Manage AWS KMS

ONTAP 9.15.1 REST API reference

NetApp
September 11, 2024

Table of Contents

Manage AWS KMS

Security aws-kms endpoint overview

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": "AK7ATC35ZXU6GKUDQURT", "secret_access_key": "Ahrut-
#ghty5-881Ht"}'

# 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": "AK7ATC35ZXU6GKUDQURT",
    "_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": "AK7ATC35ZXU6GKUDQURT",
    "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": "AK7ATC35ZXU6GKUDQURT",
"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": "AK7ATC35ZXU6GKUDQURT",
"secret_access_key": "Ahrut-#ghty5-881Ht"}'
```

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'
```

Retrieve all AWS KMS instances configured for all clusters and SVMs

GET `/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

Name	Type	In	Required	Description
access_key_id	string	query	False	Filter by access_key_id
port	integer	query	False	Filter by port

Name	Type	In	Required	Description
proxy_port	integer	query	False	Filter by proxy_port
proxy_type	string	query	False	Filter by proxy_type
svm.uuid	string	query	False	Filter by svm.uuid
svm.name	string	query	False	Filter by svm.name
host	string	query	False	Filter by host
proxy_username	string	query	False	Filter by proxy_username
key_id	string	query	False	Filter by key_id
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
verify	boolean	query	False	Filter by verify
skip_verify	boolean	query	False	Filter by skip_verify
default_domain	string	query	False	Filter by default_domain
polling_period	integer	query	False	Filter by polling_period
timeout	integer	query	False	Filter by timeout
uuid	string	query	False	Filter by uuid
region	string	query	False	Filter by region
proxy_host	string	query	False	Filter by proxy_host
ekmip_reachability.reachable	boolean	query	False	Filter by ekmip_reachability.reachable

Name	Type	In	Required	Description
ekmip_reachability.message	string	query	False	Filter by ekmip_reachability.message
ekmip_reachability.code	string	query	False	Filter by ekmip_reachability.code
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
scope	string	query	False	Filter by scope
verify_host	boolean	query	False	Filter by verify_host
amazon_reachability.message	string	query	False	Filter by amazon_reachability.message
amazon_reachability.reachable	boolean	query	False	Filter by amazon_reachability.reachable
amazon_reachability.code	string	query	False	Filter by amazon_reachability.code
service	string	query	False	Filter by service
encryption_context	string	query	False	Filter by encryption_context
verify_ip	boolean	query	False	Filter by verify_ip
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: 1 • 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[aws_kms]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access_key_id": "<id_value>",
      "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_password": "awskze-Jwjje2-WJJPer",
      "proxy_port": 1234,
      "proxy_type": "http",
      "proxy_username": "proxyuser",
      "region": "us-east-1",
      "scope": "string",
      "secret_access_key": "<id_value>",
      "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.

Error Code	Description
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 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	

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.

Name	Type	Description
code	string	Code corresponding to the error message. Returns a 0 if Amazon KMS is reachable from all nodes in the cluster.
message	string	Error message returned when 'reachable' is false.
reachable	boolean	Set to true if the Amazon KMS is reachable from all nodes of the cluster.

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.

state

Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.

Name	Type	Description
cluster_state	boolean	Set to true when AWS KMS key protection is available on all nodes of the cluster.
code	string	Code corresponding to the message. Returns a 0 if AWS KMS key protection is available on all nodes of the cluster.
message	string	Error message set when cluster_state 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.

aws_kms

Name	Type	Description
_links	_links	
access_key_id	string	AWS Access Key ID of the user that has appropriate access to AWS KMS.
amazon_reachability	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.
default_domain	string	AWS KMS default domain.
ekmip_reachability	array[ekmip_reachability]	
encryption_context	string	Additional layer of authentication and logging.
host	string	AWS KMS host's hostname.
key_id	string	AWS Key ID.
polling_period	integer	Polling period in minutes.
port	integer	AWS KMS port.

Name	Type	Description
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
region	string	AWS region of the AWS KMS.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
secret_access_key	string	AWS Secret Access Key for the provided access key ID.
service	string	AWS service type.
skip_verify	boolean	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	state	Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.
svm	svm	SVM, applies only to SVM-scoped objects.
timeout	integer	AWS Connection timeout, in seconds.
uuid	string	A unique identifier for the AWS KMS.

Name	Type	Description
verify	boolean	Set to true to verify the AWS KMS host.
verify_host	boolean	Set to true to verify the AWS KMS host's hostname.
verify_ip	boolean	Set to true to verify the AWS KMS host's 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.

Configure the AWS KMS configuration for an SVM

POST `/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

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

Request Body

Name	Type	Description
_links	_links	
access_key_id	string	AWS Access Key ID of the user that has appropriate access to AWS KMS.

Name	Type	Description
amazon_reachability	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.
default_domain	string	AWS KMS default domain.
ekmip_reachability	array[ekmip_reachability]	
encryption_context	string	Additional layer of authentication and logging.
host	string	AWS KMS host's hostname.
key_id	string	AWS Key ID.
polling_period	integer	Polling period in minutes.
port	integer	AWS KMS port.
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
region	string	AWS region of the AWS KMS.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

Name	Type	Description
secret_access_key	string	AWS Secret Access Key for the provided access key ID.
service	string	AWS service type.
skip_verify	boolean	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	state	Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.
svm	svm	SVM, applies only to SVM-scoped objects.
timeout	integer	AWS Connection timeout, in seconds.
uuid	string	A unique identifier for the AWS KMS.
verify	boolean	Set to true to verify the AWS KMS host.
verify_host	boolean	Set to true to verify the AWS KMS host’s hostname.
verify_ip	boolean	Set to true to verify the AWS KMS host’s IP address.

Example request


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_key_id": "<id_value>",
  "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_password": "awskze-Jwjje2-WJJPer",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "region": "us-east-1",
  "scope": "string",
  "secret_access_key": "<id_value>",
  "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": ""
}
```


Response

```
Status: 201, Created
```

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

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access_key_id": "<id_value>",
      "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_password": "awskze-Jwjje2-WJJPer",
      "proxy_port": 1234,
      "proxy_type": "http",
      "proxy_username": "proxyuser",
      "region": "us-east-1",
      "scope": "string",
      "secret_access_key": "<id_value>",
      "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": ""
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

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.

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	

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.

Name	Type	Description
code	string	Code corresponding to the error message. Returns a 0 if Amazon KMS is reachable from all nodes in the cluster.
message	string	Error message returned when 'reachable' is false.
reachable	boolean	Set to true if the Amazon KMS is reachable from all nodes of the cluster.

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.

state

Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.

Name	Type	Description
cluster_state	boolean	Set to true when AWS KMS key protection is available on all nodes of the cluster.
code	string	Code corresponding to the message. Returns a 0 if AWS KMS key protection is available on all nodes of the cluster.
message	string	Error message set when cluster_state 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.

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

aws_kms

Name	Type	Description
_links	_links	
access_key_id	string	AWS Access Key ID of the user that has appropriate access to AWS KMS.
amazon_reachability	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.
default_domain	string	AWS KMS default domain.
ekmip_reachability	array[ekmip_reachability]	
encryption_context	string	Additional layer of authentication and logging.
host	string	AWS KMS host's hostname.
key_id	string	AWS Key ID.
polling_period	integer	Polling period in minutes.
port	integer	AWS KMS port.
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.

Name	Type	Description
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
region	string	AWS region of the AWS KMS.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
secret_access_key	string	AWS Secret Access Key for the provided access key ID.
service	string	AWS service type.
skip_verify	boolean	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	state	Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.
svm	svm	SVM, applies only to SVM-scoped objects.
timeout	integer	AWS Connection timeout, in seconds.
uuid	string	A unique identifier for the AWS KMS.
verify	boolean	Set to true to verify the AWS KMS host.
verify_host	boolean	Set to true to verify the AWS KMS host's hostname.

Name	Type	Description
verify_ip	boolean	Set to true to verify the AWS KMS host's IP address.

_links

Name	Type	Description
next	href	
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.

Re-key or re-version an AWS KMS key encryption key for AWS KMS

POST `/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

Name	Type	In	Required	Description
aws_kms.uuid	string	path	True	UUID of the existing AWS 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: 1 • 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 of the AWS KMS key encryption key.

Example request

```
{
  "key_id": "key01"
}
```

Response

```
Status: 202, Accepted
```

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.
65537919	External rekey failed on one or more nodes.
65537926	AWS KMS is not configured for the given 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

aws_kms_key

Name	Type	Description
key_id	string	Key identifier of the AWS KMS key encryption 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.

Re-key SVM KEK for an AWS KMS

POST `/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

Name	Type	In	Required	Description
aws_kms.uuid	string	path	True	UUID of the existing AWS 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: 1 • 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
```

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
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.
65537926	AWS KMS is not configured for the given 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.

Restore keys for an SVM from a configured AWS KMS

POST `/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

Name	Type	In	Required	Description
aws_kms.uuid	string	path	True	UUID of the existing AWS 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: 1 • 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
```

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
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 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.

Delete an AWS KMS configuration

DELETE `/security/aws-kms/{uuid}`

Introduced In: 9.12

Deletes an AWS KMS configuration.

Related ONTAP commands

- `security key-manager external aws disable`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	AWS KMS UUID

Response

```
Status: 200, Ok
```

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 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 AWS KMS configuration

GET `/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

Name	Type	In	Required	Description
uuid	string	path	True	AWS KMS UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
access_key_id	string	AWS Access Key ID of the user that has appropriate access to AWS KMS.
amazon_reachability	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.
default_domain	string	AWS KMS default domain.

Name	Type	Description
ekmip_reachability	array[ekmip_reachability]	
encryption_context	string	Additional layer of authentication and logging.
host	string	AWS KMS host's hostname.
key_id	string	AWS Key ID.
polling_period	integer	Polling period in minutes.
port	integer	AWS KMS port.
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
region	string	AWS region of the AWS KMS.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
secret_access_key	string	AWS Secret Access Key for the provided access key ID.
service	string	AWS service type.
skip_verify	boolean	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	state	Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.
timeout	integer	AWS Connection timeout, in seconds.
uuid	string	A unique identifier for the AWS KMS.
verify	boolean	Set to true to verify the AWS KMS host.
verify_host	boolean	Set to true to verify the AWS KMS host's hostname.
verify_ip	boolean	Set to true to verify the AWS KMS host's IP address.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_key_id": "<id_value>",
  "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_password": "awskze-Jwjje2-WJJPer",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "region": "us-east-1",
  "scope": "string",
  "secret_access_key": "<id_value>",
  "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 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	

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.

Name	Type	Description
code	string	Code corresponding to the error message. Returns a 0 if Amazon KMS is reachable from all nodes in the cluster.
message	string	Error message returned when 'reachable' is false.
reachable	boolean	Set to true if the Amazon KMS is reachable from all nodes of the cluster.

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.

state

Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.

Name	Type	Description
cluster_state	boolean	Set to true when AWS KMS key protection is available on all nodes of the cluster.
code	string	Code corresponding to the message. Returns a 0 if AWS KMS key protection is available on all nodes of the cluster.
message	string	Error message set when cluster_state 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.

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 AWS KMS configuration

PATCH `/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

Name	Type	In	Required	Description
uuid	string	path	True	AWS KMS UUID

Request Body

Name	Type	Description
_links	_links	
access_key_id	string	AWS Access Key ID of the user that has appropriate access to AWS KMS.

Name	Type	Description
amazon_reachability	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.
default_domain	string	AWS KMS default domain.
ekmip_reachability	array[ekmip_reachability]	
encryption_context	string	Additional layer of authentication and logging.
host	string	AWS KMS host's hostname.
key_id	string	AWS Key ID.
polling_period	integer	Polling period in minutes.
port	integer	AWS KMS port.
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
region	string	AWS region of the AWS KMS.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

Name	Type	Description
secret_access_key	string	AWS Secret Access Key for the provided access key ID.
service	string	AWS service type.
skip_verify	boolean	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	state	Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.
svm	svm	SVM, applies only to SVM-scoped objects.
timeout	integer	AWS Connection timeout, in seconds.
uuid	string	A unique identifier for the AWS KMS.
verify	boolean	Set to true to verify the AWS KMS host.
verify_host	boolean	Set to true to verify the AWS KMS host’s hostname.
verify_ip	boolean	Set to true to verify the AWS KMS host’s IP address.

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_key_id": "<id_value>",
  "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_password": "awskze-Jwjje2-WJJPer",
  "proxy_port": 1234,
  "proxy_type": "http",
  "proxy_username": "proxyuser",
  "region": "us-east-1",
  "scope": "string",
  "secret_access_key": "<id_value>",
  "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": ""
}
```


Response

```
Status: 200, Ok
```

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 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	

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.

Name	Type	Description
code	string	Code corresponding to the error message. Returns a 0 if Amazon KMS is reachable from all nodes in the cluster.
message	string	Error message returned when 'reachable' is false.
reachable	boolean	Set to true if the Amazon KMS is reachable from all nodes of the cluster.

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.

state

Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.

Name	Type	Description
cluster_state	boolean	Set to true when AWS KMS key protection is available on all nodes of the cluster.
code	string	Code corresponding to the message. Returns a 0 if AWS KMS key protection is available on all nodes of the cluster.
message	string	Error message set when cluster_state 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.

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

aws_kms

Name	Type	Description
_links	_links	
access_key_id	string	AWS Access Key ID of the user that has appropriate access to AWS KMS.
amazon_reachability	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.
default_domain	string	AWS KMS default domain.
ekmip_reachability	array[ekmip_reachability]	
encryption_context	string	Additional layer of authentication and logging.
host	string	AWS KMS host's hostname.
key_id	string	AWS Key ID.
polling_period	integer	Polling period in minutes.
port	integer	AWS KMS port.
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.

Name	Type	Description
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
region	string	AWS region of the AWS KMS.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
secret_access_key	string	AWS Secret Access Key for the provided access key ID.
service	string	AWS service type.
skip_verify	boolean	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	state	Indicates whether or not the Amazon Web Services Key Management Service (AWS KMS) key protection is available cluster-wide.
svm	svm	SVM, applies only to SVM-scoped objects.
timeout	integer	AWS Connection timeout, in seconds.
uuid	string	A unique identifier for the AWS KMS.
verify	boolean	Set to true to verify the AWS KMS host.
verify_host	boolean	Set to true to verify the AWS KMS host's hostname.

Name	Type	Description
verify_ip	boolean	Set to true to verify the AWS KMS host's 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.

Copyright information

Trademark information