



Manage Google Cloud KMS

REST API reference

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi/security_gcp-kms_endpoint_overview.html on February 11, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Manage Google Cloud KMS	1
Manage Google Cloud KMS	1
Overview	1
Examples	1
Retrieve a Google Cloud KMS configurations for all clusters and SVMs	7
Related ONTAP commands	8
Parameters	8
Response	11
Error	13
Definitions	14
Create a Google Cloud KMS configuration for an SVM	20
Required properties	20
Optional properties	20
Related ONTAP commands	21
Parameters	21
Request Body	22
Response	27
Error	27
Definitions	28
Re-key the external key in the key hierarchy for an SVM	34
Required properties	34
Optional properties	34
Related ONTAP commands	34
Parameters	34
Request Body	35
Response	36
Response	36
Error	37
Definitions	38
Delete a Google Cloud KMS configuration	40
Related ONTAP commands	40
Parameters	40
Response	41
Response	41
Error	41
Definitions	43
Retrieve the Google Cloud KMS configuration	44
Related ONTAP commands	44
Parameters	44
Response	44
Error	48
Definitions	49

Update the Google Cloud KMS configuration	52
Optional properties	52
Related ONTAP commands	53
Parameters	53
Request Body	54
Response	59
Response	59
Error	59
Definitions	60
Re-key the internal key in the key hierarchy for an SVM	66
Related ONTAP commands	66
Parameters	66
Response	67
Response	68
Error	68
Definitions	69
Restore keys for an SVM from a Google Cloud KMS	70
Related ONTAP commands	71
Parameters	71
Response	72
Response	72
Error	72
Definitions	73

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"}'
```

Changing the GCKMS key

The following example shows how to change the GCKMS key.

```
# The API:  
POST /api/security/gcp-kms/{uuid}/rekey-external  
  
# The call:  
curl -X POST 'https://<mgmt-ip>/api/security/gcp-kms/f72098a2-e908-11ea-  
bd56-005056bb4222/rekey-external' -d '{"key_name": "key2",  
"key_ring_location": "global", "key_ring_name": "testKeyRing2",  
"project_id": "testProj2"}'
```

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
port	integer	query	False	Filter by port <ul style="list-style-type: none">• Introduced in: 9.14
proxy_type	string	query	False	Filter by proxy_type
project_id	string	query	False	Filter by project_id
uuid	string	query	False	Filter by uuid
ekmip_reachability.message	string	query	False	Filter by ekmip_reachability.message
ekmip_reachability.node.name	string	query	False	Filter by ekmip_reachability.node.name
ekmip_reachability.node.uuid	string	query	False	Filter by ekmip_reachability.node.uuid
ekmip_reachability.reachable	boolean	query	False	Filter by ekmip_reachability.reachable
ekmip_reachability.code	string	query	False	Filter by ekmip_reachability.code
key_name	string	query	False	Filter by key_name

Name	Type	In	Required	Description
authentication_method	string	query	False	Filter by authentication_method <ul style="list-style-type: none"> • Introduced in: 9.17
state.code	string	query	False	Filter by state.code
state.cluster_state	boolean	query	False	Filter by state.cluster_state
state.message	string	query	False	Filter by state.message
key_ring_location	string	query	False	Filter by key_ring_location
verify_ip	boolean	query	False	Filter by verify_ip <ul style="list-style-type: none"> • Introduced in: 9.14
proxy_port	integer	query	False	Filter by proxy_port
key_ring_name	string	query	False	Filter by key_ring_name
gce_metadata_server	string	query	False	Filter by gce_metadata_server <ul style="list-style-type: none"> • Introduced in: 9.17
google_reachability.reachable	boolean	query	False	Filter by google_reachability.reachable
google_reachability.code	string	query	False	Filter by google_reachability.code
google_reachability.message	string	query	False	Filter by google_reachability.message

Name	Type	In	Required	Description
proxy_username	string	query	False	Filter by proxy_username
cloudkms_host	string	query	False	Filter by cloudkms_host <ul style="list-style-type: none"> Introduced in: 9.14
privileged_account	string	query	False	Filter by privileged_account <ul style="list-style-type: none"> Introduced in: 9.14
scope	string	query	False	Filter by scope
proxy_host	string	query	False	Filter by proxy_host
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
oauth_url	string	query	False	Filter by oauth_url <ul style="list-style-type: none"> Introduced in: 9.14
oauth_host	string	query	False	Filter by oauth_host <ul style="list-style-type: none"> Introduced in: 9.14
verify_host	boolean	query	False	Filter by verify_host <ul style="list-style-type: none"> Introduced in: 9.14
caller_account	string	query	False	Filter by caller_account <ul style="list-style-type: none"> Introduced in: 9.14
fields	array[string]	query	False	Specify the fields to return.

Name	Type	In	Required	Description
max_records	integer	query	False	Limit the number of records returned.
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Default value: 15 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is true for GET calls. When set to false, only the number of records is returned.</p> <ul style="list-style-type: none"> • Default value: 1
order_by	array[string]	query	False	Order results by specified fields and optional [asc]

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[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\">myserviceaccount@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 <code>fields</code> 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 <code>fields</code> 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	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value:

Request Body

Name	Type	Description
_links	_links	

Name	Type	Description
application_credentials	string	The Google Cloud application's service account credentials required to access the specified KMS. The <code>client_email</code> and <code>private_key</code> fields of the service account holder are required. The credentials are required if the <code>authentication_method</code> is set to <code>application_credentials_key</code> .
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 <code>authentication_method</code> is set to <code>sa_credentials_attachment</code> .
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 <code>fields</code> 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 <code>fields</code> 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\": \"\",  
    \"node\": {  
      \"name\": \"node1\",  
      \"uuid\": \"1cd8a442-86d1-11e0-ae1c-123478563412\"  
    }  
  }  
}
```

```

    "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 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.
65537753	The "key_name" value contains invalid characters. A forward slash '/' is not allowed in the key name.
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 <code>fields</code> 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 <code>fields</code> 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.

Required properties

- key_name - Google Cloud KMS key name.

Optional properties

- project_id - Google Cloud KMS project ID.
- key_ring_location - Google Cloud KMS key ring location.
- key_ring_name - Google Cloud KMS key ring name.

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.
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value:

Request Body

Name	Type	Description
key_name	string	Google Cloud KMS key name.

Name	Type	Description
key_ring_location	string	Google Cloud KMS key ring location.
key_ring_name	string	Google Cloud KMS key ring name.
project_id	string	Google Cloud KMS project ID.

Example request

```
{
  "key_name": "cryptokey1",
  "key_ring_location": "location1",
  "key_ring_name": "keyring1",
  "project_id": "project1"
}
```

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.
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 rerun 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.
65537753	The "key_name" value contains invalid characters. A forward slash '/' is not allowed in the key name.
65537755	Google Cloud KMS configuration details were not found for the 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

gcp_kms_key

Name	Type	Description
key_name	string	Google Cloud KMS key name.
key_ring_location	string	Google Cloud KMS key ring location.
key_ring_name	string	Google Cloud KMS key ring name.
project_id	string	Google Cloud KMS project ID.

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

Name	Type	Description
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

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 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]	

Name	Type	Description
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.
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.

Name	Type	Description
proxy_host	string	Proxy host name.
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 <code>fields</code> 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

```

"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": "svml",
  "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
<code>uuid</code>	string	path	True	Google Cloud KMS UUID

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0

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 <code>client_email</code> and <code>private_key</code> fields of the service account holder are required. The credentials are required if the <code>authentication_method</code> is set to <code>application_credentials_key</code> .
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 <code>authentication_method</code> is set to <code>sa_credentials_attachment</code> .
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 <code>fields</code> query parameter or GET for all advanced properties is enabled.
oauth_host	string	Open authorization server host name.

Name	Type	Description
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".
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 <code>fields</code> 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.

Name	Type	Description
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.
65537757	The "key_name", "project_id", "key_ring_name" and "key_ring_location" fields cannot be modified directly. Use the REST API POST method "/api/security/gcp-kms/{uuid}/rekey-external" to modify these fields.

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 <code>fields</code> 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 <code>fields</code> 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	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value:

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	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none">• Default value: 0• Max value: 120• Min value: 0
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none">• Default value:

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.

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.