Manage SSH security configuration

REST API reference

NetApp
September 09, 2025

Table of Contents

Manage SSH security configuration

Security SSH svms svm.uuid endpoint overview

Overview

This endpoint is used to retrieve or modify the SSH security configuration of a data SVM.

The SSH security algorithms include key exchange algorithms, ciphers for payload encryption, MAC algorithms, host key algorithms and the maximum authentication retry attempts allowed before closing the connection. svm.uuid corresponds to the UUID of the SVM for which the SSH security setting is being retrieved or modified and it is obtained from the response body of a GET operation performed on the *api/security/ssh/svms* API.

Examples

Updating the SSH security parameters

Specify the algorithms in the body of the PATCH request.

```
# The API:
PATCH "/api/security/ssh/svms/{svm.uuid}"

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/ssh/svms/02c9e252-41be-11e9-
81d5-00a0986138f7" -d '{ "ciphers": [ "aes256_ctr", "aes192_ctr" ],
"key_exchange_algorithms": [ "diffie_hellman_group_exchange_sha256",
"ecdh_sha2_nistp256", "diffie_hellman_group16_sha512" ], "mac_algorithms":
[ "hmac_sha2_512_etm", "umac_128_etm" ], "host_key_algorithms": [
"ecdsa_sha2_nistp256", "ssh_ed25519"
],"is_rsa_in_publickey_algorithms_enabled": false,
"max_authentication_retry_count": 3 }'
```

Retrieving the SSH security configuration of an SVM.

```
# The API:
GET "/api/security/ssh/svms/{svm.uuid}"

# The call:
curl -X GET "https://<mgmt-ip>/api/security/ssh/svms/02c9e252-41be-11e9-
81d5-00a0986138f7"

# The response:
{
"ciphers": [
  "aes256_ctr",
  "aes192_ctr"
],
"key_exchange_algorithms": [
  "diffie_hellman_group_exchange_sha256",
  "ecdh_sha2_nistp256",
  "diffie_hellman_group16_sha512"
],
"mac_algorithms": [
  "hmac_sha2_512_etm",
  "umac_128_etm"
],
"host_key_algorithms": [
  "ecdsa_sha2_nistp256",
  "ssh_ed25519"
],
"is_rsa_in_publickey_algorithms_enabled": false,
"max_authentication_retry_count": 3,
"svm": {
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7",
  "_links": {
    "self": {
      "href": "/api/svm/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
},
"_links": {
  "self": {
    "href": "/api/security/ssh/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
}
```

Retrieve the SSH server configuration for an SVM

GET `/security/ssh/svms/{svm.uuid}`

Introduced In: 9.10

Retrieves the SSH server configuration for the specified data SVM.

Related ONTAP commands

- `security ssh`

Parameters

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

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
ciphers	array[string]	Ciphers for encrypting the data.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.

Name	Type	Description
key_exchange_algorithms	array[string]	Key exchange algorithms.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
svm	svm	SVM name and UUID for which the SSH server is configured.

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "host_key_algorithms": [
    "ecdsa_sha2_nistp256",
    "ssh_ed25519",
    "ssh_rsa"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

svm

SVM name and UUID for which the SSH server is configured.

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

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

Update the SSH server configuration for an SVM

PATCH `/security/ssh/svms/{svm.uuid}`

Introduced In: 9.10

Updates the SSH server configuration for the specified data SVM.

Optional parameters

- `ciphers` - Encryption algorithms for the payload
- `key_exchange_algorithms` - SSH key exchange algorithms
- `host_key_algorithms` - Host key algorithms
- `mac_algorithms` - MAC algorithms
- `max_authentication_retry_count` - Maximum authentication retries allowed before closing the connection
- `is_rsa_in_publickey_algorithms_enabled` - *ssh-rsa* enabled status for public key algorithms

Related ONTAP commands

- `security ssh`

Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	SVM UUID

Request Body

Name	Type	Description
ciphers	array[string]	Ciphers for encrypting the data.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.

Name	Type	Description
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.
key_exchange_algorithms	array[string]	Key exchange algorithms.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
svm	svm	SVM name and UUID for which the SSH server is configured.

Example request

```
{
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "host_key_algorithms": [
    "ecdsa_sha2_nistp256",
    "ssh_ed25519",
    "ssh_rsa"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
10682372	There must be at least one key exchange algorithm associated with the SSH configuration.

Error Code	Description
10682373	There must be at least one cipher associated with the SSH configuration.
10682375	Failed to modify SSH key exchange algorithms.
10682378	Failed to modify SSH ciphers.
10682399	Key exchange algorithm not supported in FIPS-enabled mode.
10682400	Failed to modify SSH MAC algorithms.
10682401	MAC algorithm not supported in FIPS-enabled mode.
10682403	There must be at least one MAC algorithm with the SSH configuration.
10682413	Failed to modify maximum authentication retry attempts.
10682418	Cipher not supported in FIPS-enabled mode.
10682420	To modify the SSH configuration of the admin SVM, use the /api/security/ssh REST API.
10682423	There must be at least one host key algorithm associated with the SSH configuration.
10682424	Host key algorithm not supported in FIPS enabled mode.
10682425	Failed to modify Host key algorithms.
10682426	Failed to modify *ssh-rsa* enabled status for publickey algorithms configuration.
10682428	Cipher not supported in FIPS enabled mode.
10682429	Adding 'diffie_hellman_group16_sha512' or 'diffie_hellman_group18_sha512' to the SSH key exchange algorithms list requires an effective cluster version of ONTAP 9.16.1 or later.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

SVM name and UUID for which the SSH server is configured.

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

svm_ssh_server

Name	Type	Description
ciphers	array[string]	Ciphers for encrypting the data.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithm 'ssh_ed25519' can be configured only in non-FIPS mode.
is_rsa_in_publickey_algorithms_enabled	boolean	Enables or disables the *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, for RSA keys in public key algorithms. If this flag is *false*, older SSH implementations might fail to authenticate using RSA keys. This flag should be enabled only as a temporary measure until legacy SSH client implementations can be upgraded or reconfigured with another key type, for example: ECDSA.
key_exchange_algorithms	array[string]	Key exchange algorithms.

Name	Type	Description
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
svm	svm	SVM name and UUID for which the SSH server is configured.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

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