client or server type are supported.
66257142	Failed to create IPsec policy because the specified SVM is being migrated.
66257143	Invalid IPsec policy provided. The subnet must be non-empty.
66257153	The policy requires a post-quantum pre-shared key because ppk-identity is specified for this policy.
66257154	The policy requires a post-quantum pre-shared identity because ppk-shared-key is specified for this policy.
66257199	Not all of the nodes in the cluster are running a version that supports the IPsec feature.
66257200	The shared key does not meet required ASCII-range characters length.

Error Code	Description
66257201	Support for the feature available with effective cluster version or later.
66257305	The certificate UUID does not match the provided certificate name.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

certificate

Certificate for the IPsec policy.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

ipspace

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

Name	Type	Description
name	string	IPspace name
uuid	string	IPspace UUID

local_endpoint

Local endpoint for the IPsec policy.

Name	Type	Description
address	string	IPv4 or IPv6 address
netmask	string	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 the netmask length.
port	string	Application port to be covered by the IPsec policy

ppk

Post-quantum pre-shared key information.

Name	Type	Description
identity	string	Post-quantum pre-shared key identity.

remote_endpoint

Remote endpoint for the IPsec policy.

Name	Type	Description
address	string	IPv4 or IPv6 address
netmask	string	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 the netmask length.
port	string	Application port to be covered by the IPsec policy

svm

SVM, applies only to SVM-scoped objects.

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

ipsec_policy

IPsec policy object.

Name	Type	Description
certificate	certificate	Certificate for the IPsec policy.
enabled	boolean	Indicates whether or not the policy is enabled.
local_endpoint	local_endpoint	Local endpoint for the IPsec policy.

Name	Type	Description
local_identity	string	Local Identity
ppk	ppk	Post-quantum pre-shared key information.
protocol	string	Lower layer protocol to be covered by the IPsec policy.
remote_endpoint	remote_endpoint	Remote endpoint for the IPsec policy.
remote_identity	string	Remote Identity
uuid	string	Unique identifier of the IPsec policy.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View IPsec security associations

View IPsec security associations

Overview

- Collection Get: GET security/ipsec/security-associations

- Instance Get: GET security/ipsec/security-associations/uuid

Retrieve IPsec and IKE security associations

GET `/security/ipsec/security-associations`

Introduced In: 9.8

Retrieves the IPsec and IKE (Internet Key Exchange) security associations.

Related ONTAP commands

- `security ipsec show-ipsecsa`
- `security ipsec show-ikesa`

Parameters

Name	Type	In	Required	Description
ike.state	string	query	False	Filter by ike.state
ike.is_initiator	boolean	query	False	Filter by ike.is_initiator
ike.version	integer	query	False	Filter by ike.version
ike.responder_security_parameter_index	string	query	False	Filter by ike.responder_security_parameter_index
ike.authentication	string	query	False	Filter by ike.authentication
ike.initiator_security_parameter_index	string	query	False	Filter by ike.initiator_security_parameter_index
cipher_suite	string	query	False	Filter by cipher_suite
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
local_address	string	query	False	Filter by local_address
remote_address	string	query	False	Filter by remote_address

Name	Type	In	Required	Description
ipsec.state	string	query	False	Filter by ipsec.state
ipsec.inbound.bytes	integer	query	False	Filter by ipsec.inbound.bytes
ipsec.inbound.packets	integer	query	False	Filter by ipsec.inbound.packets
ipsec.inbound.offload_packets	integer	query	False	Filter by ipsec.inbound.offload_packets • Introduced in: 9.16
ipsec.inbound.offload_bytes	integer	query	False	Filter by ipsec.inbound.offload_bytes • Introduced in: 9.16
ipsec.inbound.security_parameter_index	string	query	False	Filter by ipsec.inbound.security_parameter_index
ipsec.outbound.security_parameter_index	string	query	False	Filter by ipsec.outbound.security_parameter_index
ipsec.outbound.bytes	integer	query	False	Filter by ipsec.outbound.bytes
ipsec.outbound.packets	integer	query	False	Filter by ipsec.outbound.packets
ipsec.outbound.offload_packets	integer	query	False	Filter by ipsec.outbound.offload_packets • Introduced in: 9.16

Name	Type	In	Required	Description
ipsec.outbound.offload_bytes	integer	query	False	Filter by ipsec.outbound.offload_bytes • Introduced in: 9.16
ipsec.action	string	query	False	Filter by ipsec.action
type	string	query	False	Filter by type
policy_name	string	query	False	Filter by policy_name
scope	string	query	False	Filter by scope
lifetime	integer	query	False	Filter by lifetime
node.uuid	string	query	False	Filter by node.uuid
node.name	string	query	False	Filter by node.name
uuid	string	query	False	Filter by uuid
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
error	error	
num_records	integer	Number of records
records	array[records]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist"
  },
  "num_records": 1,
  "records": [
    {
      "cipher_suite": "string",
      "ike": {
        "authentication": "string",
        "initiator_security_parameter_index": "string",
        "responder_security_parameter_index": "string",
        "state": "string"
      },
      "ipsec": {
        "action": "string",
        "inbound": {
          "security_parameter_index": "string"
        },
        "outbound": {
          "security_parameter_index": "string"
        },
        "state": "string"
      },
      "local_address": "string",
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
```

```
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "policy_name": "string",
      "remote_address": "string",
      "scope": "string",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "type": "string",
      "uuid": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

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

ike

Objects containing parameters specific to IKE (Internet Key Exchange) security association.

Name	Type	Description
authentication	string	Authentication method for internet key exchange protocol.
initiator_security_parameter_index	string	Initiator's security parameter index for the IKE security association.
is_initiator	boolean	Indicates whether or not IKE has been initiated by this node.

Name	Type	Description
responder_security_parameter_index	string	Responder’s security parameter index for the IKE security association.
state	string	State of the IKE connection.
version	integer	Internet key exchange protocol version.

inbound

Status for inbound parameters for the IPsec security association.

Name	Type	Description
bytes	integer	Number of inbound bytes for the IPsec security association.
offload_bytes	integer	Number of inbound bytes processed by offload for the IPsec security association.
offload_packets	integer	Number of inbound packets processed by offload for the IPsec security association.
packets	integer	Number of inbound packets for the IPsec security association.
security_parameter_index	string	Inbound security parameter index for the IPSec security association.

outbound

Status for outbound parameters for the IPsec security association.

Name	Type	Description
bytes	integer	Number of outbound bytes for the IPsec security association.
offload_bytes	integer	Number of outbound bytes processed by offload for the IPsec security association.

Name	Type	Description
offload_packets	integer	Number of outbound packets processed by offload for the IPsec security association.
packets	integer	Number of outbound packets for the IPsec security association.
security_parameter_index	string	Outbound security parameter index for the IPSec security association.

ipsec

Objects containing parameters specific to IPsec security association.

Name	Type	Description
action	string	Action for the IPsec security association.
inbound	inbound	Status for inbound parameters for the IPsec security association.
outbound	outbound	Status for outbound parameters for the IPsec security association.
state	string	State of the IPsec security association.

_links

Name	Type	Description
self	href	

node

Node with the security association.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

svm

SVM, applies only to SVM-scoped objects.

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

records

Security association object for IPsec security association and IKE (Internet Key Exchange) security association.

Name	Type	Description
cipher_suite	string	Cipher suite for the security association.
ike	ike	Objects containing parameters specific to IKE (Internet Key Exchange) security association.
ipsec	ipsec	Objects containing parameters specific to IPsec security association.
lifetime	integer	Lifetime for the security association in seconds.
local_address	string	Local address of the security association.
node	node	Node with the security association.
policy_name	string	Policy name for the security association.
remote_address	string	Remote address of the security association.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Type of security association, it can be IPsec or IKE (Internet Key Exchange).
uuid	string	Unique identifier of the security association.

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve an IPsec or IKE security association

GET `/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

Name	Type	In	Required	Description
uuid	string	path	True	UUID of IPsec or IKE security association.

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
cipher_suite	string	Cipher suite for the security association.
ike	ike	Objects containing parameters specific to IKE (Internet Key Exchange) security association.
ipsec	ipsec	Objects containing parameters specific to IPsec security association.
lifetime	integer	Lifetime for the security association in seconds.
local_address	string	Local address of the security association.
node	node	Node with the security association.
policy_name	string	Policy name for the security association.
remote_address	string	Remote address of the security association.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Type of security association, it can be IPsec or IKE (Internet Key Exchange).

Name	Type	Description
uuid	string	Unique identifier of the security association.

Example response


```
{
  "cipher_suite": "string",
  "ike": {
    "authentication": "string",
    "initiator_security_parameter_index": "string",
    "responder_security_parameter_index": "string",
    "state": "string"
  },
  "ipsec": {
    "action": "string",
    "inbound": {
      "security_parameter_index": "string"
    },
    "outbound": {
      "security_parameter_index": "string"
    },
    "state": "string"
  },
  "local_address": "string",
  "node": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "policy_name": "string",
  "remote_address": "string",
  "scope": "string",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "string",
  "uuid": "string"
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

ike

Objects containing parameters specific to IKE (Internet Key Exchange) security association.

Name	Type	Description
authentication	string	Authentication method for internet key exchange protocol.
initiator_security_parameter_index	string	Initiator's security parameter index for the IKE security association.
is_initiator	boolean	Indicates whether or not IKE has been initiated by this node.
responder_security_parameter_index	string	Responder's security parameter index for the IKE security association.
state	string	State of the IKE connection.
version	integer	Internet key exchange protocol version.

inbound

Status for inbound parameters for the IPsec security association.

Name	Type	Description
bytes	integer	Number of inbound bytes for the IPsec security association.
offload_bytes	integer	Number of inbound bytes processed by offload for the IPsec security association.
offload_packets	integer	Number of inbound packets processed by offload for the IPsec security association.
packets	integer	Number of inbound packets for the IPsec security association.

Name	Type	Description
security_parameter_index	string	Inbound security parameter index for the IPSec security association.

outbound

Status for outbound parameters for the IPsec security association.

Name	Type	Description
bytes	integer	Number of outbound bytes for the IPsec security association.
offload_bytes	integer	Number of outbound bytes processed by offload for the IPsec security association.
offload_packets	integer	Number of outbound packets processed by offload for the IPsec security association.
packets	integer	Number of outbound packets for the IPsec security association.
security_parameter_index	string	Outbound security parameter index for the IPSec security association.

ipsec

Objects containing parameters specific to IPsec security association.

Name	Type	Description
action	string	Action for the IPsec security association.
inbound	inbound	Status for inbound parameters for the IPsec security association.
outbound	outbound	Status for outbound parameters for the IPsec security association.
state	string	State of the IPsec security association.

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

node

Node with the security association.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

svm

SVM, applies only to SVM-scoped objects.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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.

Manage JIT privilege user configurations

Manage JIT privilege user configurations

Overview

This API is used to create, retrieve, and delete relevant information related to user-specific JIT privilege session configurations. Prerequisites: You must create a user that has a JIT supported login method configured on the SVM that you want to create the elevated session configurations.

Examples

Creating the JIT session configuration for a user

```
# The API:
POST "/api/security/jit-privilege-users"

# The call:
curl -X POST "https://<mgmt-ip>/api/security/jit-privilege-
users?return_records=true" -H "accept: application/hal+json" -d '{
"owner": { "name": "Cserver"} , "account": { "name": "joe"},
"application": "ssh","role": {"name": "admin"},"session_validity":
"PT30M","jit_validity": "PT2H10M20S"}'

# The response:
{}
```

Retrieving the configured JIT privilege sessions for users

Retrieves the JIT privilege user session configurations or a filtered list (for a specific SVM, user, etc).

```
# The API:
GET "/api/security/jit-privilege-users"

# The call:
curl -X GET  "https://<mgmt-ip>/api/security/jit-privilege-users" -H
"accept: application/hal+json"

# The response:
{
  "records": [
    {
      "owner": {
        "uuid": "b009a9e7-4081-b576-7575-ada21efcaf16",
        "name": "Cserver",
        "_links": {
          "self": {
            "href": "/api/svm/svms/b009a9e7-4081-b576-7575-ada21efcaf16"
          }
        }
      },
      "account": {
        "name": "testUser"
      },
      "application": "ssh",
        "_links": {
          "self": {
            "href": "/api/security/jit-privilege-users/b009a9e7-4081-b576-
7575-ada21efcaf16/testUser/ssh"
          }
        }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/jit-privilege-users"
    }
  }
}
```

Retrieve the JIT privilege user configurations for an SVM

GET `/security/jit-privilege-users`

Introduced In: 9.17

Retrieves the JIT privilege user configurations for an SVM.

Related ONTAP commands

- `security jit-privilege user show`

Parameters

Name	Type	In	Required	Description
start_time	string	query	False	Filter by start_time
end_time	string	query	False	Filter by end_time
account.name	string	query	False	Filter by account.name
session_validity	string	query	False	Filter by session_validity
comment	string	query	False	Filter by comment
application	string	query	False	Filter by application
owner.name	string	query	False	Filter by owner.name
owner.uuid	string	query	False	Filter by owner.uuid
jit_state	string	query	False	Filter by jit_state
role.name	string	query	False	Filter by role.name
jit_validity	string	query	False	Filter by jit_validity
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. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • 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[security_jit_privilege_user]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "account": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "joe.smith"
      },
      "application": "string",
      "comment": "Comment text",
      "end_time": "2024-11-08 06:15:31 -0500",
      "jit_state": "active",
      "jit_validity": "P90D",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "role": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "admin"
      },
      "session_validity": "PT1H",
      "start_time": "2024-11-08 05:15:31 -0500"
```

```
      }
    ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

account_reference

The name of the user.

Name	Type	Description
_links	_links	
name	string	User account

owner

Owner name and UUID that uniquely identifies the JIT settings for a user.

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

role

The role the user will be elevated to.

Name	Type	Description
_links	_links	
name	string	Role name

security_jit_privilege_user

Name	Type	Description
account	account_reference	The name of the user.
application	string	The name of the application.
comment	string	The description of the elevation rule.
end_time	string	The end date and time of the JIT privilege session in UTC.
jit_state	string	The current status of the rule: preactive, idle, or active.
jit_validity	string	The JIT validity period on this SVM for this user.
owner	owner	Owner name and UUID that uniquely identifies the JIT settings for a user.
role	role	The role the user will be elevated to.
session_validity	string	The session validity period on this SVM for this user.
start_time	string	The start date and time of the JIT privilege session in UTC.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create JIT privilege user configurations for an SVM

POST `/security/jit-privilege-users`

Introduced In: 9.17

Creates the JIT privilege user configurations for an SVM.

Required properties

- `owner.uuid` - Account owner UUID.
- `account.name` - User name.
- `application` - Application

Related ONTAP commands

- `security jit-privilege user create`

Parameters

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

Request Body

Name	Type	Description
account	account_reference	The name of the user.
application	string	The name of the application.

Name	Type	Description
comment	string	The description of the elevation rule.
end_time	string	The end date and time of the JIT privilege session in UTC.
jit_state	string	The current status of the rule: preactive, idle, or active.
jit_validity	string	The JIT validity period on this SVM for this user.
owner	owner	Owner name and UUID that uniquely identifies the JIT settings for a user.
role	role	The role the user will be elevated to.
session_validity	string	The session validity period on this SVM for this user.
start_time	string	The start date and time of the JIT privilege session in UTC.

Example request

```
{
  "account": {
    "name": "joe.smith"
  },
  "application": "string",
  "comment": "Comment text",
  "end_time": "2024-11-08 06:15:31 -0500",
  "jit_state": "active",
  "jit_validity": "P90D",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "role": {
    "name": "admin"
  },
  "session_validity": "PT1H",
  "start_time": "2024-11-08 05:15:31 -0500"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records.
records	array[security_jit_privilege_user]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "account": {
        "name": "joe.smith"
      },
      "application": "string",
      "comment": "Comment text",
      "end_time": "2024-11-08 06:15:31 -0500",
      "jit_state": "active",
      "jit_validity": "P90D",
      "owner": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "role": {
        "name": "admin"
      },
      "session_validity": "PT1H",
      "start_time": "2024-11-08 05:15:31 -0500"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default, Error
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

account_reference

The name of the user.

Name	Type	Description
name	string	User account

owner

Owner name and UUID that uniquely identifies the JIT settings for a user.

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

role

The role the user will be elevated to.

Name	Type	Description
name	string	Role name

security_jit_privilege_user

Name	Type	Description
account	account_reference	The name of the user.
application	string	The name of the application.
comment	string	The description of the elevation rule.

Name	Type	Description
end_time	string	The end date and time of the JIT privilege session in UTC.
jit_state	string	The current status of the rule: preactive, idle, or active.
jit_validity	string	The JIT validity period on this SVM for this user.
owner	owner	Owner name and UUID that uniquely identifies the JIT settings for a user.
role	role	The role the user will be elevated to.
session_validity	string	The session validity period on this SVM for this user.
start_time	string	The start date and time of the JIT privilege session in UTC.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete JIT privilege user configurations for an SVM

DELETE `/security/jit-privilege-users/{owner.uuid}/{account.name}/{application}`

Introduced In: 9.17

Deletes the JIT privilege user configurations for an SVM.

Related ONTAP commands

- `security jit-privilege user delete`

Required properties

- `owner.uuid`
- `application`
- `account.name`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	
account.name	string	path	True	
application	string	path	True	

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the JIT privilege user configurations for an SVM

GET `/security/jit-privilege-users/{owner.uuid}/{account.name}/{application}`

Introduced In: 9.17

Retrieves the JIT privilege user configurations for an SVM.

Related ONTAP commands

- `security jit-privilege user show`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Used to identify a cluster or an SVM
account.name	string	path	True	The username.
application	string	path	True	The name of the application.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
account	account_reference	The name of the user.
application	string	The name of the application.
comment	string	The description of the elevation rule.
end_time	string	The end date and time of the JIT privilege session in UTC.
jit_state	string	The current status of the rule: preactive, idle, or active.

Name	Type	Description
jit_validity	string	The JIT validity period on this SVM for this user.
owner	owner	Owner name and UUID that uniquely identifies the JIT settings for a user.
role	role	The role the user will be elevated to.
session_validity	string	The session validity period on this SVM for this user.
start_time	string	The start date and time of the JIT privilege session in UTC.

Example response


```
{
  "account": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "application": "string",
  "comment": "Comment text",
  "end_time": "2024-11-08 06:15:31 -0500",
  "jit_state": "active",
  "jit_validity": "P90D",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "session_validity": "PT1H",
  "start_time": "2024-11-08 05:15:31 -0500"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

account_reference

The name of the user.

Name	Type	Description
_links	_links	
name	string	User account

owner

Owner name and UUID that uniquely identifies the JIT settings for a user.

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

role

The role the user will be elevated to.

Name	Type	Description
_links	_links	
name	string	Role name

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage global JIT privilege configurations

Manage global JIT privilege configurations

Overview

This API is used to retrieve and configure relevant information related to the Global JIT (Just In Time) privilege configuration in the cluster.

Examples

Retrieving the configured JIT privilege settings for the cluster

Retrieves the JIT privileges for the cluster or a filtered list (for a specific SVM).

```
# The API:
GET "/api/security/jit-privileges"

# The call
curl -k https://<mgmt-ip>/api/security/jit-privileges

# the response:
{
"records": [
{
  "owner": {
    "uuid": "b009a9e7-4081-b576-7575-ada21efcaf16",
    "name": "Cserver",
    "_links": {
      "self": {
        "href": "/api/svm/svms/b009a9e7-4081-b576-7575-ada21efcaf16"
      }
    }
  },
  "application": "ssh",
  "_links": {
    "self": {
      "href": "/api/security/jit-privileges/b009a9e7-4081-b576-7575-
ada21efcaf16/ssh"
    }
  }
}
]
}
```

Retrieve global JIT privilege configurations for an SVM

GET `/security/jit-privileges`

Introduced In: 9.17

Retrieves global JIT privilege configurations on an SVM.

Related ONTAP commands

- `security jit-privilege show`

Parameters

Name	Type	In	Required	Description
owner.name	string	query	False	Filter by owner.name
owner.uuid	string	query	False	Filter by owner.uuid
default_session_validity_period	string	query	False	Filter by default_session_validity_period
application	string	query	False	Filter by application
max_jit_validity_period	string	query	False	Filter by max_jit_validity_period
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0

Name	Type	In	Required	Description
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[security_jit_privilege]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "application": "string",
      "default_session_validity_period": "PT1H",
      "max_jit_validity_period": "P90D",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

owner

Owner name and UUID that uniquely identifies the JIT privilege global settings.

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

security_jit_privilege

Name	Type	Description
_links	_links	
application	string	The name of the application.
default_session_validity_period	string	The default session validity period on this SVM.
max_jit_validity_period	string	The maximum JIT validity period allowed on this SVM.

Name	Type	Description
owner	owner	Owner name and UUID that uniquely identifies the JIT privilege global settings.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve JIT privilege configurations for an SVM

GET `/security/jit-privileges/{owner.uuid}/{application}`

Introduced In: 9.17

Retrieves the JIT privilege configurations for an SVM.

Related ONTAP commands

- `security jit-privilege show`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Used to identify a cluster or an SVM.

Name	Type	In	Required	Description
application	string	path	True	Application name.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
application	string	The name of the application.
default_session_validity_period	string	The default session validity period on this SVM.
max_jit_validity_period	string	The maximum JIT validity period allowed on this SVM.
owner	owner	Owner name and UUID that uniquely identifies the JIT privilege global settings.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "application": "string",
  "default_session_validity_period": "PT1H",
  "max_jit_validity_period": "P90D",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

owner

Owner name and UUID that uniquely identifies the JIT privilege global settings.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Modify JIT privilege configurations for an SVM

PATCH `/security/jit-privileges/{owner.uuid}/{application}`

Introduced In: 9.17

Modifies the JIT privilege configurations for an SVM.

Related ONTAP commands

- `security jit-privilege modify`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Used to identify a cluster or an SVM.
application	string	path	True	Application name.

Request Body

Name	Type	Description
default_session_validity_period	string	The default session validity period on this SVM.
max_jit_validity_period	string	The maximum JIT validity period allowed on this SVM.

Example request

```
{
  "default_session_validity_period": "PT1H",
  "max_jit_validity_period": "P90D"
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
default_session_validity_period	string	The default session validity period on this SVM.
max_jit_validity_period	string	The maximum JIT validity period allowed on this SVM.

Example response


```
{
  "default_session_validity_period": "PT1H",
  "max_jit_validity_period": "P90D"
}
```


Error

```
Status: Default, Error
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

owner

Owner name and UUID that uniquely identifies the JIT privilege global settings.

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

security_jit_privilege

Name	Type	Description
default_session_validity_period	string	The default session validity period on this SVM.
max_jit_validity_period	string	The maximum JIT validity period allowed on this SVM.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

View and update key manager configurations

View and update key manager configurations

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,
"health_monitor_policy": {
  "akv": {
    "enabled": true,
    "manage_volume_offline": true
  },
  "gcp": {
    "enabled": true,
    "manage_volume_offline": true
  },
  "aws": {
    "enabled": true,
    "manage_volume_offline": true
  },
  "ikp": {
    "enabled": true,
    "manage_volume_offline": true
  },
  "okm": {
    "enabled": true,
    "manage_volume_offline": true
  },
  "kmip": {
    "enabled": true,
    "manage_volume_offline": true
  }
},
"_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" and "passphrase" 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 "{ \"cc_mode_enabled\" : \"true\",
\"passphrase\": \"current_passphrase\" }"
```

Shows the keystore level health monitor policy

The following example shows how to retrieve the health monitor policies for Amazon Web Services and Google Cloud.

```
# The API:
GET /api/security/key-manager-configs

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-manager-
configs?fields=health_monitor_policy.aws,health_monitor_policy.gcp' -H
'accept: application/hal+json'

# The response:
{
"health_monitor_policy": {
  "gcp": {
    "enabled": false,
    "manage_volume_offline": false
  },
  "aws": {
    "enabled": false,
    "manage_volume_offline": false
  }
},
"_links": {
  "self": {
    "href": "/api/security/key-manager-configs"
  }
}
}
```

Updates the keytore level health monitor policy

The following example shows how to modify the Amazon Web Services "enabled" field and the Google Cloud "manage_volume_offline" field of the health monitor policy.

```
# 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_policy": {"aws":
{"enabled": "false"}, "gcp": {"manage_volume_offline": "false"}}}'
```

Retrieve key manager configurations

GET `/security/key-manager-configs`

Introduced In: 9.10

Retrieves key manager configurations. Retrieves the key manager health monitor policy (fields=health_monitor_policy).

Related ONTAP commands

- `security key-manager config show`
- `security key-manager health policy show`

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	
cc_mode_enabled	boolean	Indicates whether the Common Criteria Mode configuration is enabled.
cloud_kms_retry_count	integer	Cloud key manager connection retry count. Supported value range of 0-10.
health_monitor_policy	health_monitor_policy	Manages the keystore configurations.
health_monitor_polling_interval	integer	Health Monitor Polling Period, in minutes. Supported value range of 15-30 minutes.
passphrase	string	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


```
{
  "_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
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

akv

Azure Key Vault Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

aws

Amazon Web Services Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

barbican

Barbican Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.

Name	Type	Description
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

gcp

Google Cloud Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

ikp

IBM Key Protect Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

kmip

External Key Manager policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

okm

Onboard Key Manager policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

health_monitor_policy

Manages the keystore configurations.

Name	Type	Description
akv	akv	Azure Key Vault Key Management Service policy options
aws	aws	Amazon Web Services Key Management Service policy options
barbican	barbican	Barbican Key Management Service policy options
gcp	gcp	Google Cloud Key Management Service policy options
ikp	ikp	IBM Key Protect Key Management Service policy options
kmip	kmip	External Key Manager policy options
okm	okm	Onboard Key Manager policy options

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update key manager configurations

PATCH `/security/key-manager-configs`

Introduced In: 9.10

Updates key manager configurations. Updates the key manager health monitor policy.

Related ONTAP commands

- `security key-manager config modify`
- `security key-manager health policy modify`

Request Body

Name	Type	Description
cc_mode_enabled	boolean	Indicates whether the Common Criteria Mode configuration is enabled.
cloud_kms_retry_count	integer	Cloud key manager connection retry count. Supported value range of 0-10.
health_monitor_policy	health_monitor_policy	Manages the keystore configurations.
health_monitor_polling_interval	integer	Health Monitor Polling Period, in minutes. Supported value range of 15-30 minutes.
passphrase	string	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

```
{
  "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.
65537301	The Onboard Key Manager is not enabled.
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.
65539303	Modifying the health monitor policy requires an effective cluster version of 9.15 or later.

Error Code	Description
65539304	The health monitor policy feature is not enabled.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

akv

Azure Key Vault Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

aws

Amazon Web Services Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

barbican

Barbican Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

gcp

Google Cloud Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

ikp

IBM Key Protect Key Management Service policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

kmip

External Key Manager policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

okm

Onboard Key Manager policy options

Name	Type	Description
enabled	boolean	Indicates whether health monitor is enabled.
manage_volume_offline	boolean	Indicates whether the health monitor manages the volume offline operation.

health_monitor_policy

Manages the keystore configurations.

Name	Type	Description
akv	akv	Azure Key Vault Key Management Service policy options
aws	aws	Amazon Web Services Key Management Service policy options
barbican	barbican	Barbican Key Management Service policy options
gcp	gcp	Google Cloud Key Management Service policy options
ikp	ikp	IBM Key Protect Key Management Service policy options
kmip	kmip	External Key Manager policy options
okm	okm	Onboard Key Manager policy options

key_manager_config

Manages the various key manager configuration options.

Name	Type	Description
cc_mode_enabled	boolean	Indicates whether the Common Criteria Mode configuration is enabled.
cloud_kms_retry_count	integer	Cloud key manager connection retry count. Supported value range of 0-10.
health_monitor_policy	health_monitor_policy	Manages the keystore configurations.

Name	Type	Description
health_monitor_polling_interval	integer	Health Monitor Polling Period, in minutes. Supported value range of 15-30 minutes.
passphrase	string	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

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage key managers

Manage key managers

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"
        },
        {
          "server": "10.225.89.34:5696"
        }
      ]
    },
    "_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": [
  {
    "configuration": {
      "uuid": "2345f09c-d6c9-11e8-b5bf-005056bb017d",
      "name" : "default"
    },
    "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": "",
          "create_remove_timeout": 10,
          "_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",
          "create_remove_timeout": 10,
          "_links": {
            "self": {
              "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-
005056bb017d/key-servers/vs0.local1:3678/"
            }
          }
        }
      ]
    },
    "_links": {
      "self": {
        "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-
005056bb017d"
      }
```

```
    }
  },
  {
   "configuration": {
      "uuid": "815e9462-dc57-11e8-9b2c-005056bb017d",
      "name" : "default"
    },
    "enabled": true,
    "uuid": "815e9462-dc57-11e8-9b2c-005056bb017d",
    "scope": "cluster",
    "external": {
      "client_certificate": {
        "uuid": "5fb1701a-d922-11e8-bfe8-005056bb017d",
        "_links": {
          "self": {
            "href": "/api/security/certificates/5fb1701a-d922-11e8-bfe8-
005056bb017d/"
          }
        }
      },
      "server_ca_certificates": [
        {
          "uuid": "827d7d31-d6c8-11e8-b5bf-005056bb017d",
          "_links": {
            "self": {
              "href": "/api/security/certificates/827d7d31-d6c8-11e8-b5bf-
005056bb017d/"
            }
          }
        }
      ],
      "servers": [
        {
          "server": "10.225.89.33:5696",
          "timeout": 25,
          "username": "",
          "create_remove_timeout": 10,
          "_links": {
            "self": {
              "href": "/api/security/key-managers/815e9462-dc57-11e8-9b2c-
005056bb017d/key-servers/10.225.89.33:5696/"
            }
          }
        }
      ]
    },
```

```
    "_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": [
  {
   "configuration": {
      "uuid": "815e9462-dc57-11e8-9b2c-005056bb017d",
      "name" : "default"
    },
    "enabled": true,
    "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 'accept:
application/hal+jon'

# The response:
{
"records": [
  {
    "configuration": {
      "uuid": "ac305d46-aef4-11e9-ad3c-005056bb7636",
      "name" : "default"
    },
    "enabled": true,
    "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:
{
"configuration": {
      "uuid": "2345f09c-d6c9-11e8-b5bf-005056bb017d",
      "name" : "default"
},
"enabled": true,
"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": "",
      "create_remove_timeout": 10,
```

```
      "_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": "",
      "create_remove_timeout": 10,
      "_links": {
        "self": {
          "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-
005056bb017d/key-servers/vs0.local1:3678/"
        }
      }
    }
  ]
},
"_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"
    ],
    "create_remove_timeout": 10,
    "_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": "",
    "create_remove_timeout": 10,
    "_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"
],
"create_remove_timeout": 10,
"_links": {
  "self": {
    "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-
005056bb017d/key-servers/10.225.89.34:5696"
  }
}
}
```

Retrieving a specific primary key server (and any associated secondary key servers) (and connectivity, an expensive field) 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"
],
"create_remove_timeout": 10,
"connectivity": {
  "cluster_availability": true,
  "node_states": [
    {
      "node": {
        "name": "sti65-vsim-ucs148i",
        "uuid": "661843b3-a0e5-11ed-81ef-005056a7306b"
      },
      "state": "available"
    },
    {
      "node": {
        "name": "sti65-vsim-ucs148j",
        "uuid": "551843b3-a0e5-11ed-81ef-005056a7306b"
      },
      "state": "not_responding"
    }
  ]
}
}
```

Retrieving the connectivity status of a specific node for a specific primary key server configured in an external key manager

The following example shows how to retrieve the connectivity status for a specific node for a specific primary key server 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/43e0c191-dc5c-
11e8-9b2c-005056bb017d/key-
servers/10.225.89.34:5696?fields=connectivity&connectivity.node_states.nod
e.name=sti65-vsim-ucs148i&return_unmatched_nested_array_objects=false' -H
'accept: application/hal+json'

# The response:
{
"uuid": "43e0c191-dc5c-11e8-9b2c-005056bb017d",
"server": "10.225.89.34:5696",
"connectivity": {
  "cluster_availability": true,
  "node_states": [
    {
      "node": {
        "name": "sti65-vsim-ucs148i",
        "uuid": "661843b3-a0e5-11ed-81ef-005056a7306b"
      },
      "state": "available"
    }
  ]
}
}
```

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'
```

Retrieve key managers

GET `/security/key-managers`

Introduced In: 9.6

Retrieves key managers.

Expensive properties

There is an added computational cost to retrieving these properties. They are excluded from default GET results and must be explicitly requested using the `fields` query parameter. For more details, see Requesting specific fields. Additionally, these fields are unavailable for inactive configurations as they are only relevant to active configurations.

- `status.message`
- `status.code`

Examples

- To retrieve basic information about a key manager:

```
GET /security/key-managers
```

- To retrieve specific fields, including expensive properties:

```
GET /security/key-managers/?fields=status.code,status.message
```

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

Name	Type	In	Required	Description
configuration.name	string	query	False	Filter by configuration.name • Introduced in: 9.16

Name	Type	In	Required	Description
configuration.uuid	string	query	False	Filter by configuration.uuid • Introduced in: 9.16
enabled	boolean	query	False	Filter by enabled • Introduced in: 9.16
onboard.enabled	boolean	query	False	Filter by onboard.enabled
onboard.key_backup	string	query	False	Filter by onboard.key_backup • Introduced in: 9.7
external.server_ca_certificates.name	string	query	False	Filter by external.server_ca_certificates.name • Introduced in: 9.8
external.server_ca_certificates.uuid	string	query	False	Filter by external.server_ca_certificates.uuid
external.client_certificate.name	string	query	False	Filter by external.client_certificate.name • Introduced in: 9.8
external.client_certificate.uuid	string	query	False	Filter by external.client_certificate.uuid

Name	Type	In	Required	Description
external.servers.timeout	integer	query	False	Filter by external.servers.timeout • Max value: 60 • Min value: 1
external.servers.username	string	query	False	Filter by external.servers.username
external.servers.secondary_key_servers	string	query	False	Filter by external.servers.secondary_key_servers • Introduced in: 9.8
external.servers.server	string	query	False	Filter by external.servers.server
external.servers.connectivity.node_states.state	string	query	False	Filter by external.servers.connectivity.node_states.state • Introduced in: 9.13
external.servers.connectivity.node_states.node.uuid	string	query	False	Filter by external.servers.connectivity.node_states.node.uuid • Introduced in: 9.13
external.servers.connectivity.node_states.node.name	string	query	False	Filter by external.servers.connectivity.node_states.node.name • Introduced in: 9.13

Name	Type	In	Required	Description
external.servers.connectivity.cluster_availability	boolean	query	False	Filter by external.servers.connectivity.cluster_availability • Introduced in: 9.7
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
uuid	string	query	False	Filter by uuid
is_default_data_at_rest_encryption_disabled	boolean	query	False	Filter by is_default_data_at_rest_encryption_disabled • Introduced in: 9.7
volume_encryption.message	string	query	False	Filter by volume_encryption.message • Introduced in: 9.7
volume_encryption.supported	boolean	query	False	Filter by volume_encryption.supported • Introduced in: 9.7
volume_encryption.code	integer	query	False	Filter by volume_encryption.code • Introduced in: 9.7
scope	string	query	False	Filter by scope

Name	Type	In	Required	Description
status.code	integer	query	False	Filter by status.code • Introduced in: 9.7
status.message	string	query	False	Filter by status.message • Introduced in: 9.7
policy	string	query	False	Filter by policy • Introduced in: 9.9
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 15
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
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[security_key_manager]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "configuration": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
      },
      "external": {
        "client_certificate": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "string",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "server_ca_certificates": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "name": "string",
```

```
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
          }
        ],
        "servers": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "connectivity": {
              "node_states": [
                {
                  "node": {
                    "_links": {
                      "self": {
                        "href": "/api/resourcelink"
                      }
                    },
                    "name": "node1",
                    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
                  },
                  "state": "not_responding"
                }
              ]
            },
            "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--------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAAxBFWWAAAAACEAAAAAAAAA
QAAAAAAAAABzDyyVAAAAALI5Jsjvy6gUxnT78KoDKXHYb6sSeraM00quOULY6BeV
n6dMFxuErCD1lbERaOQZSuaYy1p8oQHtTEfGMLZM4TYiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAADV1Vd/AAAAAMFM9Q229Bhp
mDaTSdqku5DCd8wG+fOZSr4bx4JT5WHvV/r5gJnXDQQAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

```
following nodes - node1, node2."
      }
    }
  ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

configuration

Security keystore object reference.

Name	Type	Description
_links	_links	
name	string	Name of the configuration.
uuid	string	Keystore UUID.

client_certificate

Client certificate (name and UUID)

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

server_ca_certificates

Security certificate object reference

Name	Type	Description
_links	_links	

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

self_link

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

key_server_state

The connectivity state of the key server for a specific node.

Name	Type	Description
node	node	
state	string	Key server connectivity state

connectivity

This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
cluster_availability	boolean	Set to true when key server connectivity state is available on all nodes of the cluster.
node_states	array[key_server_state]	An array of key server connectivity states for each node.

key_server_readcreate

Name	Type	Description
_links	self_link	
connectivity	connectivity	This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.
secondary_key_servers	string	A comma delimited string 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.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	Username credentials for connecting with the key server.

external

Configures external key management

Name	Type	Description
client_certificate	client_certificate	Client certificate (name and UUID)
server_ca_certificates	array[server_ca_certificates]	The array of certificates that are common for all the keyservers per SVM.
servers	array[key_server_readcreate]	The set of external key servers.

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.

Name	Type	Description
enabled	boolean	Is the onboard key manager enabled?
existing_passphrase	string	The cluster-wide passphrase. This is not audited.
key_backup	string	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.

status

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

Name	Type	Description
code	integer	Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added computational 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	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 computational 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

SVM, applies only to SVM-scoped objects.

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

volume_encryption

Indicates whether volume encryption is supported in the cluster.

Name	Type	Description
code	integer	Code corresponding to the status message. Returns a 0 if volume encryption is supported in all nodes of the cluster.
message	string	Reason for not supporting volume encryption.
supported	boolean	Set to true when volume encryption support is available on all nodes of the cluster.

security_key_manager

Name	Type	Description
_links	_links	
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
external	external	Configures external key management

Name	Type	Description
is_default_data_at_rest_encryption_disabled	boolean	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 • x-nullable: true
onboard	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.
policy	string	Security policy associated with the key manager. This value is currently ignored if specified for the onboard key manager.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
status	status	Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	
volume_encryption	volume_encryption	Indicates whether volume encryption is supported in the cluster.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a key manager

POST `/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.

Optional parameters:

- `create_inactive` - Create a configuration without enabling it. This flag is set to "false" by default.

Related ONTAP commands

- `security key-manager external enable`
- `security key-manager onboard enable`
- `security key-manager onboard sync`

Parameters

Name	Type	In	Required	Description
create_inactive	boolean	query	False	Indicates whether to create an active or inactive configuration. • Introduced in: 9.16
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0

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

Request Body

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
external	external	Configures external key management
onboard	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.
policy	string	Security policy associated with the key manager. This value is currently ignored if specified for the onboard key manager.
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	

Example request


```
{
  "configuration": {
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  },
  "external": {
    "client_certificate": {
      "name": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "server_ca_certificates": [
      {
        "name": "string",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    ],
    "servers": [
      {
        "secondary_key_servers": "secondary1.com, 10.2.3.4",
        "server": "keyserver1.com:5698",
        "timeout": 60,
        "username": "admin"
      }
    ]
  },
  "is_default_data_at_rest_encryption_disabled": true,
  "onboard": {
    "existing_passphrase": "The cluster password of length 32-256 ASCII
characters.",
    "key_backup": "'--------------------------BEGIN
BACKUP--------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAAxBFWWAAAAACEAAAAAAAAA
QAAAAAAAAABzDyyVAAAAALI5Jsjvy6gUxnT78KoDKXHYb6sSeraM00quOULY6BeV
n6dMFxuErCD1lbERaOQZSuaYy1p8oQHtTEfGMLZM4TYiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAADV1Vd/AAAAAMFM9Q229Bhp
mDaTSdqku5DCd8wG+fOZSr4bx4JT5WHvV/r5gJnXDQQAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
AQAAAAMAAAAYAQAAAAAALgePkcAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
KAAAAAAAAACIlCHZAAAAAAAAAAAAAAAAAgAAAAAAQCafcabsxRXMM7gxhLRrzxh
AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAA2JjQBQAAAACt4IqXcNpVggahl0axLsN4
yQjnNVKWY7mANB29O42hI7b70DTGCTaVAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
7sbaoQAAAAAiAAAAAAAAACgAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkA
ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAAoAAAAAAAALOHfWkAAAAA
AAAAAAAAAACAAAAAAABAMoI9UxrHOGthQm/CB+EHdAAAAAAAAAACQAAAAAAAA
gAAAAAAAACnMmUtAAAAAGVk8AtPzENFgsGdsFvnmucmYrlQCsFew0HDSFKaZqK6
W8IEVzBAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
----------------------------END BACKUP----------------------------'",
    "passphrase": "The cluster password of length 32-256 ASCII
characters."
  },
  "policy": "string",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "string"
}
```


Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "uuid": "string"
  }
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262224	Failed to contact the peer cluster.
262228	Failed to contact the peer cluster.
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.
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.

Error Code	Description
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 because 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.
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.
65537247	Internal error. Unable to sync the Onboard Key Manager on local cluster.
65537248	Unable to sync the Onboard Key Manager on local cluster.
65538111	The key manager policy is invalid.
65538120	The key manager policy is not supported on the admin SVM.

Error Code	Description
65539216	The Admin SVM has a key manager already configured.
65539221	Failed to configure the Onboard Key Manager because the MetroCluster peer cluster is unhealthy. Verify that the peer cluster is online and healthy.
65539500	Cannot create an inactive external key manager on this SVM because inactive external key managers can only be created on the admin SVM.
65539501	Cannot create an inactive external key manager on the admin SVM because an external key manager already exists on the admin SVM.
65539503	Cannot create an inactive external key manager on the admin SVM while MetroCluster is configured.
65539504	An effective cluster version of ONTAP 9.16.1 or later is required to create an inactive external key manager on the admin SVM.
65539511	Cannot create an inactive Onboard Key Manager on the admin SVM while MetroCluster is configured.
65539512	An effective cluster version of ONTAP 9.16.1 or later is required to create an inactive Onboard Key Manager configuration on the admin SVM.
65539580	Failed to create inactive Onboard Key Manager configuration.
65539581	Cannot create an inactive Onboard Key Manager on the admin SVM because an inactive Onboard Key Manager configuration already exists on the admin SVM.
65539582	Cannot specify the configuration name parameter. Only one Onboard Key Manager is supported for the admin SVM.
65539704	The key manager cannot be configured because the SVM has NAE volumes.
65539706	The Onboard Key Manager is already configured. Use the PATCH to sync all nodes with the Onboard Key Manager 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.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

configuration

Security keystore object reference.

Name	Type	Description
name	string	Name of the configuration.
uuid	string	Keystore UUID.

client_certificate

Client certificate (name and UUID)

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

server_ca_certificates

Security certificate object reference

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

self_link

node

Name	Type	Description
name	string	
uuid	string	

key_server_state

The connectivity state of the key server for a specific node.

Name	Type	Description
node	node	
state	string	Key server connectivity state

connectivity

This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
cluster_availability	boolean	Set to true when key server connectivity state is available on all nodes of the cluster.
node_states	array[key_server_state]	An array of key server connectivity states for each node.

key_server_readcreate

Name	Type	Description
secondary_key_servers	string	A comma delimited string 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.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	Username credentials for connecting with the key server.

external

Configures external key management

Name	Type	Description
client_certificate	client_certificate	Client certificate (name and UUID)
server_ca_certificates	array[server_ca_certificates]	The array of certificates that are common for all the keyservers per SVM.
servers	array[key_server_readcreate]	The set of external key servers.

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.

Name	Type	Description
enabled	boolean	Is the onboard key manager enabled?
existing_passphrase	string	The cluster-wide passphrase. This is not audited.
key_backup	string	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	The cluster-wide passphrase. This is not audited.
synchronize	boolean	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

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

Name	Type	Description
code	integer	Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added computational 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	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 computational 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

SVM, applies only to SVM-scoped objects.

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

volume_encryption

Indicates whether volume encryption is supported in the cluster.

Name	Type	Description
code	integer	Code corresponding to the status message. Returns a 0 if volume encryption is supported in all nodes of the cluster.
message	string	Reason for not supporting volume encryption.
supported	boolean	Set to true when volume encryption support is available on all nodes of the cluster.

security_key_manager

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
external	external	Configures external key management
onboard	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.
policy	string	Security policy associated with the key manager. This value is currently ignored if specified for the onboard key manager.
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete key managers

DELETE `/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

Name	Type	In	Required	Description
uuid	string	path	True	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.
	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

Error Code	Description
NAE aggregates are found in the cluster.	Also see the table of common errors in the Response body overview section of this documentation. * name: KEYMANAGER_MESSAGE_ERR_KM_DISABLE_ENC_CORE_CHECK_TIMEOUT message: Failed to disable the key manager because of a timeout when checking for encrypted cores.

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve key managers

GET `/security/key-managers/{uuid}`

Introduced In: 9.6

Retrieves key managers.

Expensive properties

There is an added computational cost to retrieving these properties. They are excluded from default GET results and must be explicitly requested using the `fields` query parameter. For more details, see Requesting specific fields. Additionally, these fields are unavailable for inactive configurations as they are only relevant to active configurations.

- `status.message`
- `status.code`

Examples

- To retrieve basic information about a key manager:

```
GET /security/key-managers/{uuid}
```

- To retrieve specific fields, including expensive properties:

```
GET /security/key-managers/{uuid}?fields=status.message
```

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

Name	Type	In	Required	Description
uuid	string	path	True	Key manager UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
external	external	Configures external key management

Name	Type	Description
is_default_data_at_rest_encryption_disabled	boolean	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 • x-nullable: true
onboard	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.
policy	string	Security policy associated with the key manager. This value is currently ignored if specified for the onboard key manager.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
status	status	Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	
volume_encryption	volume_encryption	Indicates whether volume encryption is supported in the cluster.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "configuration": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  },
  "external": {
    "client_certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "server_ca_certificates": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "string",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    ],
    "servers": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "connectivity": {
```

```
          "node_states": [
            {
              "node": {
                "_links": {
                  "self": {
                    "href": "/api/resourcelink"
                  }
                },
                "name": "node1",
                "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
              },
              "state": "not_responding"
            }
          ]
        },
        "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-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAAxBFWWAAAAACEAAAAAAAAA
QAAAAAAAAABzDyyVAAAAALI5Jsjvy6gUxnT78KoDKXHYb6sSeraM00quOULY6BeV
n6dMFxuErCD1lbERaOQZSuaYy1p8oQHtTEfGMLZM4TYiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAADV1Vd/AAAAAMFM9Q229Bhp
mDaTSdqku5DCd8wG+fOZSr4bx4JT5WHvV/r5gJnXDQQAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
yQjnNVKWY7mANB29O42hI7b70DTGCTaVAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAA
7sbaoQAAAAAiAAAAAAAAACgAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAkA
ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAAoAAAAAAAALOHfWkAAAAA
AAAAAAAAAACAAAAAAABAMoI9UxrHOGthQm/CB+EHdAAAAAAAAAACQAAAAAAAA
gAAAAAAAACnMmUtAAAAAGVk8AtPzENFgsGdsFvnmucmYrlQCsFew0HDSFKaZqK6
W8IEVzBAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
----------END BACKUP----------'",
    "synchronize": true
  },
  "policy": "string",
  "scope": "string",
  "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
65536894	This cluster is part of a MetroCluster configuration. Configure an external key manager on the partner cluster providing the same key servers before proceeding with any key manager operations.
65537201	There are no key servers configured for this SVM in the local cluster.
65537202	There are no key servers configured for this SVM in the remote cluster.
65537203	Internal error. Failed to check for key servers on partner cluster.
65537204	This cluster is part of a MetroCluster configuration. Configure an external key manager on the partner cluster providing the same key servers before proceeding with any key manager operations.

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

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

configuration

Security keystore object reference.

Name	Type	Description
_links	_links	
name	string	Name of the configuration.
uuid	string	Keystore UUID.

client_certificate

Client certificate (name and UUID)

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

server_ca_certificates

Security certificate object reference

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

self_link

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

key_server_state

The connectivity state of the key server for a specific node.

Name	Type	Description
node	node	
state	string	Key server connectivity state

connectivity

This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
cluster_availability	boolean	Set to true when key server connectivity state is available on all nodes of the cluster.
node_states	array[key_server_state]	An array of key server connectivity states for each node.

key_server_readcreate

Name	Type	Description
_links	self_link	

Name	Type	Description
connectivity	connectivity	This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.
secondary_key_servers	string	A comma delimited string 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.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	Username credentials for connecting with the key server.

external

Configures external key management

Name	Type	Description
client_certificate	client_certificate	Client certificate (name and UUID)
server_ca_certificates	array[server_ca_certificates]	The array of certificates that are common for all the keyservers per SVM.
servers	array[key_server_readcreate]	The set of external key servers.

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.

Name	Type	Description
enabled	boolean	Is the onboard key manager enabled?
existing_passphrase	string	The cluster-wide passphrase. This is not audited.
key_backup	string	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.

status

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

Name	Type	Description
code	integer	Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added computational 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	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 computational 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

SVM, applies only to SVM-scoped objects.

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

volume_encryption

Indicates whether volume encryption is supported in the cluster.

Name	Type	Description
code	integer	Code corresponding to the status message. Returns a 0 if volume encryption is supported in all nodes of the cluster.
message	string	Reason for not supporting volume encryption.
supported	boolean	Set to true when volume encryption support is available on all nodes of the cluster.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Update key managers

PATCH `/security/key-managers/{uuid}`

Introduced In: 9.6

Updates a key manager. **Note:** When validate_certificates is set, the API returns a 202 status code for successful creation of the job, otherwise an error is returned.

Required properties (when patching the Onboard Key Manager)

- `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.

Required properties (when patching an external key manager)

- `external.client_certificate` or `external.server_ca_certificates` - Client certificate or Server CA certificate. Required when modifying an external key manager.

Optional parameters (when patching an external key manager):

- `validate_certificates` - Validate certificates by testing the connection to the KMIP server using them. This flag is set to "false" by default.

Related ONTAP commands

- `security key-manager external modify`
- `security key-manager onboard sync`
- `security key-manager onboard update-passphrase`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Key manager UUID

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
enabled	boolean	Indicates whether the configuration is enabled.
external	external	Configures external key management

Name	Type	Description
is_default_data_at_rest_encryption_disabled	boolean	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 • x-nullable: true
onboard	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.
uuid	string	

Example request


```
{
  "external": {
    "client_certificate": {
      "name": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "server_ca_certificates": [
      {
        "name": "string",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    ]
  },
  "onboard": {
    "existing_passphrase": "The cluster password of length 32-256 ASCII
characters.",
    "key_backup": "'-------------------------BEGIN
BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAAxBFWWAAAAACEAAAAAAAAA
QAAAAAAAAABzDyyVAAAAALI5Jsjvy6gUxnT78KoDKXHYb6sSeraM00quOULY6BeV
n6dMFxuErCD1lbERaOQZSuaYy1p8oQHtTEfGMLZM4TYiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAADV1Vd/AAAAMFM9Q229Bhp
mDaTSdqku5DCd8wG+fOZSr4bx4JT5WHvV/r5gJnXDQQAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
W8IEVzBAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
----------------------------END BACKUP----------------------------'",
    "passphrase": "The cluster password of length 32-256 ASCII
characters."
  },
  "uuid": "string"
}
```

Response

```
Status: 200, Ok
```

Response

```
Status: 202, Accepted
```

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.
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.

Error Code	Description
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.
65538120	The key manager policy is not supported on the admin SVM.
65539586	Cannot modify an inactive key manager 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.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

configuration

Security keystore object reference.

Name	Type	Description
name	string	Name of the configuration.
uuid	string	Keystore UUID.

client_certificate

Client certificate (name and UUID)

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

server_ca_certificates

Security certificate object reference

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

self_link

node

Name	Type	Description
name	string	
uuid	string	

key_server_state

The connectivity state of the key server for a specific node.

Name	Type	Description
node	node	
state	string	Key server connectivity state

connectivity

This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
cluster_availability	boolean	Set to true when key server connectivity state is available on all nodes of the cluster.
node_states	array[key_server_state]	An array of key server connectivity states for each node.

key_server_readcreate

Name	Type	Description
secondary_key_servers	string	A comma delimited string of the secondary key servers associated with the primary key server.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	Username credentials for connecting with the key server.

external

Configures external key management

Name	Type	Description
client_certificate	client_certificate	Client certificate (name and UUID)

Name	Type	Description
server_ca_certificates	array[server_ca_certificates]	The array of certificates that are common for all the keyservers per SVM.

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.

Name	Type	Description
enabled	boolean	Is the onboard key manager enabled?
existing_passphrase	string	The cluster-wide passphrase. This is not audited.
key_backup	string	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	The cluster-wide passphrase. This is not audited.
synchronize	boolean	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

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

Name	Type	Description
code	integer	Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added computational 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	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 computational 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

SVM, applies only to SVM-scoped objects.

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

volume_encryption

Indicates whether volume encryption is supported in the cluster.

Name	Type	Description
code	integer	Code corresponding to the status message. Returns a 0 if volume encryption is supported in all nodes of the cluster.
message	string	Reason for not supporting volume encryption.
supported	boolean	Set to true when volume encryption support is available on all nodes of the cluster.

security_key_manager

Name	Type	Description
enabled	boolean	Indicates whether the configuration is enabled.
external	external	Configures external key management
is_default_data_at_rest_encryption_disabled	boolean	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 • x-nullable: true
onboard	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.
uuid	string	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage authentication keys

Manage authentication keys

Overview

Used to create and list authentication keys (NSE-AK).

Example

Creates an authentication key.

an external key manager must be configured on the admin SVM, as the authentication key will be associated with the admin SVM. The following example shows how to create an authentication key.

```
# The API:
POST /api/security/key-managers/{security_key_manager.uuid}/auth-keys

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-managers/5fb1701a-d922-
11e8-bfe8-005056bb017d/auth-keys?return_timeout=15&return_records=true' -H
'accept: application/hal+json'

# The response:
{
"num_records": 1,
"records": [
  {
    "key_id":
"000000000000000002000000000000100531d8cdc38437c2627b6b1726dd2675c000000000
0000000",
    "key_tag": "vsim1"
  }
]
}
```

Retrieving a list of all of the authentication keys associated with the admin SVM.

The following example shows how to retrieve a list of all of the authentication keys associated with the admin SVM.

```
# The API:
GET /api/security/key-managers/{security_key_manager.uuid}/auth-keys

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers/5fb1701a-d922-
11e8-bfe8-005056bb017d/auth-keys?fields=*' -H 'accept:
application/hal+json'

# The response:
{
"num_records": 2,
"records": [
  {
    "security_key_manager": {
      "uuid": "d36a654d-14b4-11ed-b82e-005056bb8f59"
    },
    "key_id":
"00000000000000000200000000000100052ab79fc51a430dbb16f1c0d2054cfe000000000
0000000",
    "key_tag": "vsim1"
  },
  {
    "security_key_manager": {
      "uuid": "d36a654d-14b4-11ed-b82e-005056bb8f59"
    },
    "key_id":
"00000000000000000200000000001003f32ce2dc55d2764c07da74e722c179b000000000
0000000",
    "key_tag": "vsim1"
  }
]
}
```

Retrieving a specific authentication key associated with the admin SVM.

The following example shows how to a specific authentication key associated with the admin SVM and return the key-tag.

```
= The API:

GET /api/security/key-managers/{security_key_manager.uuid}/auth-
keys/\{key-id}

= The call:
```

```
curl -X GET 'https://+++<mgmt-ip>+++/api/security/key-managers/5fb1701a-
d922-11e8-bfe8-005056bb017d/auth-
keys/0000000000000000020000000000010041a2dda969b0d179db8f1c78d629d0f100000
00000000000?fields=key_tag' -H 'accept: application/hal+json'+++</mgmt-
ip>+++

= The response:

{
"security_key_manager": {
  "uuid": "d36a654d-14b4-11ed-b82e-005056bb8f59"
},
"key_id":
"0000000000000000020000000000010041a2dda969b0d179db8f1c78d629d0f1000000000
0000000",
"key_tag": "vsim1"
}
```

```
[[IDa94ed58b83a75aa6bed3f7b612ea1850]]
= Retrieve authentication keys associated with the admin SVM

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/key-managers/{security_key_manager.uuid}/auth-keys`#

*Introduced In:* 9.12

Retrieves a list of all authentication keys associated with the admin SVM.

== Related ONTAP commands

* `security key-manager key query`

== Required properties

* `security_key_manager.uuid` - UUID of the external key manager.


== Parameters

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

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

|key_id
|string
|query
|False
a|Filter by key_id


|key_tag
|string
|query
|False
a|Filter by key_tag


|security_key_manager.uuid
|string
|path
|True
a|External key manager 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: 15
* 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:#key_manager_auth_key[key_manager_auth_key]]
a|

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "key_id":
"00000000000000000200000000001003aa8ce6a4fea3e466620134bea9510a100000000000000000",
      "key_tag": "Authentication-Key-01",
      "security_key_manager": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
      }
    }
  ]
}
====

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65536828
| External key management is not enabled for the SVM.

| 65536856
| No key servers found for the SVM.

| 65536896
| External key management is not configured on the partner site.

| 65538800
| External KMIP DKMIP keymanager not configured on administrative Vserver.

| 65538801
| Internal error while accessing keymanager database.

| 65538802
| The UUID provided is not associated with the administrator SVM key
manager.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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|

|===


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

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

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

|===


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

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

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

```
|===


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

Security key manager object reference.


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

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

|uuid
|string
a|Key manager UUID


|===


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

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

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

|key_id
|string
a|Key identifier.
```

```
|key_tag
|string
a|Optional parameter to define key-tag for the authentication key, length
0-32 characters.


|security_key_manager
|link:#security_key_manager[security_key_manager]
a|Security key manager object reference.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID59fc8856caa3ed58089c0238b1799602]]
= Create an authentication key

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/key-managers/{security_key_manager.uuid}/auth-keys`#

*Introduced In:* 9.12

Creates an authentication key.

== Related ONTAP commands

* `security key-manager key create`

== Required properties

* `security_key_manager.uuid` - UUID of the external key manager.
```

```
== Parameters

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

|Name
|Type
|In
|Required
|Description

|security_key_manager.uuid
|string
|path
|True
a|External key manager UUID


|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.


|key_tag
|string
a|Optional parameter to define key-tag for the authentication key, length
```

```
0-32 characters.


|passphrase
|string
a|Authentication passphrase, length 20-32 characters. May contain the '='
character.


|security_key_manager
|link:#security_key_manager[security_key_manager]
a|Security key manager object reference.


|===


.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "key_id":
"00000000000000000200000000001003aa8ce6a4fea3e466620134bea9510a1000000000
0000000",
  "key_tag": "Authentication-Key-01",
  "passphrase": "AuthenticationKey_01",
  "security_key_manager": {
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  }
}
====

== Response
```

Status: 201, Created

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

|num_records
|integer
a|Number of records
```

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

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "records": [
    {
      "key_id":
"000000000000000002000000000001003aa8ce6a4fea3e466620134bea9510a100000000000000000",
      "key_tag": "Authentication-Key-01",
      "passphrase": "AuthenticationKey_01",
      "security_key_manager": {
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
      }
    }
  ]
}
====

=== Headers

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

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===
```

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65536048
| The maximum number of authentication keys are already configured.

| 65536053
| Invalid passphrase length; passphrase must be 20-32 ASCII-range
characters.

| 65536056
| The key tag value provided contains invalid characters.

| 65536056
| The key-tag option cannot contain any spaces, tabs or new lines.

| 65536076
| Failed to push authentication key to any registered key servers.

| 65536160
| Unable to determine the current number of configured authentication
keys.

| 65536264
| Failed to create authentication key.

| 65536265
| Failed to create a key-id for the authentication key.

| 65536828
| External key management is not enabled for the SVM.

| 65536856
| No key servers found for the SVM.

| 65536872
| Error cleaning up key database after key creation error.

| 65536896
| External key management is not configured on the partner site.
```

```
| 65536987
| One or more key servers are unavailable.

| 65538800
| External KMIP DKMIP keymanager not configured on administrative Vserver.

| 65538801
| Internal error while accessing keymanager database.

| 65538802
| The UUID provided is not associated with the administrator SVM key
manager.

| 66060289
| Failed to store authentication key on key server.

| 66060304
| Invalid key length.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


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

Security key manager object reference.


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

|uuid
|string
a|Key manager UUID


|===


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

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

|key_id
|string
a|Key identifier.


|key_tag
|string
```

```
a|Optional parameter to define key-tag for the authentication key, length
0-32 characters.


|passphrase
|string
a|Authentication passphrase, length 20-32 characters. May contain the '='
character.


|security_key_manager
|link:#security_key_manager[security_key_manager]
a|Security key manager object reference.


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID81a4c0acce8575498408b8eb67e0de72]]
= Delete an authentication key

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/key-managers/{security_key_manager.uuid}/auth-
keys/{key_id}`#

*Introduced In:* 9.12

Deletes an authentication key.

== Related ONTAP commands

* `security key-manager key delete`
```

```
== Required properties

* `security_key_manager.uuid` - UUID of the external key manager.
* `key_id` - Key ID of the authentication key to be deleted.


== Parameters

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

|Name
|Type
|In
|Required
|Description

|security_key_manager.uuid
|string
|path
|True
a|External key manager UUID


|key_id
|string
|path
|True
a|Key ID of the authentication key to be deleted.

|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description
```

```
| 65536828
| External key management is not enabled for the SVM.

| 65536859
| Authentication key-Id provided for deletion is in use.

| 65536860
| Key-id provided for deletion is not an authentication key.

| 65538800
| External KMIP DKMIP keymanager not configured on administrative Vserver.

| 65538801
| Internal error while accessing keymanager database.

| 65538802
| The UUID provided is not associated with the administrator SVM key
manager.

| 66060296
| Failed to delete key from an external key server.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

|error
|link:#returned_error[returned_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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID1706dfd0857a68eed87d45771089acb4]]
= List all authentication keys associated with the admin SVM

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/key-managers/{security_key_manager.uuid}/auth-
keys/{key_id}`#

*Introduced In:* 9.12

Retrieves the authentication key identified by the 'key_id' and associated
with the admin SVM.
```

```
== Related ONTAP commands

* `security key-manager key query`

== Required properties

* `security_key_manager.uuid` - UUID of the external key manager.
* `key_id` - Key ID of the authentication key to be retrieved.


== Parameters

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

|Name
|Type
|In
|Required
|Description

|key_tag
|string
|query
|False
a|Filter by key_tag


|security_key_manager.uuid
|string
|path
|True
a|External key manager UUID


|key_id
|string
|path
|True
a|Key ID of the authentication key to be retrieved.


|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: 15
* 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:#self_link[self_link]
a|

|key_id
|string
a|Key identifier.


|key_tag
|string
a|Optional parameter to define key-tag for the authentication key, length
0-32 characters.


|security_key_manager
|link:#security_key_manager[security_key_manager]
a|Security key manager object reference.


|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "key_id":
"00000000000000000200000000001003aa8ce6a4fea3e466620134bea9510a1000000000
0000000",
  "key_tag": "Authentication-Key-01",
  "security_key_manager": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
```

```
      }
    },
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  }
}
====

== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 65536828
| External key management is not enabled for the SVM.

| 65536856
| No key servers found for the SVM.

| 65536896
| External key management is not configured on the partner site.

| 65538800
| External KMIP DKMIP keymanager not configured on administrative Vserver.

| 65538801
| Internal error while accessing keymanager database.

| 65538802
| The UUID provided is not associated with the administrator SVM key
manager.
|===

Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.



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

```
|Description

|error
|link:#returned_error[returned_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|

|===


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

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

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

|===


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

Security key manager object reference.
```

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

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

|uuid
|string
a|Key manager UUID


|===


[#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


|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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


[[IDb04d1930e6a30072dfa32f9e354f8027]]
= View security key managers



: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-
managers/{security_key_manager.uuid}/keys/{node.uuid}/key-ids

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers/f4f98a48-8a5c-
c548-cd03-c6335f5803a8/keys/00000000-0000-0000-0000-000000000000/key-
ids/00000000000000000200000000005009ad4da8fea2cafe2bed803078b780ebe000000
0000000c01' -H 'accept: application/hal+json'

# The response:
{
  "security_key_manager": {
    "uuid": "f4f98a48-8a5c-c548-cd03-c6335f5803a8"
  },
  "node": {
    "uuid": "00000000-0000-0000-0000-000000000000"
  },
  "key_id":
"00000000000000000200000000005009ad4da8fea2cafe2bed803078b780ebe0000000000
0000c01",
  "svm": {
    "name": "cluster-1"
  },
  "key_tag": "vsim1",
  "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/000000000000000002000000000005009ad4da8fea2cafe2bed803078b780ebe000000
0000000c01"
    }
  }
}
----

'''

=== Retrieving key manager key-id information of a specific key-type for a
node

The following example shows how to retrieve key-ids of a specific key-type
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/security/key-managers/7c179931-044b-11ed-b7cd-005056bbc535/keys/44dac31e-0449-11ed-b7cd-005056bbc535/key-ids?key_type=nse_ak&return_records=true&return_timeout=15" -H "accept: application/json"</mgmt-ip>

The response:

{ "records": [{ "key_server": "10.225.89.34:5696", "key_id": "000000000000000002000000000001003d5c5f8c497e8e36aa80566e08749a3d0000000000000000", "key_type": "nse_ak" }, { "key_server": "10.225.89.34:5696", "key_id": "000000000000000002000000000000100c2dce9a3a15aeb8480db8d49c17d056c0000000000000000", "key_type": "nse_ak" }], "num_records": 2 }

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`
- `security key-manager key query -node <node>`
- `security key-manager key query -node <node> -key-manager <key_manager>`

Parameters

Name	Type	In	Required	Description
key_type	string	query	False	Filter by key_type • Introduced in: 9.12
scope	string	query	False	Filter by scope • Introduced in: 9.14
policy	string	query	False	Filter by policy • Introduced in: 9.12
key_store	string	query	False	Filter by key_store • Introduced in: 9.12
key_id	string	query	False	Filter by key_id • Introduced in: 9.12
svm.name	string	query	False	Filter by svm.name • Introduced in: 9.14
svm.uuid	string	query	False	Filter by svm.uuid • Introduced in: 9.14

Name	Type	In	Required	Description
key_manager	string	query	False	Filter by key_manager • Introduced in: 9.12
key_server	string	query	False	Filter by key_server • Introduced in: 9.12
restored	boolean	query	False	Filter by restored • Introduced in: 9.12
key_user	string	query	False	Filter by key_user • Introduced in: 9.12
crn	string	query	False	Filter by crn • Introduced in: 9.12
key_store_type	string	query	False	Filter by key_store_type • Introduced in: 9.12
encryption_algorithm	string	query	False	Filter by encryption_algorithm • Introduced in: 9.12
node.name	string	query	False	Filter by node.name • Introduced in: 9.12
key_tag	string	query	False	Filter by key_tag • Introduced in: 9.12

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. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • 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"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "crn": "CRN=v1:bluemix:public:containers-kubernetes",
      "encryption_algorithm": "XTS-AES-256",
      "key_id":
"00000000000000000200000000001008963c9213194c59555c1bec8db3603c800000000",
      "key_manager": "keyserver1.local:5696",
      "key_server": "keyserver1.com:5698",
      "key_store": "string",
      "key_store_type": "string",
      "key_tag": "key#",
      "key_type": "string",
      "key_user": "vs1",
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "policy": "IBM_Key_Lore",
      "restored": 1,
      "scope": "string",
      "security_key_manager": {
        "_links": {
          "self": {
```

```
            "href": "/api/resourcelink"
          }
        },
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
      },
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
65537125	The provided key manager UUID is not the UUID of a keymanager.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
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	

security_key_manager

Security key manager object reference.

Name	Type	Description
_links	_links	
uuid	string	Key manager UUID

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	

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

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.
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.

Name	Type	Description
node	node	
policy	string	Key store policy.
restored	boolean	Indicates whether the key is present locally on the node.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
security_key_manager	security_key_manager	Security key manager object reference.
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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>`
- `security key-manager key query -key-id <key_id> -node <node>`
- `security key-manager key query -key-id <key_id> -node <node> -key-manager <key_manager>`

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
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.

Name	Type	Description
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.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
security_key_manager	security_key_manager	Security key manager object reference.
svm	svm	SVM, applies only to SVM-scoped objects.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "crn": "CRN=v1:bluemix:public:containers-kubernetes",
  "encryption_algorithm": "XTS-AES-256",
  "key_id":
"00000000000000000200000000001008963c9213194c59555c1bec8db3603c800000000",
  "key_manager": "keyserver1.local:5696",
  "key_server": "keyserver1.com:5698",
  "key_store": "string",
  "key_store_type": "string",
  "key_tag": "key#",
  "key_type": "string",
  "key_user": "vs1",
  "node": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "policy": "IBM_Key_Lore",
  "restored": 1,
  "scope": "string",
  "security_key_manager": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
```

```
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

security_key_manager

Security key manager object reference.

Name	Type	Description
_links	_links	
uuid	string	Key manager UUID

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve and restore unrestored keys

POST `/security/key-managers/{security_key_manager.uuid}/restore`

Introduced In: 9.13

Retrieves and restores any current unrestored keys (associated with the storage controller) from the specified key management server.

Required properties

- `security_key_manager.uuid` - UUID of the key management server. The UUID of the external key manager can be retrieved using [`GET /api/security/key-managers`].

Related ONTAP commands

- `security key-manager external restore`

Parameters

Name	Type	In	Required	Description
security_key_manager.uuid	string	path	True	Key manager UUID.
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
key_id	string	Key identifier.

Name	Type	Description
key_server	string	External key server for key management.
key_tag	string	Additional information associated with the key.
node	node	

Example request

```
{
  "key_id":
"00000000000000000200000000001003aa8ce6a4fea3e466620134bea9510a1000000
0000000000",
  "key_server": "keyserver1.com:5698",
  "key_tag": "Authentication-Key-01",
  "node": {
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  }
}
```

Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
65536083	Internal error. Failed to restore the authentication key.
65536843	The key management server is not configured for the SVM.
65536855	Internal error. Failed to restore the volume encryption key.
65538500	This command only restores keys from primary key servers.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

node

Name	Type	Description
uuid	string	

security_key_manager_restore_keys

Name	Type	Description
key_id	string	Key identifier.
key_server	string	External key server for key management.
key_tag	string	Additional information associated with the key.
node	node	

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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`]. The UUID of Amazon Web Services key manager can be fetched using [`GET /api/security/aws-kms`].

Related ONTAP commands

- `security key-manager key 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	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: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
uuid	string	Key manager UUID

Example request

```
{
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
}
```

Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Response

```
Status: 201, Created
```

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.

Error Code	Description
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.
65537611	Key migration cannot be performed on the SVM while the enabled keystore configuration is being switched. If a previous attempt to switch the keystore configuration failed, or was interrupted, the system will continue to prevent key migration for the SVM. Use the REST API PATCH method "/api/security/key-stores/{uuid}" to re-run and complete 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.
65539434	Cannot perform key migration on the SVM while the keystore is being initialized. Wait until the keystore is in the active state, and rerun the key migration operation.
65539435	Cannot perform key migration on the SVM while the keystore is being disabled.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

info

Migration destination key manager UUID

Name	Type	Description
uuid	string	Key manager UUID

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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.

Expensive properties

There is an added computational cost to retrieving these properties. They are excluded from default GET results and must be explicitly requested using the `fields` query parameter. For more details, see Requesting specific fields. Additionally, these fields are unavailable for inactive configurations as they are only relevant to active configurations.

- `connectivity.cluster_availability`
- `connectivity.node_states.node.name`
- `connectivity.node_states.node.uuid`
- `connectivity.node_states.state`

Examples

- To retrieve basic information about a key server:

```
GET /security/key-managers/{uuid}/key-servers
```

- To retrieve specific fields, including expensive properties:

```
GET /security/key-managers/{uuid}/key-
servers?fields=connectivity.cluster_availability,connectivity.node_state
s.node.name
```

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
timeout	integer	query	False	Filter by timeout • Max value: 60 • Min value: -1
connectivity.node_states.state	string	query	False	Filter by connectivity.node_states.state • Introduced in: 9.13
connectivity.node_states.node.uuid	string	query	False	Filter by connectivity.node_states.node.uuid • Introduced in: 9.13
connectivity.node_states.node.name	string	query	False	Filter by connectivity.node_states.node.name • Introduced in: 9.13
connectivity.cluster_availability	boolean	query	False	Filter by connectivity.cluster_availability • Introduced in: 9.7
username	string	query	False	Filter by username
create_remove_timeout	integer	query	False	Filter by create_remove_timeout • Introduced in: 9.14 • Max value: 60 • Min value: -1

Name	Type	In	Required	Description
secondary_key_servers	string	query	False	Filter by secondary_key_servers • Introduced in: 9.8
server	string	query	False	Filter by server
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 15
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
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"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "connectivity": {
        "node_states": [
          {
            "node": {
              "_links": {
                "self": {
                  "href": "/api/resourcelink"
                }
              },
              "name": "node1",
              "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
            },
            "state": "not_responding"
          }
        ]
      },
      "create_remove_timeout": 60,
      "password": "password",
      "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	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

key_server_state

The connectivity state of the key server for a specific node.

Name	Type	Description
node	node	
state	string	Key server connectivity state

connectivity

This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
cluster_availability	boolean	Set to true when key server connectivity state is available on all nodes of the cluster.

Name	Type	Description
node_states	array[key_server_state]	An array of key server connectivity states for each node.

records

Name	Type	Description
_links	_links	
connectivity	connectivity	This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.
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 `records` 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
connectivity	connectivity	This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.
create_remove_timeout	integer	The key server timeout for create and remove operations. -1 indicates that the server will wait indefinitely for the event to occur. 0 indicates that the server will not wait and will immediately timeout if it does not receive a response.
password	string	Password credentials for connecting with the key server. This is not audited.
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 `records` is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server. -1 indicates that the server will wait indefinitely for the event to occur. 0 indicates that the server will not wait and will immediately timeout if it does not receive a response.
username	string	KMIP username credentials for connecting with the key server.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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

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

Request Body

Name	Type	Description
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 `server` is provided.
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 `records` is provided.

Example request

```
{
  "password": "password",
  "records": [
    {
      "password": "password",
      "server": "bulkkeyserver.com:5698"
    }
  ],
  "server": "keyserver1.com:5698"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[key_server]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "password": "password",
      "records": [
        {
          "password": "password",
          "server": "bulkkeyserver.com:5698"
        }
      ],
      "server": "keyserver1.com:5698"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

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.

Error Code	Description
65536821	The certificate is not installed.
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.
65536870	The key management servers already exist.
65536871	Duplicate key management servers exist.
65536921	Unable to execute the command on the 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.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

node

Name	Type	Description
name	string	
uuid	string	

key_server_state

The connectivity state of the key server for a specific node.

Name	Type	Description
node	node	
state	string	Key server connectivity state

connectivity

This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
cluster_availability	boolean	Set to true when key server connectivity state is available on all nodes of the cluster.
node_states	array[key_server_state]	An array of key server connectivity states for each node.

records

Name	Type	Description
password	string	Password credentials for connecting with the key server. This is not audited.

Name	Type	Description
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 `records` is provided.

key_server

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 `server` is provided.
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 `records` is provided.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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 when 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. • 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 of quorum.
65536700	The key server contains keys that are currently in use and not available from any other configured key server in the SVM.
65536843	The key management server is not configured for the SVM.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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.

Expensive properties

There is an added computational cost to retrieving these properties. They are excluded from default GET results and must be explicitly requested using the `fields` query parameter. For more details, see Requesting specific fields. Additionally, these fields are unavailable for inactive configurations as they are only relevant to active configurations.

- `connectivity.cluster_availability`
- `connectivity.node_states.node.name`
- `connectivity.node_states.node.uuid`
- `connectivity.node_states.state`

Examples

- To retrieve basic information about a key server:

```
GET /security/key-managers/{uuid}/key-servers/{server}
```

- To retrieve specific fields, including expensive properties:

```
GET /security/key-managers/{uuid}/key-
servers/{server}?fields=connectivity.cluster_availability,connectivity.n
ode_states.node.name
```

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	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	

Name	Type	Description
connectivity	connectivity	This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.
create_remove_timeout	integer	The key server timeout for create and remove operations. -1 indicates that the server will wait indefinitely for the event to occur. 0 indicates that the server will not wait and will immediately timeout if it does not receive a response.
password	string	Password credentials for connecting with the key server. This is not audited.
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 `records` is provided.
timeout	integer	I/O timeout in seconds for communicating with the key server. -1 indicates that the server will wait indefinitely for the event to occur. 0 indicates that the server will not wait and will immediately timeout if it does not receive a response.
username	string	KMIP username credentials for connecting with the key server.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "connectivity": {
    "node_states": [
      {
        "node": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "node1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "state": "not_responding"
      }
    ]
  },
  "create_remove_timeout": 60,
  "password": "password",
  "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	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

key_server_state

The connectivity state of the key server for a specific node.

Name	Type	Description
node	node	
state	string	Key server connectivity state

connectivity

This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
cluster_availability	boolean	Set to true when key server connectivity state is available on all nodes of the cluster.
node_states	array[key_server_state]	An array of key server connectivity states for each node.

records

Name	Type	Description
_links	_links	
connectivity	connectivity	This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.
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 `records` 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

returned_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.

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
create_remove_timeout	integer	The key server timeout for create and remove operations. -1 indicates that the server will wait indefinitely for the event to occur. 0 indicates that the server will not wait and will immediately timeout if it does not receive a response.
password	string	Password credentials for connecting with the key server. This is not audited.

Name	Type	Description
secondary_key_servers	array[string]	A list of the secondary key servers associated with the primary key server.
timeout	integer	I/O timeout in seconds for communicating with the key server. -1 indicates that the server will wait indefinitely for the event to occur. 0 indicates that the server will not wait and will immediately timeout if it does not receive a response.
username	string	KMIP username credentials for connecting with the key server.

Example request

```
{
  "create_remove_timeout": 60,
  "password": "password",
  "secondary_key_servers": [
    "secondary1.com",
    "10.1.2.3"
  ],
  "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
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.
65536880	One or more of the following values must be provided "timeout", "username", "password", "secondary_key_servers", "create_remove_timeout".
65536921	Unable to execute the command on the KMIP server.
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.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

node

Name	Type	Description
name	string	
uuid	string	

key_server_state

The connectivity state of the key server for a specific node.

Name	Type	Description
node	node	
state	string	Key server connectivity state

connectivity

This property contains the key server connectivity state of all nodes in the cluster. This is an advanced property; there is an added computational 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.

Name	Type	Description
cluster_availability	boolean	Set to true when key server connectivity state is available on all nodes of the cluster.
node_states	array[key_server_state]	An array of key server connectivity states for each node.

records

Name	Type	Description
password	string	Password credentials for connecting with the key server. This is not audited.

Name	Type	Description
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
create_remove_timeout	integer	The key server timeout for create and remove operations. -1 indicates that the server will wait indefinitely for the event to occur. 0 indicates that the server will not wait and will immediately timeout if it does not receive a response.
password	string	Password credentials for connecting with the key server. This is not audited.
secondary_key_servers	array[string]	A list of the secondary key servers associated with the primary key server.
timeout	integer	I/O timeout in seconds for communicating with the key server. -1 indicates that the server will wait indefinitely for the event to occur. 0 indicates that the server will not wait and will immediately timeout if it does not receive a response.
username	string	KMIP username credentials for connecting with the key server.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage keystores

Manage keystores

Overview

A keystore describes a key-manager configuration, specifically the type of key-manager and whether the configuration is currently enabled for the configured SVM.

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'

# The response:
{
"records": [
  {
    "type": "okm",
    "configuration": {
      "name": "default",
      "uuid": "ec8711c9-4e9f-11ef-b477-005056bb677e"
    },
    "uuid": "ec8711c9-4e9f-11ef-b477-005056bb677e",
```

```
    "enabled": true,
    "location": "onboard",
    "scope": "cluster",
    "state": "active"
  },
  {
    "type": "kmip",
    "configuration": {
      "name": "default",
      "uuid": "d81f43cd-4e9f-11ef-b477-005056bb677e"
    },
    "uuid": "d81f43cd-4e9f-11ef-b477-005056bb677e",
    "enabled": false,
    "location": "external",
    "scope": "cluster"
  },
  {
    "type": "kmip",
    "configuration": {
      "name": "default",
      "uuid": "7da22185-4ea0-11ef-b477-005056bb677e"
    },
    "uuid": "7da22185-4ea0-11ef-b477-005056bb677e",
    "enabled": true,
    "location": "external",
    "scope": "svm",
    "svm": {
      "name": "vs0",
      "uuid": "3cbe691b-4ea0-11ef-b477-005056bb677e"
    },
    "state": "active"
  }
],
"num_records": 3
}
```


Retrieving a specific keystore by its UUID

The following example shows how to retrieve information about a specific keystore.

```
# The API:
GET /api/security/key-stores/{uuid}

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-stores/33421d82-0a8d-11ec-
ae88-005056bb5955?fields=*' -H 'accept: application/hal+json'

# The response:
{
"type": "okm",
"configuration": {
  "name": "default",
  "uuid": "ec8711c9-4e9f-11ef-b477-005056bb677e"
},
"uuid": "ec8711c9-4e9f-11ef-b477-005056bb677e",
"enabled": true,
"location": "onboard",
"scope": "cluster",
"state": "active"
}
```

Enabling a specific keystore configuration

The following example shows how to enable a specific keystore configuration.

```
# The API:
PATCH /api/security/key-stores/{uuid}

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/key-stores/33421d82-0a8d-
11ec-ae88-005056bb5955' -H 'accept: application/hal+json' -d "{
\"enabled\": true }"
```

Deleting a specific keystore configuration

The following example shows how to delete a specific keystore configuration. Only an inactive configuration can be deleted.

```
# The API:
DELETE /api/security/key-stores/{uuid}

# The call:
curl -X DELETE 'https://<mgmt-ip>/api/security/key-stores/33421d82-0a8d-
11ec-ae88-005056bb5955' -H 'accept: application/hal+json'
```

Retrieve keystores

GET `/security/key-stores`

Introduced In: 9.10

Retrieves keystores.

Related ONTAP commands

- `security key-manager show-key-store`
- `security key-manager keystore show`

Parameters

Name	Type	In	Required	Description
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
location	string	query	False	Filter by location
enabled	boolean	query	False	Filter by enabled • Introduced in: 9.14
configuration.name	string	query	False	Filter by configuration.name • Introduced in: 9.14
configuration.uuid	string	query	False	Filter by configuration.uuid • Introduced in: 9.14

Name	Type	In	Required	Description
scope	string	query	False	Filter by scope • Introduced in: 9.14
type	string	query	False	Filter by type
state	string	query	False	Filter by state • Introduced in: 9.16
uuid	string	query	False	Filter by uuid
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
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[security_keystore]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "configuration": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
      },
      "location": "string",
      "scope": "string",
      "state": "string",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "type": "string",
      "uuid": "string"
    }
  ]
}
```


Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
13434920	SVM does not exist.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

configuration

Security keystore object reference.

Name	Type	Description
_links	_links	
name	string	Name of the configuration.
uuid	string	Keystore UUID.

svm

SVM, applies only to SVM-scoped objects.

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

security_keystore

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
location	string	Indicates whether the keystore is onboard or external. * 'onboard' - Onboard Key Database * 'external' - External Key Database, including KMIP and Cloud Key Management Systems
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
state	string	State of the keystore: * 'active' - The key manager is active and serving new and existing keys. * 'mixed' - The key manager has a mixed configuration. New keys can’t be created. * 'svm_kek_rekey' - An SVM key encryption key (KEK) rekey is in progress. New keys can’t be created. * 'blocked' - The key manager is blocked and cannot serve new and existing keys. * 'switching' - Switching the enabled key manager keystore configuration. Some operations are blocked. * 'initializing' - The key manager is being initialized. All operations are blocked. * 'disabling' - The key manager is being disabled. All operations are blocked.
svm	svm	SVM, applies only to SVM-scoped objects.

Name	Type	Description
type	string	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 * 'ikp' - IBM Key Protect Key Management Service * 'barbican' - Barbican Key Management Service
uuid	string	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete an inactive keystore configuration

DELETE `/security/key-stores/{uuid}`

Introduced In: 9.14

Deletes an inactive keystore configuration.

Related ONTAP commands

- `security key-manager keystore delete`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262155	This operation requires an effective cluster version of 9.14.0 or later.
65538905	The keystore configuration is currently enabled and cannot be deleted.
65538907	The method is not yet supported for deleting the given UUID's type of configuration.
65538908	The specified keystore configuration UUID either does not exist or corresponds to a keystore configuration that is not supported by this operation.
65539521	An effective cluster version of ONTAP 9.16.1 or later is required to delete an inactive key manager on the admin SVM.
65539522	This command does not support disabling key manager configurations with the specified keystore type on the admin SVM.
65539593	Cannot delete an inactive key manager configuration while the keystore is in the switching state.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve keystore configuration details with the specified UUID

GET `/security/key-stores/{uuid}`

Introduced In: 9.14

Retrieves details of the keystore configuration with the specified UUID.

Related ONTAP commands

- `security key-manager keystore show`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Keystore configuration UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
location	string	Indicates whether the keystore is onboard or external. * 'onboard' - Onboard Key Database * 'external' - External Key Database, including KMIP and Cloud Key Management Systems
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

Name	Type	Description
state	string	State of the keystore: * 'active' - The key manager is active and serving new and existing keys. * 'mixed' - The key manager has a mixed configuration. New keys can’t be created. * 'svm_kek_rekey' - An SVM key encryption key (KEK) rekey is in progress. New keys can’t be created. * 'blocked' - The key manager is blocked and cannot serve new and existing keys. * 'switching' - Switching the enabled key manager keystore configuration. Some operations are blocked. * 'initializing' - The key manager is being initialized. All operations are blocked. * 'disabling' - The key manager is being disabled. All operations are blocked.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	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 * 'ikp' - IBM Key Protect Key Management Service * 'barbican' - Barbican Key Management Service
uuid	string	

Example response


```
{
  "configuration": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  },
  "location": "string",
  "scope": "string",
  "state": "string",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "string",
  "uuid": "string"
}
```


Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
65539523	Internal error. The keymanager_config table is missing.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

configuration

Security keystore object reference.

Name	Type	Description
_links	_links	
name	string	Name of the configuration.
uuid	string	Keystore UUID.

svm

SVM, applies only to SVM-scoped objects.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Enable a keystore configuration

PATCH `/security/key-stores/{uuid}`

Introduced In: 9.14

Enables a keystore configuration

Related ONTAP commands

- `security key-manager keystore enable`
- `security key-manager keystore disable`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Keystore configuration UUID

Name	Type	In	Required	Description
return_timeout	integer	query	False	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: 0 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
location	string	Indicates whether the keystore is onboard or external. * 'onboard' - Onboard Key Database * 'external' - External Key Database, including KMIP and Cloud Key Management Systems

Name	Type	Description
state	string	State of the keystore: * 'active' - The key manager is active and serving new and existing keys. * 'mixed' - The key manager has a mixed configuration. New keys can’t be created. * 'svm_kek_rekey' - An SVM key encryption key (KEK) rekey is in progress. New keys can’t be created. * 'blocked' - The key manager is blocked and cannot serve new and existing keys. * 'switching' - Switching the enabled key manager keystore configuration. Some operations are blocked. * 'initializing' - The key manager is being initialized. All operations are blocked. * 'disabling' - The key manager is being disabled. All operations are blocked.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	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 * 'ikp' - IBM Key Protect Key Management Service * 'barbican' - Barbican Key Management Service
uuid	string	

Example request


```
{
  "configuration": {
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
  },
  "location": "string",
  "state": "string",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "string",
  "uuid": "string"
}
```


Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "uuid": "string"
  }
}
```


Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262155	This operation requires an effective cluster version of 9.14.0 or later.
65536203	Internal error. Failed to generate SVM key. Cluster key database is not initialized.
65536204	Internal error. Failed to generate SVM key. Cluster key encryption key is not found.
65536207	Internal error. Failed to store SVM key.
65536212	Internal error. Failed to delete SVM volume key.
65536217	Internal error. Failed to delete key from cryptomod.
65536602	Cannot perform enable/switch while nodes are out of quorum.
65536856	No external key management server configured for SVM.
65536882	Internal error. UUID is missing for the volume.
65536883	Internal error. Volume encryption key is missing.
65536884	Internal error. Volume encryption key is invalid for the volume.
65536889	Internal error. The volume has an invalid encryption blob.
65536890	Internal error. Failed to generate VDEK blob.
65536973	Internal error. Volume DSID is missing for the volume.
65536987	One or more key servers are unavailable.
65537527	Internal error. Failed to rewrap SVM key encryption key.
65537533	Internal error. Failed to unwrap SVM key encryption key.
65537605	Failed to establish connectivity with the cloud key management service.
65538908	The specified keystore configuration UUID either does not exist or corresponds to a keystore configuration that is not supported by this operation.
65538909	A value for enabled is required.
65538910	Disabling an enabled configuration through this method is currently not supported.
65539200	The key custodian was not provided with an external key value store.
65539201	Failed to encrypt.

Error Code	Description
65539205	This command does not support enabling key manager configurations with the specified keystore type.
65539206	The SVM associated with the supplied keystore UUID already has a keystore configuration enabled. This command does not support migrating from configurations of that keystore type".
65539207	The specified keystore configuration does not exist.
65539212	Cannot switch the enabled keystore configuration when it is not in the 'active' or 'switching' state.
65539218	The specified keystore configuration is already enabled.
65539222	Switching between configurations of different keystore types is not supported for data SVMs.
65539416	Internal error. Failed to parse key value store response.
65539442	Internal error. Failed to generate AES blob.
65539444	Internal error. Failed to update the VDEK blob.
65539513	An effective cluster version of ONTAP 9.16.1 or later is required to enable an inactive key manager on the admin SVM.
65539514	This command does not support enabling key manager configurations with the specified keystore type on the admin SVM.
65539515	Cannot switch keystore types on the admin SVM. The keystore type for the invalid configuration must be OKM and the enabled configuration must be KMIP, or vice versa.
65539518	Internal error. Cannot find the enabled configuration.
65539520	Cannot enable the Onboard Key Manager on the admin SVM because an inactive Onboard Key Manager already exists on the admin SVM.
65539534	Cannot switch admin SVM Key Manager when system root volumes are present.
65539535	Failed to find unwrapped key on any nodes.
65539536	Internal error. Failed to find the existing wrapped key blob for the volume.
65539538	SVM-KEK not created for the SVM.
65539539	SVM-KEK not restored for SVM.
65539583	Cannot switch to the Onboard Key Manager when the external key manager has a policy associated with it

Error Code	Description
65539585	Cannot enable an external key manager on the admin SVM because an inactive external key manager already exists on the admin SVM.
65539590	Cannot switch to the Onboard Key Manager if there are more than two NSE-AKs in the cluster.
65539591	Cannot switch to the Onboard Key Manager if there are fewer than two NSE-AKs in the cluster.
65539704	The key manager cannot be configured because the SVM has NAE volumes.
65539837	The key manager configured does not have any volumes to migrate.
65539838	Cannot migrate to a cloud key manager when the external key manager has a policy associated with it.
65539839	Cannot migrate to a cloud key manager when the key manager is not in a mixed state.
65539840	Failed to clean up the keys stored on the external key servers.
65539842	Failed to restore the SVM-KEK.
65539845	Cannot migrate SVM volumes to the Onboard Key Manager when the key manager is not in the mixed or active state.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

configuration

Security keystore object reference.

Name	Type	Description
name	string	Name of the configuration.
uuid	string	Keystore UUID.

svm

SVM, applies only to SVM-scoped objects.

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

security_keystore

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
location	string	Indicates whether the keystore is onboard or external. * 'onboard' - Onboard Key Database * 'external' - External Key Database, including KMIP and Cloud Key Management Systems

Name	Type	Description
state	string	State of the keystore: * 'active' - The key manager is active and serving new and existing keys. * 'mixed' - The key manager has a mixed configuration. New keys can’t be created. * 'svm_kek_rekey' - An SVM key encryption key (KEK) rekey is in progress. New keys can’t be created. * 'blocked' - The key manager is blocked and cannot serve new and existing keys. * 'switching' - Switching the enabled key manager keystore configuration. Some operations are blocked. * 'initializing' - The key manager is being initialized. All operations are blocked. * 'disabling' - The key manager is being disabled. All operations are blocked.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	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 * 'ikp' - IBM Key Protect Key Management Service * 'barbican' - Barbican Key Management Service
uuid	string	

job_link

Name	Type	Description
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

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage security login messages

Manage security login messages

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: application/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: application/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: application/json" -d "{ \"banner\": \"\", \"message\": \"\"
}"
```

Retrieve the login banner and messages of the day

GET `/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

Name	Type	In	Required	Description
uuid	string	query	False	Filter by uuid
message	string	query	False	Filter by message • maxLength: 2048 • minLength: 0
banner	string	query	False	Filter by banner • maxLength: 2048 • minLength: 0
scope	string	query	False	Filter by scope
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
show_cluster_message	boolean	query	False	Filter by show_cluster_message

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
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[login_messages]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "banner": "string",
      "message": "string",
      "scope": "string",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "uuid": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

svm

SVM, applies only to SVM-scoped objects.

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

login_messages

The login banner and message of the day (MOTD) configuration.

Name	Type	Description
_links	_links	

Name	Type	Description
banner	string	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	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	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
show_cluster_message	boolean	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 cluster administrators. Optional in the PATCH body.
svm	svm	SVM, applies only to SVM-scoped objects.

Name	Type	Description
uuid	string	The unique identifier (ID) of the login messages configuration.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a login message configuration by UUID

GET `/security/login/messages/{uuid}`

Introduced In: 9.6

Retrieves the login messages configuration by UUID.

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Login messages configuration UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
banner	string	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	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	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
show_cluster_message	boolean	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 cluster administrators. Optional in the PATCH body.

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	The unique identifier (ID) of the login messages configuration.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "banner": "string",
  "message": "string",
  "scope": "string",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

svm

SVM, applies only to SVM-scoped objects.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update a login message configuration

PATCH `/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

Name	Type	In	Required	Description
uuid	string	path	True	Login messages configuration UUID

Request Body

Name	Type	Description
banner	string	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	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.

Name	Type	Description
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
show_cluster_message	boolean	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 cluster administrators. Optional in the PATCH body.
uuid	string	The unique identifier (ID) of the login messages configuration.

Example request

```
{
  "banner": "string",
  "message": "string",
  "scope": "string",
  "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.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

SVM, applies only to SVM-scoped objects.

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

login_messages

The login banner and message of the day (MOTD) configuration.

Name	Type	Description
banner	string	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.

Name	Type	Description
message	string	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	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
show_cluster_message	boolean	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 cluster administrators. Optional in the PATCH body.
uuid	string	The unique identifier (ID) of the login messages configuration.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

View and create TOTP profiles

View and create TOTP profiles

Overview

This API configures the TOTP(Time based OTP) profile for user accounts for secure shell (SSH) access. Prerequisites: You must configure TOTP as a secondary authentication method in /security/accounts when creating users. You must have a TOTP application that you can use to get TOTP keys. You are only allowed to create a TOTP profile for yourself, not for others. Admin cannot create TOTP profiles for any users.

Examples

Creating a TOTP profile for cluster-scoped user accounts

Specify the user account name 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/login/totps"

# The call:
curl -k https://<mgmt-ip>/api/security/login/totps --request POST --data
'{ "account": { "name": "pubuser2" },"comment": "Cserver-Creation"}'

# The response:
{
"num_records": 1,
"records": [
{
  "owner": {
    "uuid": "b009a9e7-4081-b576-7575-ada21efcaf16",
    "name": "Default",
    "_links": {
      "self": {
        "href": "/api/svm/svms/b009a9e7-4081-b576-7575-ada21efcaf16"
      }
    }
  },
```

```
  "account": {
    "name": "pubuser2"
  },
  "secret_key": "<ACCOUNT-TOTP-SECRET-KEY>"
  "install_url":
"https://www.google.com/chart?chs=200x200&chld=M&#124;0&cht=qr&chl=otpauth
://totp/root@node1%3Fsecret%3DDRY5CAJGTQCL5TV4D3UAMYXJFM%26issuer%3Dnode1"
,
  "verification_code": "946090",
  "emergency_codes": [
    "54200192",
    "10418385",
    "52726505",
    "41704451",
    "20744310"
  ],
  "_links": {
    "self": {
      "href": "/api/security/login/totps/b009a9e7-4081-b576-7575-
ada21efcaf16/pubuser2"
    }
  }
}
 ]
}
```

Creating a TOTP profile for SVM-scoped user accounts

For an 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 TOTP profile 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/login/totps"

# The call:
curl -k https://<mgmt-ip>/api/security/login/totps --request POST --data
'{ "account": { "name": "pubuser4" },"comment": "Vserver-
Creation","owner.name":"vs0" }'

# The response:
{
"num_records": 1,
"records": [
{
```

```
  "owner": {
    "uuid": "b019a9e7-4081-b576-7575-ada21efcaf16",
    "name": "vs0",
    "_links": {
      "self": {
        "href": "/api/svm/svms/b019a9e7-4081-b576-7575-ada21efcaf16"
      }
    }
  },
  "account": {
    "name": "pubuser4"
  },
  "secret_key": "<ACCOUNT-TOTP-SECRET-KEY>",
  "install_url":
"https://www.google.com/chart?chs=200x200&chld=M&#124;0&cht=qr&chl=otpauth
://totp/root@node1%3Fsecret%3DDRY5CAJGTQCL5TV4D3UAMYXJFM%26issuer%3Dnode1"
,
  "verification_code": "946090",
  "emergency_codes": [
    "54200192",
    "10418385",
    "52726505",
    "41704451",
    "20744310"
  ],
  "_links": {
    "self": {
      "href": "/api/security/login/totps/b019a9e7-4081-b576-7575-
ada21efcaf16/pubuser4"
    }
  }
}
 ]
}
```

Retrieving the configured TOTP profile for user accounts

Retrieves the TOTP profiles associated with the user accounts or a filtered list (for a specific user account name, a specific SVM and so on).

```
# The API:
GET "/api/security/login/totps"

# The call to retrieve TOTP profiles associated with TOTP configured user
accounts in the cluster:
curl -k https://<mgmt-ip>/api/security/login/totps

# the response:
{
"records": [
{
  "owner": {
    "uuid": "b009a9e7-4081-b576-7575-ada21efcaf16",
    "name": "Default",
    "_links": {
      "self": {
        "href": "/api/svm/svms/b009a9e7-4081-b576-7575-ada21efcaf16"
      }
    }
  },
  "account": {
    "name": "pubuser2",
    "_links": {
      "self": {
        "href": "/api/security/accounts/b009a9e7-4081-b576-7575-
ada21efcaf16/pubuser2"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/security/login/totps/b009a9e7-4081-b576-7575-
ada21efcaf16/pubuser2"
    }
  }
}
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/security/login/totps"
  }
}
}
```

Retrieve TOTP profiles configured for user accounts

GET `/security/login/totps`

Introduced In: 9.13

Retrieves the TOTP profiles configured for user accounts.

Related ONTAP commands

- `security login totp show`

Learn more

- DOC /security/login/totps
- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
owner.name	string	query	False	Filter by owner.name
owner.uuid	string	query	False	Filter by owner.uuid
enabled	boolean	query	False	Filter by enabled
comment	string	query	False	Filter by comment
account.name	string	query	False	Filter by account.name
sha_fingerprint	string	query	False	Filter by sha_fingerprint
scope	string	query	False	Filter by scope
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records.
records	array[totp]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "account": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "joe.smith"
      },
      "comment": "string",
      "enabled": "",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "scope": "string",
      "sha_fingerprint": "string"
    }
  ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

account_reference

Name	Type	Description
_links	_links	
name	string	User account

owner

Owner name and UUID that uniquely identifies the TOTP profile.

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

totp

TOTP profile for the user account used to access SSH.

Name	Type	Description
_links	_links	

Name	Type	Description
account	account_reference	
comment	string	Optional comment for the TOTP profile.
enabled	boolean	Status of the TOTP profile.
owner	owner	Owner name and UUID that uniquely identifies the TOTP profile.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
sha_fingerprint	string	SHA fingerprint for the TOTP secret key.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create the TOTP profile for a user account

POST `/security/login/totps`

Introduced In: 9.13

Creates a TOTP profile for a user account.

Required properties

- `owner.uuid` - Account owner UUID.
- `account.name` - Account user name.

Related ONTAP commands

- `security login totp create`

Learn more

- DOC /security/login/totps
- DOC /security/accounts

Parameters

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

Request Body

Name	Type	Description
account	account_reference	
comment	string	Optional comment for the TOTP profile.
owner	owner	Owner name and UUID that uniquely identifies the TOTP profile.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
sha_fingerprint	string	SHA fingerprint for the TOTP secret key.

Example request

```
{
  "account": {
    "name": "joe.smith"
  },
  "comment": "string",
  "enabled": "",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "string",
  "sha_fingerprint": "string"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records.
records	array[totp_post]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "account": {
        "name": "joe.smith"
      },
      "comment": "string",
      "emergency_codes": "17503785",
      "enabled": 1,
      "install_url": "string",
      "owner": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "scope": "string",
      "secret_key": "string",
      "sha_fingerprint": "string",
      "verification_code": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
144834561	TOTP is not configured for the user.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

account_reference

Name	Type	Description
name	string	User account

owner

Owner name and UUID that uniquely identifies the TOTP profile.

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

totp

TOTP profile for the user account used to access SSH.

Name	Type	Description
account	account_reference	
comment	string	Optional comment for the TOTP profile.
owner	owner	Owner name and UUID that uniquely identifies the TOTP profile.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Name	Type	Description
sha_fingerprint	string	SHA fingerprint for the TOTP secret key.

totp_post

Response object of the TOTP profile creation.

Name	Type	Description
account	account_reference	
comment	string	Optional comment for the TOTP profile.
emergency_codes	array[string]	TOTP profile emergency codes for a user. These codes are for emergency use when a user cannot access 2FA codes through other means.
install_url	string	TOTP profile installation URL for a user.
owner	owner	Owner name and UUID that uniquely identifies the TOTP profile.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
secret_key	string	TOTP profile secret key for a user.
sha_fingerprint	string	SHA fingerprint for the TOTP secret key.
verification_code	string	TOTP profile verification code for a user.

error_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage TOTP profiles

Manage TOTP profiles

Overview

This API configures the TOTP profile for user accounts. Specify the owner UUID and the account user name. The owner UUID corresponds to the UUID of the SVM containing the user account associated with the TOTP profile and can be obtained from the response body of the GET request performed on the API "`/api/svm/svms".

Examples

Retrieving the specific configured TOTP profile for user accounts

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

# The call:
curl -k https://<mgmt-ip>/api/security/login/totps/513a78c7-8c13-11e9-
8f78-005056bbf6ac/pubuser4

# the response:
{
"owner": {
    "uuid": "b009a9e7-4081-b576-7575-ada21efcaf16",
    "name": "Default",
  "_links": {
    "self": {
      "href": "/api/svm/svms/b009a9e7-4081-b576-7575-ada21efcaf16"
    }
  }
},
"account": {
  "name": "pubuser2",
  "_links": {
    "self": {
      "href": "/api/security/accounts/b009a9e7-4081-b576-7575-
ada21efcaf16/pubuser2"
    }
  }
},
"sha_fingerprint":
"21364f5417600e3d9d6a7ac6c05dd244aed9f15dce6786a2c89399a41ff0fdb0",
"scope": "cluster",
"_links": {
  "self": {
    "href": "/api/security/login/totps/b009a9e7-4081-b576-7575-
ada21efcaf16/pubuser2"
  }
}
}
```

Modifying the TOTP profile for a user account

```
# The API:
PATCH "/api/security/login/totps/{owner.uuid}/{account.name}"

# The call:
curl -k "https://<mgmt-ip>/api/security/login/totps/6865196a-8b59-11ed-
874c-0050568e36ed/ysadmin" --request PATCH --data "{  \"comment\":
\"Testing\",  \"enabled\": false}"

# the response:
{}
```

Deleting the TOTP profile for user accounts

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

# The call:
curl -k https://<mgmt-ip>/api/security/login/totps/d49de271-8c11-11e9-
8f78-005056bbf6ac/pubuser1 --request DELETE

# the response:
{}
```

Delete the TOTP profile for a user account

DELETE `/security/login/totps/{owner.uuid}/{account.name}`

Introduced In: 9.13

Deletes the TOTP profile for a user account.

Related ONTAP commands

- `security login totp delete`

Learn more

- DOC /security/login/totps/{owner.uuid}/{account.name}
- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID.

Name	Type	In	Required	Description
account.name	string	path	True	Account user name.

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the TOTP profile for a user account

GET `/security/login/totps/{owner.uuid}/{account.name}`

Introduced In: 9.13

Retrieves the TOTP profile configured for a user account.

Related ONTAP commands

- `security login totp show`

Learn more

- DOC /security/login/totps/{owner.uuid}/{account.name}
- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID.
account.name	string	path	True	Account user name.

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
account	account_reference	
comment	string	Optional comment for the TOTP profile.
enabled	boolean	Status of the TOTP profile.
owner	owner	Owner name and UUID that uniquely identifies the TOTP profile.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
sha_fingerprint	string	SHA fingerprint for the TOTP secret key.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "account": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "comment": "string",
  "enabled": "",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "string",
  "sha_fingerprint": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

account_reference

Name	Type	Description
_links	_links	
name	string	User account

owner

Owner name and UUID that uniquely identifies the TOTP profile.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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 TOTP profile for a user account

PATCH `/security/login/totps/{owner.uuid}/{account.name}`

Introduced In: 9.13

Updates a TOTP user account.

Related ONTAP commands

- `security login totp modify`

Learn more

- DOC /security/login/totps/{owner.uuid}/{account.name}
- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID
account.name	string	path	True	User account name

Request Body

Name	Type	Description
comment	string	Optional comment for the TOTP profile.
enabled	boolean	Status of the TOTP profile.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Name	Type	Description
sha_fingerprint	string	SHA fingerprint for the TOTP secret key.

Example request

```
{
  "comment": "string",
  "enabled": "",
  "scope": "string",
  "sha_fingerprint": "string"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
144834564	Only users with the admin role are allowed to modify the TOTP status.
144834565	Invalid option for the field -enabled
144834566	The user does not have a TOTP configuration available for modification.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

account_reference

Name	Type	Description
name	string	User account

owner

Owner name and UUID that uniquely identifies the TOTP profile.

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

totp

TOTP profile for the user account used to access SSH.

Name	Type	Description
comment	string	Optional comment for the TOTP profile.
enabled	boolean	Status of the TOTP profile.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
sha_fingerprint	string	SHA fingerprint for the TOTP secret key.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage the multi-admin-verify global setting

Manage the multi-admin-verify global setting

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. Note it is recommended that multi-admin-verify is enabled equally on peered ONTAP clusters.

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. Note that the total number of approvers in an approval group must be a positive integer more than the number of required approvers. For example, if there are a total of 10 approvers in a group, the required approvers can be set between 1 and 9.

```
# 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"}'
```

Retrieve a multi-admin-verify configuration

GET `/security/multi-admin-verify`

Introduced In: 9.11

Retrieves the multi-admin-verify configuration.

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
approval_expiry	string	Default time for requests to be approved, in ISO-8601 duration format.
approval_groups	array[string]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.
enabled	boolean	
execution_expiry	string	Default time for requests to be executed once approved, in ISO-8601 duration format.
required_approvers	integer	The number of required approvers, excluding the user that made the request.

Example response


```
{
  "approval_expiry": "string",
  "approval_groups": [
    "string"
  ],
  "execution_expiry": "string"
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Modify a multi-admin-verify configuration

PATCH `/security/multi-admin-verify`

Introduced In: 9.11

Modifies the multi-admin-verify configuration.

Request Body

Name	Type	Description
approval_expiry	string	Default time for requests to be approved, in ISO-8601 duration format.
approval_groups	array[string]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.
enabled	boolean	

Name	Type	Description
execution_expiry	string	Default time for requests to be executed once approved, in ISO-8601 duration format.
required_approvers	integer	The number of required approvers, excluding the user that made the request.

Example request

```
{
  "approval_expiry": "string",
  "approval_groups": [
    "string"
  ],
  "execution_expiry": "string"
}
```

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.
262314	One or more approval groups added do not exist.

Error Code	Description
262315	Approval-groups must be specified when enabling this feature.
262316	Value must be in the range two minutes to two weeks.
262318	multi-admin-verify requires an effective cluster version of ONTAP 9.11.1 or later.

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

Definitions

See Definitions

multi_admin_verify_config

Name	Type	Description
approval_expiry	string	Default time for requests to be approved, in ISO-8601 duration format.
approval_groups	array[string]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.
enabled	boolean	
execution_expiry	string	Default time for requests to be executed once approved, in ISO-8601 duration format.
required_approvers	integer	The number of required approvers, excluding the user that made the request.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View and create multi-admin-verify approval groups

View and create multi-admin-verify approval groups

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 '{"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"
  }
}
}
```

Retrieve multi-admin-verify approval groups

GET `/security/multi-admin-verify/approval-groups`

Introduced In: 9.11

Retrieves multi-admin-verify approval groups.

Parameters

Name	Type	In	Required	Description
email	string	query	False	Filter by email
approvers	string	query	False	Filter by approvers
owner.name	string	query	False	Filter by owner.name
owner.uuid	string	query	False	Filter by owner.uuid
name	string	query	False	Filter by name
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0

Name	Type	In	Required	Description
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[multi_admin_verify_approval_group]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "approvers": [
        "string"
      ],
      "email": [
        "string"
      ],
      "name": "string",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

owner

The owner of the approval group. The only valid owner is currently the cluster.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a POST or PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

multi_admin_verify_approval_group

Name	Type	Description
approvers	array[string]	List of users that can approve a request.
email	array[string]	Email addresses that are notified when a request is created, approved, vetoed, or executed.
name	string	Name of the approval group.

Name	Type	Description
owner	owner	The owner of the approval group. The only valid owner is currently the cluster.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a multi-admin-verify approval group

POST `/security/multi-admin-verify/approval-groups`

Introduced In: 9.11

Creates a multi-admin-verify approval group.

Parameters

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

Request Body

Name	Type	Description
approvers	array[string]	List of users that can approve a request.
email	array[string]	Email addresses that are notified when a request is created, approved, vetoed, or executed.
name	string	Name of the approval group.
owner	owner	The owner of the approval group. The only valid owner is currently the cluster.

Example request

```
{
  "approvers": [
    "string"
  ],
  "email": [
    "string"
  ],
  "name": "string",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[multi_admin_verify_approval_group]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "approvers": [
        "string"
      ],
      "email": [
        "string"
      ],
      "name": "string",
      "owner": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262309	The feature must be enabled first.
262333	Invalid user in approval group.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

owner

The owner of the approval group. The only valid owner is currently the cluster.

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

multi_admin_verify_approval_group

Name	Type	Description
approvers	array[string]	List of users that can approve a request.
email	array[string]	Email addresses that are notified when a request is created, approved, vetoed, or executed.
name	string	Name of the approval group.
owner	owner	The owner of the approval group. The only valid owner is currently the cluster.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage multi-admin-verify approval groups

Manage multi-admin-verify approval groups

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"
```

Delete a multi-admin-verify approval group

DELETE `/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}`

Introduced In: 9.11

Deletes a multi-admin-verify approval group.

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	
name	string	path	True	

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262319	Cannot delete an approval group that is in the list of global approval groups.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a multi-admin-verify approval group

GET `/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}`

Introduced In: 9.11

Retrieves a multi-admin-verify approval group.

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	
name	string	path	True	
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
approvers	array[string]	List of users that can approve a request.
email	array[string]	Email addresses that are notified when a request is created, approved, vetoed, or executed.
name	string	Name of the approval group.
owner	owner	The owner of the approval group. The only valid owner is currently the cluster.

Example response


```
{
  "approvers": [
    "string"
  ],
  "email": [
    "string"
  ],
  "name": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

owner

The owner of the approval group. The only valid owner is currently the cluster.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a POST or PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update a multi-admin-verify approval group

PATCH `/security/multi-admin-verify/approval-groups/{owner.uuid}/{name}`

Introduced In: 9.11

Updates a multi-admin-verify approval group.

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	
name	string	path	True	

Request Body

Name	Type	Description
approvers	array[string]	List of users that can approve a request.
email	array[string]	Email addresses that are notified when a request is created, approved, vetoed, or executed.
owner	owner	The owner of the approval group. The only valid owner is currently the cluster.

Example request

```
{
  "approvers": [
    "string"
  ],
  "email": [
    "string"
  ],
  "owner": {
    "name": "svm1"
  }
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262331	At least one approver is required.
262332	An add or remove list is required.
262333	Invalid user in approval group.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

owner

The owner of the approval group. The only valid owner is currently the cluster.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a POST or PATCH method.

multi_admin_verify_approval_group

Name	Type	Description
approvers	array[string]	List of users that can approve a request.
email	array[string]	Email addresses that are notified when a request is created, approved, vetoed, or executed.
owner	owner	The owner of the approval group. The only valid owner is currently the cluster.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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.

Manage multi-admin-verify approval requests

Manage multi-admin-verify approval requests

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,
    "execute_on_approval": false,
    "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"
  }
}
}
```

Retrieve multi-admin-verify requests

GET `/security/multi-admin-verify/requests`

Introduced In: 9.11

Retrieves multi-admin-verify requests.

Parameters

Name	Type	In	Required	Description
operation	string	query	False	Filter by operation
user_requested	string	query	False	Filter by user_requested
state	string	query	False	Filter by state
execution_expiry_time	string	query	False	Filter by execution_expiry_time
execute_on_approval	boolean	query	False	Filter by execute_on_approval • Introduced in: 9.13
comment	string	query	False	Filter by comment
permitted_users	string	query	False	Filter by permitted_users
pending_approvers	integer	query	False	Filter by pending_approvers
approve_time	string	query	False	Filter by approve_time
user_vetoed	string	query	False	Filter by user_vetoed
create_time	string	query	False	Filter by create_time
query	string	query	False	Filter by query
index	integer	query	False	Filter by index
owner.name	string	query	False	Filter by owner.name

Name	Type	In	Required	Description
owner.uuid	string	query	False	Filter by owner.uuid
potential_approvers	string	query	False	Filter by potential_approvers
required_approvers	integer	query	False	Filter by required_approvers
approve_expiry_time	string	query	False	Filter by approve_expiry_time
approved_users	string	query	False	Filter by approved_users
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0

Name	Type	In	Required	Description
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[multi_admin_verify_request]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "approve_expiry_time": "string",
      "approve_time": "string",
      "approved_users": [
        "string"
      ],
      "comment": "string",
      "create_time": "string",
      "execution_expiry_time": "string",
      "index": 0,
      "operation": "string",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "pending_approvers": 0,
      "permitted_users": [
        "string"
      ],
      "potential_approvers": [
        "string"
      ],
      "query": "string",
      "required_approvers": 0,
      "state": "string",
      "user_requested": "string",
      "user_vetoed": "string"
    }
```

```
  ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

owner

The owner of the request. This can identify the cluster or an SVM.

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

multi_admin_verify_request

Name	Type	Description
approve_expiry_time	string	
approve_time	string	
approved_users	array[string]	The users that have approved the request.
comment	string	Optional user-provided comment that is sent to the approval-group email indicating why the request was made.

Name	Type	Description
create_time	string	
execute_on_approval	boolean	Specifies that the operation is executed automatically on final approval.
execution_expiry_time	string	
index	integer	Unique index that represents a request.
operation	string	The command to execute.
owner	owner	The owner of the request. This can identify the cluster or an SVM.
pending_approvers	integer	The number of approvers remaining that are required to approve.
permitted_users	array[string]	List of users that can execute the operation once approved. If not set, any authorized user can perform the operation.
potential_approvers	array[string]	The users that are able to approve the request.
query	string	Identifies the specific entry upon which the user wants to operate.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
state	string	The state of the request. PATCH supports approved and vetoed. The state only changes after setting to approved once no more approvers are required.

Name	Type	Description
user_requested	string	The user that created the request. Automatically set by ONTAP. • readOnly: 1 • Introduced in: 9.11 • x-nullable: true
user_vetoed	string	The user that vetoed the request.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a multi-admin-verify request

POST `/security/multi-admin-verify/requests`

Introduced In: 9.11

Creates a multi-admin-verify request.

Parameters

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

Request Body

Name	Type	Description
approve_expiry_time	string	
approve_time	string	
approved_users	array[string]	The users that have approved the request.
comment	string	Optional user-provided comment that is sent to the approval-group email indicating why the request was made.
create_time	string	
execution_expiry_time	string	
index	integer	Unique index that represents a request.
operation	string	The command to execute.
owner	owner	The owner of the request. This can identify the cluster or an SVM.
pending_approvers	integer	The number of approvers remaining that are required to approve.
permitted_users	array[string]	List of users that can execute the operation once approved. If not set, any authorized user can perform the operation.
potential_approvers	array[string]	The users that are able to approve the request.
query	string	Identifies the specific entry upon which the user wants to operate.

Name	Type	Description
required_approvers	integer	The number of required approvers, excluding the user that made the request.
state	string	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	The user that created the request. Automatically set by ONTAP. • readOnly: 1 • Introduced in: 9.11 • x-nullable: true
user_vetoed	string	The user that vetoed the request.

Example request


```
{
  "approve_expiry_time": "string",
  "approve_time": "string",
  "approved_users": [
    "string"
  ],
  "comment": "string",
  "create_time": "string",
  "execute_on_approval": true,
  "execution_expiry_time": "string",
  "index": 0,
  "operation": "string",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "pending_approvers": 0,
  "permitted_users": [
    "string"
  ],
  "potential_approvers": [
    "string"
  ],
  "query": "string",
  "required_approvers": 0,
  "state": "string",
  "user_requested": "string",
  "user_vetoed": "string"
}
```


Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[multi_admin_verify_request]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "approve_expiry_time": "string",
      "approve_time": "string",
      "approved_users": [
        "string"
      ],
      "comment": "string",
      "create_time": "string",
      "execute_on_approval": true,
      "execution_expiry_time": "string",
      "index": 0,
      "operation": "string",
      "owner": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "pending_approvers": 0,
      "permitted_users": [
        "string"
      ],
      "potential_approvers": [
        "string"
      ],
      "query": "string",
      "required_approvers": 0,
      "state": "string",
      "user_requested": "string",
      "user_vetoed": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262148	The specified command is not recognized.
262279	Invalid field set.
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.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

owner

The owner of the request. This can identify the cluster or an SVM.

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

multi_admin_verify_request

Name	Type	Description
approve_expiry_time	string	
approve_time	string	
approved_users	array[string]	The users that have approved the request.
comment	string	Optional user-provided comment that is sent to the approval-group email indicating why the request was made.
create_time	string	
execution_expiry_time	string	
index	integer	Unique index that represents a request.
operation	string	The command to execute.
owner	owner	The owner of the request. This can identify the cluster or an SVM.

Name	Type	Description
pending_approvers	integer	The number of approvers remaining that are required to approve.
permitted_users	array[string]	List of users that can execute the operation once approved. If not set, any authorized user can perform the operation.
potential_approvers	array[string]	The users that are able to approve the request.
query	string	Identifies the specific entry upon which the user wants to operate.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
state	string	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	The user that created the request. Automatically set by ONTAP. • readOnly: 1 • Introduced in: 9.11 • x-nullable: true
user_vetoed	string	The user that vetoed the request.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage a multi-admin-verify approval request

Manage a multi-admin-verify approval request

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,
"execute_on_approval": false,
"permitted_users": [
  "example_user"
],
"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", "execute_on_approval":
false}'
```

Delete a multi-admin-verify request

DELETE `/security/multi-admin-verify/requests/{index}`

Introduced In: 9.11

Deletes a multi-admin-verify request.

Parameters

Name	Type	In	Required	Description
index	string	path	True	

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262336	User not authorized to delete the request.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a multi-admin-verify request

GET `/security/multi-admin-verify/requests/{index}`

Introduced In: 9.11

Retrieves a multi-admin-verify request.

Parameters

Name	Type	In	Required	Description
index	string	path	True	
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
approve_expiry_time	string	
approve_time	string	
approved_users	array[string]	The users that have approved the request.
comment	string	Optional user-provided comment that is sent to the approval-group email indicating why the request was made.
create_time	string	
execute_on_approval	boolean	Specifies that the operation is executed automatically on final approval.
execution_expiry_time	string	
index	integer	Unique index that represents a request.
operation	string	The command to execute.
owner	owner	The owner of the request. This can identify the cluster or an SVM.
pending_approvers	integer	The number of approvers remaining that are required to approve.

Name	Type	Description
permitted_users	array[string]	List of users that can execute the operation once approved. If not set, any authorized user can perform the operation.
potential_approvers	array[string]	The users that are able to approve the request.
query	string	Identifies the specific entry upon which the user wants to operate.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
state	string	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	The user that created the request. Automatically set by ONTAP. • readOnly: 1 • Introduced in: 9.11 • x-nullable: true
user_vetoed	string	The user that vetoed the request.

Example response


```
{
  "approve_expiry_time": "string",
  "approve_time": "string",
  "approved_users": [
    "string"
  ],
  "comment": "string",
  "create_time": "string",
  "execution_expiry_time": "string",
  "index": 0,
  "operation": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "pending_approvers": 0,
  "permitted_users": [
    "string"
  ],
  "potential_approvers": [
    "string"
  ],
  "query": "string",
  "required_approvers": 0,
  "state": "string",
  "user_requested": "string",
  "user_vetoed": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

owner

The owner of the request. This can identify the cluster or an SVM.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update a multi-admin-verify request

PATCH `/security/multi-admin-verify/requests/{index}`

Introduced In: 9.11

Updates a multi-admin-verify request.

Parameters

Name	Type	In	Required	Description
index	string	path	True	

Request Body

Name	Type	Description
approve_expiry_time	string	
approve_time	string	
approved_users	array[string]	The users that have approved the request.
create_time	string	
execute_on_approval	boolean	Specifies that the operation is executed automatically on final approval.
execution_expiry_time	string	
index	integer	Unique index that represents a request.
owner	owner	The owner of the request. This can identify the cluster or an SVM.
pending_approvers	integer	The number of approvers remaining that are required to approve.
potential_approvers	array[string]	The users that are able to approve the request.
required_approvers	integer	The number of required approvers, excluding the user that made the request.

Name	Type	Description
state	string	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	The user that created the request. Automatically set by ONTAP. • readOnly: 1 • Introduced in: 9.11 • x-nullable: true
user_vetoed	string	The user that vetoed the request.

Example request


```
{
  "approve_expiry_time": "string",
  "approve_time": "string",
  "approved_users": [
    "string"
  ],
  "create_time": "string",
  "execution_expiry_time": "string",
  "index": 0,
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "pending_approvers": 0,
  "potential_approvers": [
    "string"
  ],
  "required_approvers": 0,
  "state": "string",
  "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. State can be modified to approved, vetoed, or executed.
262337	User not eligible to approve the request.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

owner

The owner of the request. This can identify the cluster or an SVM.

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

multi_admin_verify_request

Name	Type	Description
approve_expiry_time	string	
approve_time	string	
approved_users	array[string]	The users that have approved the request.
create_time	string	
execute_on_approval	boolean	Specifies that the operation is executed automatically on final approval.
execution_expiry_time	string	
index	integer	Unique index that represents a request.
owner	owner	The owner of the request. This can identify the cluster or an SVM.

Name	Type	Description
pending_approvers	integer	The number of approvers remaining that are required to approve.
potential_approvers	array[string]	The users that are able to approve the request.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
state	string	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	The user that created the request. Automatically set by ONTAP. • readOnly: 1 • Introduced in: 9.11 • x-nullable: true
user_vetoed	string	The user that vetoed the request.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message

Name	Type	Description
target	string	The target parameter that caused the error.

Manage multi-admin-verify rules

Manage multi-admin-verify rules

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
'{"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"
  }
}
}
```


Retrieve multi-admin-verify rules

GET `/security/multi-admin-verify/rules`

Introduced In: 9.11

Retrieves multi-admin-verify rules.

Parameters

Name	Type	In	Required	Description
create_time	string	query	False	Filter by create_time
system_defined	boolean	query	False	Filter by system_defined
auto_request_create	boolean	query	False	Filter by auto_request_create
operation	string	query	False	Filter by operation
query	string	query	False	Filter by query
approval_groups.name	string	query	False	Filter by approval_groups.name
execution_expiry	string	query	False	Filter by execution_expiry
approval_expiry	string	query	False	Filter by approval_expiry
owner.uuid	string	query	False	Filter by owner.uuid
owner.name	string	query	False	Filter by owner.name
required_approvers	integer	query	False	Filter by required_approvers
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[multi_admin_verify_rule]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "approval_expiry": "string",
      "approval_groups": [
        {
          "name": "string"
        }
      ],
      "create_time": "string",
      "execution_expiry": "string",
      "operation": "string",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "query": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

approval_groups

Name	Type	Description
name	string	Name of the approval group.

_links

Name	Type	Description
self	href	

owner

The owner of the rule. The only valid owner is currently the cluster.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a POST or PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

multi_admin_verify_rule

Name	Type	Description
approval_expiry	string	Time for requests to be approved, in ISO-8601 duration format. If not set, the global setting is used.

Name	Type	Description
approval_groups	array[approval_groups]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.
auto_request_create	boolean	When true, ONTAP automatically creates a request for any failed operation where there is no matching pending request. • Default value: • Introduced in: 9.11 • x-nullable: true
create_time	string	
execution_expiry	string	Time for requests to be executed once approved, in ISO-8601 duration format. If not set, the global setting is used.
operation	string	Command that requires one or more approvals.
owner	owner	The owner of the rule. The only valid owner is currently the cluster.
query	string	When specified, this property limits the entries that require approvals to those that match the specified query.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
system_defined	boolean	Specifies whether the rule is system-defined or user-defined.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a multi-admin-verify rule

POST `/security/multi-admin-verify/rules`

Introduced In: 9.11

Creates a multi-admin-verify rule.

Parameters

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

Request Body

Name	Type	Description
approval_expiry	string	Time for requests to be approved, in ISO-8601 duration format. If not set, the global setting is used.
approval_groups	array[approval_groups]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.

Name	Type	Description
auto_request_create	boolean	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 • x-nullable: true
create_time	string	
execution_expiry	string	Time for requests to be executed once approved, in ISO-8601 duration format. If not set, the global setting is used.
operation	string	Command that requires one or more approvals.
owner	owner	The owner of the rule. The only valid owner is currently the cluster.
query	string	When specified, this property limits the entries that require approvals to those that match the specified query.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
system_defined	boolean	Specifies whether the rule is system-defined or user-defined.

Example request


```
{
  "approval_expiry": "string",
  "approval_groups": [
    {
      "name": "string"
    }
  ],
  "create_time": "string",
  "execution_expiry": "string",
  "operation": "string",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "query": "string"
}
```


Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[multi_admin_verify_rule]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "approval_expiry": "string",
      "approval_groups": [
        {
          "name": "string"
        }
      ],
      "create_time": "string",
      "execution_expiry": "string",
      "operation": "string",
      "owner": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "query": "string"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

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.

Error Code	Description
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 two minutes 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.

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

Definitions

See Definitions

approval_groups

Name	Type	Description
name	string	Name of the approval group.

href

Name	Type	Description
href	string	

_links

owner

The owner of the rule. The only valid owner is currently the cluster.

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

multi_admin_verify_rule

Name	Type	Description
approval_expiry	string	Time for requests to be approved, in ISO-8601 duration format. If not set, the global setting is used.
approval_groups	array[approval_groups]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.

Name	Type	Description
auto_request_create	boolean	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 • x-nullable: true
create_time	string	
execution_expiry	string	Time for requests to be executed once approved, in ISO-8601 duration format. If not set, the global setting is used.
operation	string	Command that requires one or more approvals.
owner	owner	The owner of the rule. The only valid owner is currently the cluster.
query	string	When specified, this property limits the entries that require approvals to those that match the specified query.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
system_defined	boolean	Specifies whether the rule is system-defined or user-defined.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage a multi-admin-verify rule

Manage a multi-admin-verify rule

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"
```

Delete a multi-admin-verify rule

DELETE `/security/multi-admin-verify/rules/{owner.uuid}/{operation}`

Introduced In: 9.11

Deletes a multi-admin-verify rule.

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	
operation	string	path	True	

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.

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

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a multi-admin-verify rule

GET `/security/multi-admin-verify/rules/{owner.uuid}/{operation}`

Introduced In: 9.11

Retrieves a multi-admin-verify rule.

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	
operation	string	path	True	
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
approval_expiry	string	Time for requests to be approved, in ISO-8601 duration format. If not set, the global setting is used.
approval_groups	array[approval_groups]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.
auto_request_create	boolean	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 • x-nullable: true
create_time	string	
execution_expiry	string	Time for requests to be executed once approved, in ISO-8601 duration format. If not set, the global setting is used.
operation	string	Command that requires one or more approvals.
owner	owner	The owner of the rule. The only valid owner is currently the cluster.
query	string	When specified, this property limits the entries that require approvals to those that match the specified query.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
system_defined	boolean	Specifies whether the rule is system-defined or user-defined.

Example response


```
{
  "approval_expiry": "string",
  "approval_groups": [
    {
      "name": "string"
    }
  ],
  "create_time": "string",
  "execution_expiry": "string",
  "operation": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "query": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

approval_groups

Name	Type	Description
name	string	Name of the approval group.

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

owner

The owner of the rule. The only valid owner is currently the cluster.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a POST or PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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 multi-admin-verify rule

PATCH `/security/multi-admin-verify/rules/{owner.uuid}/{operation}`

Introduced In: 9.11

Updates a multi-admin-verify rule.

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	
operation	string	path	True	

Request Body

Name	Type	Description
approval_expiry	string	Time for requests to be approved, in ISO-8601 duration format. If not set, the global setting is used.
approval_groups	array[approval_groups]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.
auto_request_create	boolean	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 • x-nullable: true
create_time	string	

Name	Type	Description
execution_expiry	string	Time for requests to be executed once approved, in ISO-8601 duration format. If not set, the global setting is used.
owner	owner	The owner of the rule. The only valid owner is currently the cluster.
query	string	When specified, this property limits the entries that require approvals to those that match the specified query.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
system_defined	boolean	Specifies whether the rule is system-defined or user-defined.

Example request

```
{
  "approval_expiry": "string",
  "approval_groups": [
    {
      "name": "string"
    }
  ],
  "create_time": "string",
  "execution_expiry": "string",
  "owner": {
    "name": "svm1"
  },
  "query": "string"
}
```

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 two minutes to two weeks.

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

Definitions

See Definitions

approval_groups

Name	Type	Description
name	string	Name of the approval group.

href

Name	Type	Description
href	string	

_links

owner

The owner of the rule. The only valid owner is currently the cluster.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a POST or PATCH method.

multi_admin_verify_rule

Name	Type	Description
approval_expiry	string	Time for requests to be approved, in ISO-8601 duration format. If not set, the global setting is used.
approval_groups	array[approval_groups]	List of approval groups that are allowed to approve requests for rules that don't have approval groups.
auto_request_create	boolean	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 • x-nullable: true
create_time	string	

Name	Type	Description
execution_expiry	string	Time for requests to be executed once approved, in ISO-8601 duration format. If not set, the global setting is used.
owner	owner	The owner of the rule. The only valid owner is currently the cluster.
query	string	When specified, this property limits the entries that require approvals to those that match the specified query.
required_approvers	integer	The number of required approvers, excluding the user that made the request.
system_defined	boolean	Specifies whether the rule is system-defined or user-defined.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage security roles

Manage security roles

Overview

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

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

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

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

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

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

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

Predefined (built-in) roles

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

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

These predefined roles cannot be modified or deleted.

Mapped roles

Before REST APIs, the RBAC roles (legacy roles) were defined to contain the CLI commands and their access levels. Now, almost all REST APIs map to one or more CLI commands. When a role is created using a POST request on /api/security/roles, a mapped legacy role is created. This legacy role has the same access level (as that of the REST API) for the mapped CLI commands. However, if a legacy role with the same name already exists, the POST operation fails and you need to choose a unique name for the role. Legacy roles are also managed using the REST endpoint /api/security/roles and its derivatives. In CLI, legacy roles are managed using the "security login role <create \| modify \| delete> -role <rolename>" commands.</rolename>

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

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

API restrictions

A role can be a REST role or a legacy role but not both. A role cannot be defined to have a mix of privilege tuples with REST API paths and privilege tuples with command/command directory paths. However, predefined (built-in) roles are an exception to this rule. Numerous APIs are scoped for the cluster level only. This results in an access error if assigned to an SVM-scoped role. For example, *api/cluster/nodes* does not work when added as a tuple entry for an SVM-scoped role.

A number of APIs allowed for an SVM-scoped role might have restrictions on the access level. For example, */api/network/ethernet/ports* cannot have an access level of "all" for an SVM-scoped role; this results in an access error when a POST or PATCH request is made.

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

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

Resource-qualified endpoints are now supported. At present, the only supported resource-qualified endpoints are the following:

Snapshots APIs

– /api/storage/volumes/{volume.uuid}/snapshots

File System Analytics APIs

– /api/storage/volumes/{volume.uuid}/files

– /api/storage/volumes/{volume.uuid}/top-metrics/clients

– /api/storage/volumes/{volume.uuid}/top-metrics/directories

– /api/storage/volumes/{volume.uuid}/top-metrics/files

– /api/storage/volumes/{volume.uuid}/top-metrics/users

– /api/svm/svms/{svm.uuid}/top-metrics/clients

– /api/svm/svms/{svm.uuid}/top-metrics/directories

– /api/svm/svms/{svm.uuid}/top-metrics/files

– /api/svm/svms/{svm.uuid}/top-metrics/users

Ontap S3 APIs

– /api/protocols/s3/services/{svm.uuid}/users

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

Examples

Creating a cluster-scoped custom role of REST API tuples

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

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles" -d
'{"name":"cluster_role1", "privileges" :
[{"access":"readonly","path":"/api/cluster/jobs"},{"access":"all","path":"
/api/application/applications"},{"access":"readonly","path":"/api/applicat
ion/templates"}]}'
```

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

Specify the role name and the tuples (of commands/command directories, their access levels and associated optional queries) in the body of the POST request. The owner.uuid or owner.name are not required to be specified for a cluster-scoped role.

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles" -d
'{"name":"cluster_role2", "privileges" :
[{"access":"readonly","path":"volume
qtree","query":""},{"access":"all","path":"security
certificate"},{"access":"readonly","path":"snapmirror policy","query":"-
policy !CustomPol*"}]}'
```

Creating an SVM-scoped custom role of REST API tuples

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

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

# The call:
curl -X POST "https://<mgmt-ip>/api/security/roles" -d '{"owner": {"uuid"
: "9f93e553-4b02-11e9-a3f9-005056bb7acd"},"name":"svm_role1", "privileges"
:
[{"access":"readonly","path":"/api/cluster/jobs"},{"access":"all","path":"
/api/application/applications"},{"access":"readonly","path":"/api/applicat
ion/templates"}]}'
```

Creating an SVM-scoped custom role of command and/or command directory tuples

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

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

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

Creating a custom role with a resource-qualified endpoint

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

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

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

Creating a custom role with a private CLI endpoint

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

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

Retrieving the configured roles

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

```
# The API:
GET "/api/security/roles?fields=%2A"

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

# The response:
{
"records": [
```

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

```
      "_links": {
        "self": {
          "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "customRole_rest",
    "privileges": [
      {
        "path": "/api/storage/volumes/738e3c9f-9897-41f2-be92-
a00945fd9bdb/snapshots",
        "access": "readonly",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_rest/privileges/%2Fapi%2Fstorage%2Fvolumes%2F738e3
c9f-9897-41f2-be92-a00945fd9bdb%2Fsnapshots"
          }
        }
      },
      {
        "path": "/api/storage/volumes/e621583b-f445-4713-ba9e-
a052d53c8a83/snapshots",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_rest/privileges/%2Fapi%2Fstorage%2Fvolumes%2Fe6215
83b-f445-4713-ba9e-a052d53c8a83%2Fsnapshots"
          }
        }
      }
      {
        "path": "/api/svm/svms/881764b5-9ea1-11ec-8771-005056bb1a7c/top-
metrics/directories",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/881764b5-9ea1-11ec-8771-
005056bb1a7c/customRole_rest/privileges/%2Fapi%2Fstorage%2Fsvm%2F881764b5-
9ea1-11ec-8771-005056bb1a7c%2Ftop-metrics%2Fdirectories"
          }
        }
      }
    ],
    "builtin": false,
```

```
    "scope": "cluster",
    "_links": {
      "self": {
        "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_rest"
      }
    }
  },
  {
    "owner": {
      "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
      "name": "cluster1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "customRole_legacy",
    "privileges": [
      {
        "path": "volume",
        "access": "readonly",
        "query":"-is_svm_root false",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_legacy/privileges/volume"
          }
        }
      },
      {
        "path": "volume snapshot",
        "access": "all",
        "query": "-volume vol1&#124;vol2",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_legacy/privileges/volume%20snapshot"
          }
        }
      }
    ],
    "builtin": false,
    "scope": "cluster",
    "_links": {
```

```
      "self": {
        "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-
0050568e2e25/customRole_legacy"
      }
    }
  },
  {
    "owner": {
      "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
      "name": "svm1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "vsadmin",
    "privileges": [
      {
        "path": "/api/application/applications",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fapplication%2Fapplications"
          }
        }
      },
      {
        "path": "/api/application/templates",
        "access": "readonly",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fapplication%2Ftemplates"
          }
        }
      },
      {
        "path": "/api/cluster",
        "access": "readonly",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fcluster"
          }
```

```
        }
      },
      {
        "path": "/api/cluster/jobs",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fcluster%2Fjobs"
          }
        }
      },
      {
        "path": "/api/cluster/schedules",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/%2Fapi%2Fcluster%2Fschedules"
          }
        }
      },
      {
        "path": "DEFAULT",
        "access": "none",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/DEFAULT"
          }
        }
      },
      {
        "path": "application create",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/vsadmin/privileges/application%20create"
          }
        }
      },
      {
        "path": "application delete",
        "access": "all",
        "_links": {
```

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

Using a scoped call to retrieve the configured roles

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

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

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

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

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

Retrieve a list of roles configured in the cluster

GET `/security/roles`

Introduced In: 9.6

Retrieves a list of roles configured in the cluster.

Related ONTAP commands

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

Learn more

- DOC /security/roles

Parameters

Name	Type	In	Required	Description
owner.name	string	query	False	Filter by owner.name • Introduced in: 9.7
owner.uuid	string	query	False	Filter by owner.uuid • Introduced in: 9.7
name	string	query	False	Filter by name • Introduced in: 9.7
builtin	boolean	query	False	Filter by builtin • Introduced in: 9.7
privileges.access	string	query	False	Filter by privileges.access • Introduced in: 9.7

Name	Type	In	Required	Description
privileges.path	string	query	False	Filter by privileges.path • Introduced in: 9.7
privileges.query	string	query	False	Filter by privileges.query • Introduced in: 9.11
scope	string	query	False	Filter by scope • Introduced in: 9.7
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0

Name	Type	In	Required	Description
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[role]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "admin",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "privileges": [
        {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "access": "all",
          "path": "volume move start",
          "query": "-vserver vs1|vs2|vs3 -destination-aggregate
aggr1|aggr2"
        }
      ],
      "scope": "string"
    }
  ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

owner

Owner name and UUID that uniquely identifies the role.

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

role_privilege

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

Snapshots APIs

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

File System Analytics APIs

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

- */api/storage/volumes/{volume.uuid}/top-metrics/clients*
- */api/storage/volumes/{volume.uuid}/top-metrics/directories*
- */api/storage/volumes/{volume.uuid}/top-metrics/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/users*
- */api/svm/svms/{svm.uuid}/top-metrics/clients*
- */api/svm/svms/{svm.uuid}/top-metrics/directories*
- */api/svm/svms/{svm.uuid}/top-metrics/files*
- */api/svm/svms/{svm.uuid}/top-metrics/users*
- */api/protocols/s3/services/{svm.uuid}/users*

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

Name	Type	Description
_links	_links	
access	string	Access level for the REST endpoint or command/command directory path. If it denotes the access level for a command/command directory path, the only supported enum values are 'none','readonly' and 'all'.
path	string	Either of REST URI/endpoint OR command/command directory path.

Name	Type	Description
query	string	Optional attribute that can be specified only if the "path" attribute refers to a command/command directory path. The privilege tuple implicitly defines a set of objects the role can or cannot access at the specified access level. The query further reduces this set of objects to a subset of objects that the role is allowed to access. The query attribute must be applicable to the command/command directory specified by the "path" attribute. It is defined using one or more parameters of the command/command directory path specified by the "path" attribute.

role

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

Name	Type	Description
_links	_links	
builtin	boolean	Indicates if this is a built-in (pre-defined) role which cannot be modified or deleted.
name	string	Role name
owner	owner	Owner name and UUID that uniquely identifies the role.
privileges	array[role_privilege]	The list of privileges that this role has been granted.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a new cluster-scoped or SVM-scoped role

POST `/security/roles`

Introduced In: 9.6

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

Required parameters

- `name` - Name of the role to be created.
- `privileges` - Array of privilege tuples. Each tuple consists of a REST API or command/command directory path and its desired access level. If the tuple refers to a command/command directory path, it could optionally contain a query.

Optional parameters

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

Related ONTAP commands

- `security login rest-role create`
- `security login role create`

Learn more

- DOC /security/roles

Parameters

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

Request Body

Name	Type	Description
builtin	boolean	Indicates if this is a built-in (pre-defined) role which cannot be modified or deleted.
name	string	Role name
owner	owner	Owner name and UUID that uniquely identifies the role.
privileges	array[role_privilege]	The list of privileges that this role has been granted.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example request


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


Response

```
Status: 201, Created
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1263347	Cannot modify pre-defined roles
2621462	The supplied SVM does not exist.
5636129	Role with given name has not been defined.
5636143	Vserver admin cannot use the API with this access level.

Error Code	Description
5636144	Invalid value specified for access level.
5636168	This role is mapped to a rest-role and cannot be modified directly. Modifications must be done with rest-role.
5636169	Invalid character in URI.
5636170	URI does not exist.
5636171	Role already exists in legacy role table.
5636184	Expanded REST roles for granular resource control feature is currently disabled.
5636185	The specified UUID was not found.
5636186	Expanded REST roles for granular resource control requires an effective cluster version of 9.10.1 or later.
5636191	The "path" parameter in a "privileges" tuple can contain only API endpoint entries or only command and command directory entries.
5636192	The query parameter cannot be specified for the privileges tuple with API endpoint entries.
5636200	The specified value of the access parameter is invalid, if a command or command directory is specified in the path parameter.
5636210	User creation failed because LDAP is not configured for the SVM or the LDAP connection is not secure.
5636262	Cannot create a role with the specified role name because it is reserved by the system.
13434890	Vserver-ID failed for Vserver roles.
13434891	UUID lookup failed for Vserver roles.
13434892	Roles is a required field.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

owner

Owner name and UUID that uniquely identifies the role.

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

role_privilege

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

Snapshots APIs

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

File System Analytics APIs

- */api/storage/volumes/{volume.uuid}/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/clients*
- */api/storage/volumes/{volume.uuid}/top-metrics/directories*
- */api/storage/volumes/{volume.uuid}/top-metrics/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/users*
- */api/svm/svms/{svm.uuid}/top-metrics/clients*
- */api/svm/svms/{svm.uuid}/top-metrics/directories*
- */api/svm/svms/{svm.uuid}/top-metrics/files*
- */api/svm/svms/{svm.uuid}/top-metrics/users*
- */api/protocols/s3/services/{svm.uuid}/users*

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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

role

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

Name	Type	Description
builtin	boolean	Indicates if this is a built-in (pre-defined) role which cannot be modified or deleted.
name	string	Role name

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View or delete a role

View or delete a role

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></i> 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.</svm-name>

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

Examples

Retrieving the role configuration for a REST role

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

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

# The response:
{
"owner": {
  "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
  "name": "svm1",
  "_links": {
    "self": {
      "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
    }
  }
},
"name": "secure_role",
"privileges": [
  {
    "path": "/api/security",
    "access": "all",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/secure_role/privileges/%2Fapi%2Fsecurity"
      }
    }
  },
  {
    "path": "/api/storage/volumes/651f7fdf-7752-11eb-8d4e-
0050568ed6bd/snapshots",
    "access": "readonly",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/secure_role/privileges/%2Fapi%2Fstorage%2Fvolumes%2F651f7fdf-
```

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

Retrieving the role configuration for a custom legacy role

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

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

# The response:
{
"owner": {
  "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
  "name": "svm1",
  "_links": {
    "self": {
      "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
    }
```

```
    }
  },
  "name": "finVolNoDel",
  "privileges": [
    {
      "path": "DEFAULT",
      "access": "none",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/finVolNoDel/privileges/DEFAULT"
        }
      }
    },
    {
      "path": "volume",
      "access": "all",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/finVolNoDel/privileges/volume"
        }
      }
    },
    {
      "path": "volume delete",
      "access": "none",
      "query": "-volume vol_fin*",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/finVolNoDel/privileges/volume%20delete"
        }
      }
    }
  ],
  "builtin": false,
  "scope": "svm",
  "_links": {
    "self": {
      "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/finVolNoDel"
    }
  }
}
```

Deleting a custom role

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

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

Delete a role

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

Introduced In: 9.6

Deletes the specified role.

Required parameters

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

Related ONTAP commands

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

Learn more

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

Parameters

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

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1263347	Cannot modify pre-defined roles.
5636169	Specified URI path is invalid or not supported. Resource-qualified endpoints are not supported.
5636170	URI does not exist.
5636172	User accounts detected with this role assigned. Update or delete those accounts before deleting this role.
5636173	Features require an effective cluster version of 9.6 or later.
5636184	Expanded REST roles for granular resource control feature is currently disabled.
5636185	The specified UUID was not found.
5636186	Expanded REST roles for granular resource control requires an effective cluster version of 9.10.1 or later.
5636245	Failed to delete the role because it is part of the group role-mapping configuration.
5636246	Failed to delete the rest role because it is part of the group role-mapping configuration.
5636247	Failed to delete the rest role because it is part of the external-role-mapping configuration.
5636249	Failed to delete the role because it is part of the external-role-mapping configuration.
13434890	Vserver-ID failed for Vserver roles.
13434893	The SVM does not exist.

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

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the details of a role

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

Introduced In: 9.6

Retrieves the details of the specified role.

Related ONTAP commands

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

Learn more

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Role owner UUID
name	string	path	True	Role name
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
builtin	boolean	Indicates if this is a built-in (pre-defined) role which cannot be modified or deleted.
name	string	Role name
owner	owner	Owner name and UUID that uniquely identifies the role.
privileges	array[role_privilege]	The list of privileges that this role has been granted.

Name	Type	Description
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example response


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


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

owner

Owner name and UUID that uniquely identifies the role.

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

role_privilege

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

Snapshots APIs

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

File System Analytics APIs

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

- */api/svm/svms/{svm.uuid}/top-metrics/files*
- */api/svm/svms/{svm.uuid}/top-metrics/users*
- */api/protocols/s3/services/{svm.uuid}/users*

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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

error_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage role privilege details

Manage role privilege details

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 or creates a new role with the provided tuple. The "path" attribute can be a resource-qualified endpoint. Currently, the only supported resource-qualified endpoints are the following:

Snapshots APIs

– /api/storage/volumes/{volume.uuid}/snapshots

File System Analytics APIs

– /api/storage/volumes/{volume.uuid}/files

– /api/storage/volumes/{volume.uuid}/top-metrics/clients

– /api/storage/volumes/{volume.uuid}/top-metrics/directories

– /api/storage/volumes/{volume.uuid}/top-metrics/files

– /api/storage/volumes/{volume.uuid}/top-metrics/users

– /api/svm/svms/{svm.uuid}/top-metrics/clients

– /api/svm/svms/{svm.uuid}/top-metrics/directories

– /api/svm/svms/{svm.uuid}/top-metrics/files

– /api/svm/svms/{svm.uuid}/top-metrics/users

Ontap S3 APIs

– /api/protocols/s3/services/{svm.uuid}/users

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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>_

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&amp;#124;vs2 -aggregate aggr1&amp;#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"
      }
    }
  },
  {
    "path": "/api/storage/volumes/*/top-metrics/users",
```

```
    "access": "read_create_modify",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/svm_role1/privileges/%2Fapi%2Fstorage%2Fvolumes%2F%2A%2Ftop-
metrics%2Fusers"
      }
    }
  }
],
"num_records": 4,
"_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"
  }
}
}
```


Retrieve privilege details of the specified role

GET `/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

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Role owner UUID
name	string	path	True	Role name
fields	array[string]	query	False	Specify the fields to return.
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. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[role_privilege]	

Example response


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


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

role_privilege

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

Snapshots APIs

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

File System Analytics APIs

- */api/storage/volumes/{volume.uuid}/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/clients*
- */api/storage/volumes/{volume.uuid}/top-metrics/directories*
- */api/storage/volumes/{volume.uuid}/top-metrics/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/users*
- */api/svm/svms/{svm.uuid}/top-metrics/clients*
- */api/svm/svms/{svm.uuid}/top-metrics/directories*
- */api/svm/svms/{svm.uuid}/top-metrics/files*
- */api/svm/svms/{svm.uuid}/top-metrics/users*
- */api/protocols/s3/services/{svm.uuid}/users*

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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.

Add a privilege tuple to an existing role

POST `/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 or creates a new role with the provided tuple.

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 following:

Snapshots APIs

– /api/storage/volumes/{volume.uuid}/snapshots

File System Analytics APIs

– /api/storage/volumes/{volume.uuid}/files

– /api/storage/volumes/{volume.uuid}/top-metrics/clients

– /api/storage/volumes/{volume.uuid}/top-metrics/directories

– /api/storage/volumes/{volume.uuid}/top-metrics/files

– /api/storage/volumes/{volume.uuid}/top-metrics/users

– /api/svm/svms/{svm.uuid}/top-metrics/clients

– /api/svm/svms/{svm.uuid}/top-metrics/directories

– /api/svm/svms/{svm.uuid}/top-metrics/files

– /api/svm/svms/{svm.uuid}/top-metrics/users

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

- `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

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Role owner UUID
name	string	path	True	Role name
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
access	string	Access level for the REST endpoint or command/command directory path. If it denotes the access level for a command/command directory path, the only supported enum values are 'none','readonly' and 'all'.
path	string	Either of REST URI/endpoint OR command/command directory path.

Name	Type	Description
query	string	Optional attribute that can be specified only if the "path" attribute refers to a command/command directory path. The privilege tuple implicitly defines a set of objects the role can or cannot access at the specified access level. The query further reduces this set of objects to a subset of objects that the role is allowed to access. The query attribute must be applicable to the command/command directory specified by the "path" attribute. It is defined using one or more parameters of the command/command directory path specified by the "path" attribute.

Example request

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

Response

```
Status: 201, Created
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1263347	Cannot modify pre-defined roles.
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.
5636168	This role is mapped to a rest-role and cannot be modified directly. Modifications must be done with rest-role.
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	The 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.
5636192	The query parameter cannot be specified for the privileges tuple with API endpoint entries.
5636200	The specified value of the access parameter is invalid, if a command or command directory is specified in the path parameter.
5636262	Cannot create a role with the specified role name because it is reserved by the system.
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.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

role_privilege

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

Snapshots APIs

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

File System Analytics APIs

- */api/storage/volumes/{volume.uuid}/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/clients*
- */api/storage/volumes/{volume.uuid}/top-metrics/directories*
- */api/storage/volumes/{volume.uuid}/top-metrics/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/users*
- */api/svm/svms/{svm.uuid}/top-metrics/clients*
- */api/svm/svms/{svm.uuid}/top-metrics/directories*
- */api/svm/svms/{svm.uuid}/top-metrics/files*
- */api/svm/svms/{svm.uuid}/top-metrics/users*
- */api/protocols/s3/services/{svm.uuid}/users*

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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.

Manage role privilege path

Manage role privilege path

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 the following:

Snapshots APIs

– /api/storage/volumes/{volume.uuid}/snapshots

File System Analytics APIs

– /api/storage/volumes/{volume.uuid}/files

– /api/storage/volumes/{volume.uuid}/top-metrics/clients

– /api/storage/volumes/{volume.uuid}/top-metrics/directories

– /api/storage/volumes/{volume.uuid}/top-metrics/files

– /api/storage/volumes/{volume.uuid}/top-metrics/users

– /api/svm/svms/{svm.uuid}/top-metrics/clients

– /api/svm/svms/{svm.uuid}/top-metrics/directories

– /api/svm/svms/{svm.uuid}/top-metrics/files

– /api/svm/svms/{svm.uuid}/top-metrics/users

Ontap S3 APIs

– /api/protocols/s3/services/{svm.uuid}/users

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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>

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&amp;#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%2Ffiles" -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:
/api/svm/svms/{svm.uuid}/top-metrics/files
curl -X DELETE "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fstorage%2Fsvm%2F6e000659-
9a16-11ec-819e-005056bb1a7c%2Ftop-metrics%2Ffiles"
```

Delete a privilege tuple from the role

DELETE `/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 the following:

Snapshots APIs

– /api/storage/volumes/{volume.uuid}/snapshots

File System Analytics APIs

– /api/storage/volumes/{volume.uuid}/files

– /api/storage/volumes/{volume.uuid}/top-metrics/clients

– /api/storage/volumes/{volume.uuid}/top-metrics/directories

– /api/storage/volumes/{volume.uuid}/top-metrics/files

– /api/storage/volumes/{volume.uuid}/top-metrics/users

– /api/svm/svms/{svm.uuid}/top-metrics/clients

– /api/svm/svms/{svm.uuid}/top-metrics/directories

– /api/svm/svms/{svm.uuid}/top-metrics/files

– /api/svm/svms/{svm.uuid}/top-metrics/users

Ontap S3 APIs

– /api/protocols/s3/services/{svm.uuid}/users

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic

privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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/svm/svms/43256a71-be02-474d-a2a9-9642e12a6a2c/top-metrics/users*). Currently, resource-qualified endpoints are limited to the *Snapshots* and *File System Analytics* endpoints listed above in the description.

Related ONTAP commands

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

Learn more

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Role owner UUID
name	string	path	True	Role name
path	string	path	True	REST API path or command/command directory path

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1263347	Cannot modify pre-defined roles.

Error Code	Description
5636168	This role is mapped to a rest-role and cannot be modified directly. Modifications must be done with rest-role.
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.

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

Name	Type	Description
error	returned_error	

Example error


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

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the access level for a REST API path or command/command directory path for a role

GET `/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 the following:

Snapshots APIs

– /api/storage/volumes/{volume.uuid}/snapshots

File System Analytics APIs

– /api/storage/volumes/{volume.uuid}/files

– /api/storage/volumes/{volume.uuid}/top-metrics/clients

– /api/storage/volumes/{volume.uuid}/top-metrics/directories

– /api/storage/volumes/{volume.uuid}/top-metrics/files

– /api/storage/volumes/{volume.uuid}/top-metrics/users

– /api/svm/svms/{svm.uuid}/top-metrics/clients

– /api/svm/svms/{svm.uuid}/top-metrics/directories

– /api/svm/svms/{svm.uuid}/top-metrics/files

– /api/svm/svms/{svm.uuid}/top-metrics/users

Ontap S3 APIs

– /api/protocols/s3/services/{svm.uuid}/users

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

Related ONTAP commands

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

Learn more

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Role owner UUID
name	string	path	True	Role name
path	string	path	True	REST API path or command/command directory path
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

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

Example response


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

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the access level for a REST API path or command/command directory path

PATCH `/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 the following:

Snapshots APIs

– /api/storage/volumes/{volume.uuid}/snapshots

File System Analytics APIs

– /api/storage/volumes/{volume.uuid}/files

– /api/storage/volumes/{volume.uuid}/top-metrics/clients

– /api/storage/volumes/{volume.uuid}/top-metrics/directories

– /api/storage/volumes/{volume.uuid}/top-metrics/files

– /api/storage/volumes/{volume.uuid}/top-metrics/users

– /api/svm/svms/{svm.uuid}/top-metrics/clients

– /api/svm/svms/{svm.uuid}/top-metrics/directories

– /api/svm/svms/{svm.uuid}/top-metrics/files

– /api/svm/svms/{svm.uuid}/top-metrics/users

Ontap S3 APIs

– /api/protocols/s3/services/{svm.uuid}/users

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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* and *File System Analytics* endpoints listed above in the description.

Optional parameters

- `access` - Access level for the path.
- `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

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

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Role owner UUID
name	string	path	True	Role name
path	string	path	True	REST API path or command/command directory path

Request Body

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

Example request

```
{
  "access": "all",
  "query": "-vserver vs1|vs2|vs3 -destination-aggregate aggr1|aggr2"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636168	This role is mapped to a rest-role and cannot be modified directly. Modifications must be done with rest-role.
5636192	The query parameter cannot be specified for the privileges tuple with API endpoint entries.
5636200	The specified value of the access parameter is invalid, if a command or command directory is specified in the path parameter.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

role_privilege

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

Snapshots APIs

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

File System Analytics APIs

- */api/storage/volumes/{volume.uuid}/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/clients*
- */api/storage/volumes/{volume.uuid}/top-metrics/directories*
- */api/storage/volumes/{volume.uuid}/top-metrics/files*
- */api/storage/volumes/{volume.uuid}/top-metrics/users*
- */api/svm/svms/{svm.uuid}/top-metrics/clients*
- */api/svm/svms/{svm.uuid}/top-metrics/directories*
- */api/svm/svms/{svm.uuid}/top-metrics/files*
- */api/svm/svms/{svm.uuid}/top-metrics/users*
- */api/protocols/s3/services/{svm.uuid}/users*

In the above APIs, wildcard character * could be used in place of *{volume.uuid}* or *{svm.uuid}* to denote *all* volumes or *all* SVMs, depending upon whether the REST endpoint references volumes or SVMs. The *{volume.uuid}* refers to the *-instance-uuid* field value in the "volume show" command output at diagnostic privilege level. It can also be fetched through REST endpoint */api/storage/volumes*.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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.

Manage SSH server

Manage SSH server

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* 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, maximum authentication retry attempts allowed before closing the connection, and *ssh-rsa* enabled status for public key algorithms) and SSH connection limits.

The security algorithms include SSH key exchange algorithms, ciphers for payload encryption, MAC algorithms and host key 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", "ecdh_sha2_nistp256",
"diffie_hellman_group18_sha512" ], "mac_algorithms": [
"hmac_sha2_512_etm", "umac_128_etm" ], "host_key_algorithms": [
"ecdsa_sha2_nistp256", "ssh_rsa" ], "max_authentication_retry_count": 3,
"is_rsa_in_publickey_algorithms_enabled": true  }'
```

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:
{
"ciphers": [
  "aes256_ctr",
  "aes192_ctr"
],
"key_exchange_algorithms": [
  "diffie_hellman_group_exchange_sha256",
  "ecdh_sha2_nistp256",
  "diffie_hellman_group18_sha512"
],
"mac_algorithms": [
  "hmac_sha2_512_etm",
  "umac_128_etm"
],
"host_key_algorithms": [
  "ecdsa_sha2_nistp256",
  "ssh_rsa"
],
"max_authentication_retry_count": 3,
"connections_per_second": 8,
"max_instances": 10,
"is_rsa_in_publickey_algorithms_enabled": true,
"per_source_limit": 5,
"_links": {
  "self": {
    "href": "/api/security/ssh"
  }
}
}
```

Retrieve cluster SSH server ciphers, MAC algorithms, key exchange algorithms, and connection limits

GET `/security/ssh`

Introduced In: 9.7

Retrieves the cluster SSH server ciphers, MAC algorithms, key exchange algorithms, host key algorithms, connection limits, and *ssh-rsa* enabled status for public key algorithms.

Related ONTAP commands

- `security ssh`
- `security protocol ssh`

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
ciphers	array[string]	Ciphers for encrypting the data.
connections_per_second	integer	Maximum connections allowed per second.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.
key_exchange_algorithms	array[string]	Key exchange algorithms.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
max_instances	integer	Maximum possible simultaneous connections.

Name	Type	Description
per_source_limit	integer	Maximum connections from the same client host.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "host_key_algorithms": [
    "ecdsa_sha2_nistp256",
    "ssh_rsa"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256",
    "diffie_hellman_group18_sha512"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the SSH server setting for a cluster

PATCH `/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

- `host_key_algorithms` - Host key 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
- `is_rsa_in_publickey_algorithms_enabled` - *ssh-rsa* enabled status for public key algorithms
- `per_source_limit` - Maximum allowed connections from the same client host

Related ONTAP commands

- `security ssh`
- `security protocol ssh`

Request Body

Name	Type	Description
ciphers	array[string]	Ciphers for encrypting the data.
connections_per_second	integer	Maximum connections allowed per second.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.
key_exchange_algorithms	array[string]	Key exchange algorithms.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.

Name	Type	Description
max_instances	integer	Maximum possible simultaneous connections.
per_source_limit	integer	Maximum connections from the same client host.

Example request

```
{
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "host_key_algorithms": [
    "ecdsa_sha2_nistp256",
    "ssh_rsa"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256",
    "diffie_hellman_group18_sha512"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "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.
10682423	There must be at least one host key algorithm associated with the SSH configuration.
10682424	Host key algorithm not supported in FIPS enabled mode.
10682425	Failed to modify Host key algorithms.
10682426	Failed to modify *ssh-rsa* enabled status for publickey algorithms configuration.
10682428	Cipher not supported in FIPS enabled mode.
10682429	Adding 'diffie_hellman_group16_sha512' or 'diffie_hellman_group18_sha512' to the SSH key exchange algorithms list requires an effective cluster version of ONTAP 9.16.1 or later.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

cluster_ssh_server

Name	Type	Description
ciphers	array[string]	Ciphers for encrypting the data.
connections_per_second	integer	Maximum connections allowed per second.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.
key_exchange_algorithms	array[string]	Key exchange algorithms.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
max_instances	integer	Maximum possible simultaneous connections.

Name	Type	Description
per_source_limit	integer	Maximum connections from the same client host.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View SSH SVMs

View SSH SVMs

Overview

This endpoint is used to retrieve the SSH security configuration for all data SVMs. The configuration consists of SSH security parameters. The security algorithms include SSH key exchange algorithms, ciphers for payload encryption, MAC algorithms, host key algorithms, maximum authentication retry attempts allowed before closing the connection, and *ssh-rsa* enabled status for public key algorithms. 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 data SVM, perform a PATCH operation on the *api/security/ssh/svms/{svm.uuid}* endpoint.

Example

Retrieving the SSH security configuration of all SVMs.

Retrieves the SSH security configurations associated with the owners or filtered list (for a specific data SVM and so on).

```
# The API:
GET "/api/security/ssh/svms"

# The call:
curl -X GET "https://<mgmt-ip>/api/security/ssh/svms?fields=*"

# The response
{
"records": [
  {
    "svm": {
      "uuid": "739e5da5-1a50-11ee-9cb0-005056bb97dc",
      "name": "svm1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/739e5da5-1a50-11ee-9cb0-005056bb97dc"
        }
      }
     },
     "ciphers": [
       "aes256_ctr",
       "aes192_ctr",
       "aes128_ctr",
       "aes128_gcm",
       "aes256_gcm"
     ],
     "key_exchange_algorithms": [
       "diffie_hellman_group_exchange_sha256",
       "ecdh_sha2_nistp256",
       "ecdh_sha2_nistp384",
       "ecdh_sha2_nistp521",
       "curve25519_sha256",
       "diffie_hellman_group16_sha512",
       "diffie_hellman_group18_sha512"
     ],
     "mac_algorithms": [
       "hmac_sha2_256",
       "hmac_sha2_512",
       "hmac_sha2_256_etm",
       "hmac_sha2_512_etm",
       "umac_64",
       "umac_128",
       "umac_64_etm",
       "umac_128_etm"
     ],
     "host_key_algorithms": [
```

```
        "ecdsa_sha2_nistp256",
        "ssh_rsa",
        "ssh_ed25519"
      ],
      "is_rsa_in_publickey_algorithms_enabled": true,
      "max_authentication_retry_count": 6,
      "_links": {
        "self": {
          "href": "/api/security/ssh/svms/739e5da5-1a50-11ee-9cb0-
005056bb97dc"
        }
      }
    }
 ],
 "num_records": 1,
   "_links": {
     "self": {
       "href": "/api/security/ssh/svms?fields=*"
    }
  }
}

# The call:
curl -X GET "https://<mgmt-ip>/api/security/ssh/svms"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7",
      "name": "svm1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
        }
      }
    },
    "_links": {
      "self": {
        "href": "/api/security/ssh/svms/02c9e252-41be-11e9-81d5-
00a0986138f7"
      }
    }
  }
],
```

```
"num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/ssh/svms"
    }
  }
}
```

Retrieve the SSH server configuration for all SVMs

GET `/security/ssh/svms`

Introduced In: 9.10

Retrieves the SSH server configuration for all the data SVMs.

Related ONTAP commands

- `security ssh`

Parameters

Name	Type	In	Required	Description
host_key_algorithms	string	query	False	Filter by host_key_algorithms • Introduced in: 9.16
key_exchange_algorithms	string	query	False	Filter by key_exchange_algorithms
mac_algorithms	string	query	False	Filter by mac_algorithms
max_authentication_retry_count	integer	query	False	Filter by max_authentication_retry_count • Max value: 6 • Min value: 2
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid

Name	Type	In	Required	Description
is_rsa_in_publickey_algorithms_enabled	boolean	query	False	Filter by is_rsa_in_publickey_algorithms_enabled • Introduced in: 9.16
ciphers	string	query	False	Filter by ciphers
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 15
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[svm_ssh_server]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "ciphers": [
        "aes256_ctr",
        "aes192_ctr",
        "aes128_ctr"
      ],
      "host_key_algorithms": [
        "ecdsa_sha2_nistp256",
        "ssh_ed25519",
        "ssh_rsa"
      ],
      "key_exchange_algorithms": [
        "diffie_hellman_group_exchange_sha256",
        "ecdh_sha2_nistp256"
      ],
      "mac_algorithms": [
        "hmac_sha2_512",
        "hmac_sha2_512_etm"
      ],
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
```

```
      }
    ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

svm

SVM name and UUID for which the SSH server is configured.

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

svm_ssh_server

Name	Type	Description
_links	_links	
ciphers	array[string]	Ciphers for encrypting the data.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.

Name	Type	Description
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.
key_exchange_algorithms	array[string]	Key exchange algorithms.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
svm	svm	SVM name and UUID for which the SSH server is configured.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage SSH security configuration

Manage SSH security configuration

Overview

This endpoint is used to retrieve or modify the SSH security configuration of a data SVM.

The SSH security algorithms include key exchange algorithms, ciphers for payload encryption, MAC algorithms, host key 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",
"ecdh_sha2_nistp256", "diffie_hellman_group16_sha512" ], "mac_algorithms":
[ "hmac_sha2_512_etm", "umac_128_etm" ], "host_key_algorithms": [
"ecdsa_sha2_nistp256", "ssh_ed25519"
],"is_rsa_in_publickey_algorithms_enabled": false,
"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",
  "ecdh_sha2_nistp256",
  "diffie_hellman_group16_sha512"
],
"mac_algorithms": [
  "hmac_sha2_512_etm",
  "umac_128_etm"
],
"host_key_algorithms": [
  "ecdsa_sha2_nistp256",
  "ssh_ed25519"
],
"is_rsa_in_publickey_algorithms_enabled": false,
"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"
  }
}
}
```

Retrieve the SSH server configuration for an SVM

GET `/security/ssh/svms/{svm.uuid}`

Introduced In: 9.10

Retrieves the SSH server configuration for the specified data SVM.

Related ONTAP commands

- `security ssh`

Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	SVM UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
ciphers	array[string]	Ciphers for encrypting the data.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.

Name	Type	Description
key_exchange_algorithms	array[string]	Key exchange algorithms.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
svm	svm	SVM name and UUID for which the SSH server is configured.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "host_key_algorithms": [
    "ecdsa_sha2_nistp256",
    "ssh_ed25519",
    "ssh_rsa"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

svm

SVM name and UUID for which the SSH server is configured.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the SSH server configuration for an SVM

PATCH `/security/ssh/svms/{svm.uuid}`

Introduced In: 9.10

Updates the SSH server configuration for the specified data SVM.

Optional parameters

- `ciphers` - Encryption algorithms for the payload
- `key_exchange_algorithms` - SSH key exchange algorithms
- `host_key_algorithms` - Host key algorithms
- `mac_algorithms` - MAC algorithms
- `max_authentication_retry_count` - Maximum authentication retries allowed before closing the connection
- `is_rsa_in_publickey_algorithms_enabled` - *ssh-rsa* enabled status for public key algorithms

Related ONTAP commands

- `security ssh`

Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	SVM UUID

Request Body

Name	Type	Description
ciphers	array[string]	Ciphers for encrypting the data.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.

Name	Type	Description
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.
key_exchange_algorithms	array[string]	Key exchange algorithms.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
svm	svm	SVM name and UUID for which the SSH server is configured.

Example request


```
{
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "host_key_algorithms": [
    "ecdsa_sha2_nistp256",
    "ssh_ed25519",
    "ssh_rsa"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "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.

Error Code	Description
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.
10682420	To modify the SSH configuration of the admin SVM, use the /api/security/ssh REST API.
10682423	There must be at least one host key algorithm associated with the SSH configuration.
10682424	Host key algorithm not supported in FIPS enabled mode.
10682425	Failed to modify Host key algorithms.
10682426	Failed to modify *ssh-rsa* enabled status for publickey algorithms configuration.
10682428	Cipher not supported in FIPS enabled mode.
10682429	Adding 'diffie_hellman_group16_sha512' or 'diffie_hellman_group18_sha512' to the SSH key exchange algorithms list requires an effective cluster version of ONTAP 9.16.1 or later.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

SVM name and UUID for which the SSH server is configured.

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

svm_ssh_server

Name	Type	Description
ciphers	array[string]	Ciphers for encrypting the data.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.
key_exchange_algorithms	array[string]	Key exchange algorithms.

Name	Type	Description
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
svm	svm	SVM name and UUID for which the SSH server is configured.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage WebAuthn credentials

Manage WebAuthn credentials

Overview

This API is used to retrieve all WebAuthn credentials entries.

Examples

Retrieving all Webauthn credentials entries

The following output shows all WebAuthn credentials entries.

```
## The API:
/api/security/webauthn/credentials

## The call:
curl -X GET "https://<mgmt-ip>/api/security/webauthn/credentials"

# The response:
{
"records": [
  {
    "owner": {
      "uuid": "389758ee-40cd-11ef-bb21-005056aeae31",
      "_links": {
        "self": {
          "href": "/api/svm/svms/389758ee-40cd-11ef-bb21-005056aeae31"
        }
      }
    },
    "username": "user_1",
    "index": 0,
    "relying_party": {
      "id": "ontap1.example.com",
      "name": "ontap1.example.com"
    },
    "_links": {
      "self": {
        "href": "/api/security/webauthn/credentials/389758ee-40cd-11ef-
bb21-005056aeae31/user_1/0/ontap1.example.com"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/security/webauthn/credentials/"
  }
}
}
```

Retrieve all WebAuthn credentials entries

GET `/security/webauthn/credentials`

Introduced In: 9.16

Retrieves all WebAuthn credentials entries.

Related ONTAP commands

- `security webauthn credentials show`

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records.
records	array[webauthn_credentials]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "creation_time": "2024-08-05 22:38:55 -0400",
      "credential": {
        "id_sha":
"xxxxxxxxxxxxxxxxxxxxxxebfb30f20bf6db74xxxxxxxxxxxxxxxxxxxxxxxx",
        "type": "string"
      },
      "display_name": "admin",
      "index": 0,
      "last_used_time": "2024-08-05 22:48:55 -0400",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "public_key": {
        "algorithm": "ES-256",
        "value":
"xxxxxxxxxxxxxxxxxxxxxe5sZohRRv2B10JjjALXmGRmEfFIxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxYr2+w=="
      },
      "relying_party": {
        "id": "example.com",
        "name": "example.com"
      },
```

```
      "scope": "string",
      "username": "admin"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

self_link

Name	Type	Description
self	href	

credential

Name	Type	Description
id_sha	string	SHA-256 Hashed representation of Credential ID.
type	string	Credential type.

_links

Name	Type	Description
self	href	

svm_reference

SVM, applies only to SVM-scoped objects.

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

public_key

Name	Type	Description
algorithm	string	Public key algorithm.
value	string	Public key value.

relying_party

Name	Type	Description
id	string	Relying Party ID.
name	string	Relying Party Name.

webauthn_credentials

Name	Type	Description
_links	self_link	
creation_time	string	Date and time indicating when this entry was created.
credential	credential	
display_name	string	Display name.
index	integer	Index.
last_used_time	string	Date and time indicating when this entry was last used.
owner	svm_reference	SVM, applies only to SVM-scoped objects.
public_key	public_key	
relying_party	relying_party	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
username	string	Username.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete a WebAuthn credentials entry

DELETE
`/security/webauthn/credentials/{owner.uuid}/{username}/{index}/{relying_party.id}`

Introduced In: 9.16

Deletes a WebAuthn credentials entry.

Required properties

- `owner.uuid`
- `username`
- `index`
- `relying_party.id`

Related ONTAP commands

- `security webauthn credentials delete`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Used to identify a cluster or an SVM.

Name	Type	In	Required	Description
username	string	path	True	Username.
index	integer	path	True	Index.
relying_party.id	string	path	True	Relying Party ID.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a WebAuthn credentials entry

GET
`/security/webauthn/credentials/{owner.uuid}/{username}/{index}/{relying_party.id}`

Introduced In: 9.16

Retrieves a WebAuthn credentials entry.

Related ONTAP commands

- `security webauthn credentials show`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Used to identify a cluster or an SVM.
username	string	path	True	Username.
index	integer	path	True	Index.

Name	Type	In	Required	Description
relying_party.id	string	path	True	Relying Party ID.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	
creation_time	string	Date and time indicating when this entry was created.
credential	credential	
display_name	string	Display name.
index	integer	Index.
last_used_time	string	Date and time indicating when this entry was last used.
owner	svm_reference	SVM, applies only to SVM-scoped objects.
public_key	public_key	
relying_party	relying_party	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
username	string	Username.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "creation_time": "2024-08-05 22:38:55 -0400",
  "credential": {
    "id_sha":
"xxxxxxxxxxxxxxxxxxxxxxebfb30f20bf6db74xxxxxxxxxxxxxxxxxxxxxxxxx",
    "type": "string"
  },
  "display_name": "admin",
  "index": 0,
  "last_used_time": "2024-08-05 22:48:55 -0400",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "public_key": {
    "algorithm": "ES-256",
    "value":
"xxxxxxxxxxxxxxxxxxxxxe5sZohRRv2B10JjjALXmGRmEfFIxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxYr2+w=="
  },
  "relying_party": {
    "id": "example.com",
    "name": "example.com"
  },
  "scope": "string",
  "username": "admin"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

credential

Name	Type	Description
id_sha	string	SHA-256 Hashed representation of Credential ID.
type	string	Credential type.

_links

Name	Type	Description
self	href	

svm_reference

SVM, applies only to SVM-scoped objects.

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

public_key

Name	Type	Description
algorithm	string	Public key algorithm.

Name	Type	Description
value	string	Public key value.

relying_party

Name	Type	Description
id	string	Relying Party ID.
name	string	Relying Party Name.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View WebAuthn global settings for a cluster and all SVMs

View WebAuthn global settings for a cluster and all SVMs

Overview

This API endpoint retrieves WebAuthn global settings for a cluster and all SVMs.

Examples

Retrieving the WebAuthn global settings

Retrieves all of the WebAuthn global settings for the cluster and all SVMs.

```
# The API:
GET "/api/security/webauthn/global-settings"

# The call to retrieve the WebAuthn global settings:
curl -k https://<mgmt-ip>/api/security/webauthn/global-settings
```

Retrieve WebAuthn global settings for a cluster and all SVMs

GET `/security/webauthn/global-settings`

Introduced In: 9.16

Retrieve WebAuthn global settings for a cluster and all SVMs.

Related ONTAP commands

- `security webauthn show`

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records.
records	array[webauthn_global]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "attestation": "none",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "require_rk": "",
      "resident_key": "discouraged",
      "scope": "string",
      "timeout": 600000,
      "user_verification": "discouraged"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

svm_reference

SVM, applies only to SVM-scoped objects.

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

webauthn_global

WebAuthn global settings.

Name	Type	Description
_links	self_link	
attestation	string	Attestation conveyance type.

Name	Type	Description
owner	svm_reference	SVM, applies only to SVM-scoped objects.
require_rk	boolean	Specifies whether the resident key is required.
resident_key	string	Resident key.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
timeout	integer	The timeout interval for the WebAuthn request, in milliseconds.
user_verification	string	User verification.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View a WebAuthn global setting entry

View a WebAuthn global setting entry

Overview

This API endpoint retrieves WebAuthn global settings for the cluster or SVM. Specify the owner UUID and the unique identifier for the cluster or SVM to retrieve the WebAuthn global settings for the cluster or SVM.

Examples

Retrieving the WebAuthn global settings for the cluster or SVM

```
# The API:
GET "/api/security/webauthn/global-settings/{owner.uuid}"

# The call:
curl -k https://<mgmt-ip>/api/security/webauthn/global-settings/d49de271-
8c11-11e9-8f78-005056bbf6ac
```

Retrieve a WebAuthn global setting entry

GET `/security/webauthn/global-settings/{owner.uuid}`

Introduced In: 9.16

Retrieves a WebAuthn global setting entry.

Related ONTAP commands

- `security webauthn show`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Used to identify a cluster or an SVM.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	

Name	Type	Description
attestation	string	Attestation conveyance type.
owner	svm_reference	SVM, applies only to SVM-scoped objects.
require_rk	boolean	Specifies whether the resident key is required.
resident_key	string	Resident key.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
timeout	integer	The timeout interval for the WebAuthn request, in milliseconds.
user_verification	string	User verification.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "attestation": "none",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "require_rk": "",
  "resident_key": "discouraged",
  "scope": "string",
  "timeout": 600000,
  "user_verification": "discouraged"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

svm_reference

SVM, applies only to SVM-scoped objects.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

View all WebAuthn supported algorithms

View all WebAuthn supported algorithms

Overview

This API endpoint retrieves the list of supported algorithms for WebAuthn authentication.

Examples

Retrieving the list of supported algorithms

This endpoint retrieves all of the supported algorithms for WebAuthn authentication. The following table lists the supported algorithms:

Algorithm ID	Algorithm Name	Description
-7	ES256	ECDSA w/ SHA-256
-35	ES384	ECDSA w/ SHA-384
-257	RS256	RSASSA-PKCS1-v1_5 using SHA-256

```
# The API:
GET "/api/security/webauthn/supported-algorithms"

# The call to retrieve the list of supported algorithms:
curl -k https://<mgmt-ip>/api/security/webauthn/supported-algorithms
```

Retrieve all WebAuthn supported algorithms entries

GET `/security/webauthn/supported-algorithms`

Introduced In: 9.16

Retrieve all WebAuthn supported algorithms entries.

Related ONTAP commands

- `security webauthn supported-algorithms show`

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records.

Name	Type	Description
records	array[supported_algorithms]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "algorithm": {
        "id": -7,
        "name": "ES-256",
        "type": "string"
      },
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "scope": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

self_link

Name	Type	Description
self	href	

algorithm

Name	Type	Description
id	integer	Algorithm ID.
name	string	Algorithm name.
type	string	Algorithm type.

_links

Name	Type	Description
self	href	

svm_reference

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

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

supported_algorithms

WebAuthn supported algorithms.

Name	Type	Description
_links	self_link	
algorithm	algorithm	
owner	svm_reference	SVM, applies only to SVM-scoped objects.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

View a WebAuthn supported algorithms entry

View a WebAuthn supported algorithms entry

Overview

This API endpoint retrieves a specific WebAuthn supported algorithms entry. Specify the owner UUID, the unique identifier for the cluster or SVM, and the algorithm name to retrieve the specific WebAuthn supported algorithms entry.

Examples

Retrieving the specific WebAuthn supported algorithms entry

```
# The API:
GET "/api/security/webauthn/supported-algorithms/{owner.uuid}/{alg_name}"

# The call:
curl -k https://<mgmt-ip>/api/security/webauthn/supported-
algorithms/d49de271-8c11-11e9-8f78-005056bbf6ac/ES-256
```

Retrieve a WebAuthn supported algorithms entry

GET `/security/webauthn/supported-algorithms/{owner.uuid}/{algorithm.name}`

Introduced In: 9.16

Retrieves a WebAuthn supported algorithms entry.

Related ONTAP commands

- `security webauthn supported-algorithms show`

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Used to identify a cluster or an SVM.
algorithm.name	string	path	True	Algorithm name.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	
algorithm	algorithm	
owner	svm_reference	SVM, applies only to SVM-scoped objects.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "algorithm": {
    "id": -7,
    "name": "ES-256",
    "type": "string"
  },
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

algorithm

Name	Type	Description
id	integer	Algorithm ID.
name	string	Algorithm name.
type	string	Algorithm type.

_links

Name	Type	Description
self	href	

svm_reference

SVM, applies only to SVM-scoped objects.

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

error_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.