Manage SSH server

REST API reference

NetApp
February 06, 2026

Table of Contents

Manage SSH server

Manage SSH server

Overview

ONTAP supports SSH server that can be accessed from any standard SSH client. A user account needs to be associated with SSH as the application (refer the documentation for *api/security/accounts* DOC /security/accounts . Upon connecting from a client, the user is authenticated and a command line shell is presented.

This endpoint is used to retrieve or modify the SSH configuration at the cluster level. The configuration consists of SSH security parameters (security algorithms, maximum authentication retry attempts allowed before closing the connection, SSH connection login grace time and *ssh-rsa* enabled status for public key algorithms) and SSH connection limits.

The security algorithms include SSH key exchange algorithms, ciphers for payload encryption, MAC algorithms and host key algorithms. This configuration is the default for all newly created SVMs; existing SVM configurations are not impacted. The SSH connection limits include maximum connections per second, maximum simultaneous sessions from the same client host, and overall maximum SSH connections at any given point in time. The connection limits are per node and will be the same for all nodes in the cluster.

Examples

Updating the SSH security parameters

Specify the algorithms in the body of the PATCH request.

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

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/ssh" -d '{ "ciphers": [
"aes256_ctr", "aes192_ctr" ], "key_exchange_algorithms": [
"diffie_hellman_group_exchange_sha256", "ecdh_sha2_nistp256",
"diffie_hellman_group18_sha512" ], "mac_algorithms": [
"hmac_sha2_512_etm", "umac_128_etm" ], "host_key_algorithms": [
"ecdsa_sha2_nistp256", "ssh_rsa", "ssh_ed25519", "rsa_sha2_256",
"rsa_sha2_512"], "max_authentication_retry_count": 3,
"is_rsa_in_publickey_algorithms_enabled": true , "login_grace_time": 30 }'
```

Updating the SSH connection limits

Specify the connection limits in the body of the PATCH request.

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

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/ssh" -d '{
"connections_per_second": 8, "max_instances": 10, "per_source_limit": 5 }'
```

Retrieving the cluster SSH server configuration

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

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

# The response:
{
"ciphers": [
  "aes256_ctr",
  "aes192_ctr"
],
"key_exchange_algorithms": [
  "diffie_hellman_group_exchange_sha256",
  "ecdh_sha2_nistp256",
  "diffie_hellman_group18_sha512"
],
"mac_algorithms": [
  "hmac_sha2_512_etm",
  "umac_128_etm"
],
"host_key_algorithms": [
  "ecdsa_sha2_nistp256",
  "ssh_rsa",
  "ssh_ed25519",
  "rsa_sha2_256",
  "rsa_sha2_512"
],
"max_authentication_retry_count": 3,
"connections_per_second": 8,
"max_instances": 10,
"is_rsa_in_publickey_algorithms_enabled": true,
"login_grace_time": 30,
"per_source_limit": 5,
"_links": {
  "self": {
    "href": "/api/security/ssh"
  }
}
}
```

Retrieve cluster SSH server ciphers, MAC algorithms, key exchange algorithms, and connection limits

GET `/security/ssh`

Introduced In: 9.7

Retrieves the cluster SSH server ciphers, MAC algorithms, key exchange algorithms, host key algorithms, connection limits, login grace time, and *ssh-rsa* enabled status for public key algorithms.

Related ONTAP commands

- `security ssh`
- `security protocol ssh`

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
ciphers	array[string]	Ciphers for encrypting the data.
connections_per_second	integer	Maximum connections allowed per second.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithms 'ssh_ed25519' and 'ssh_rsa' 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
login_grace_time	integer	The SSH connection login grace time allowed for the connection.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
max_instances	integer	Maximum possible simultaneous connections.
per_source_limit	integer	Maximum connections from the same client host.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "host_key_algorithms": [
    "ecdsa_sha2_nistp256",
    "ssh_rsa",
    "rsa_sha2_256",
    "rsa_sha2_512"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256",
    "diffie_hellman_group18_sha512"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


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


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

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

Update the SSH server setting for a cluster

PATCH `/security/ssh`

Introduced In: 9.7

Updates the SSH server setting for a cluster.

Optional parameters

- `ciphers` - Encryption algorithms for the payload
- `key_exchange_algorithms` - SSH key exchange algorithms

- `mac_algorithms` - MAC algorithms
- `host_key_algorithms` - Host key algorithms
- `max_authentication_retry_count` - Maximum authentication retries allowed before closing the connection
- `connections_per_second` - Maximum allowed connections per second
- `max_instances` - Maximum allowed connections per node
- `is_rsa_in_publickey_algorithms_enabled` - *ssh-rsa* enabled status for public key algorithms
- `login_grace_time` - The SSH connection login grace time
- `per_source_limit` - Maximum allowed connections from the same client host

Related ONTAP commands

- `security ssh`
- `security protocol ssh`

Request Body

Name	Type	Description
ciphers	array[string]	Ciphers for encrypting the data.
connections_per_second	integer	Maximum connections allowed per second.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithms 'ssh_ed25519' and 'ssh_rsa' 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
login_grace_time	integer	The SSH connection login grace time allowed for the connection.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.
max_instances	integer	Maximum possible simultaneous connections.
per_source_limit	integer	Maximum connections from the same client host.

Example request

```
{
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "host_key_algorithms": [
    "ecdsa_sha2_nistp256",
    "ssh_rsa",
    "rsa_sha2_256",
    "rsa_sha2_512"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256",
    "diffie_hellman_group18_sha512"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ]
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
10682372	There must be at least one key exchange algorithm associated with the SSH configuration.
10682373	There must be at least one cipher associated with the SSH configuration.
10682375	Failed to modify SSH key exchange algorithms.
10682378	Failed to modify SSH ciphers.
10682399	Key exchange algorithm not supported in FIPS enabled mode.
10682400	Failed to modify SSH MAC algorithms.
10682401	MAC algorithm not supported in FIPS enabled mode.
10682403	There must be at least one MAC algorithm with the SSH configuration.
10682413	Failed to modify maximum authentication retry attempts.
10682413	Failed to modify maximum authentication retry attempts.
10682418	Cipher not supported in FIPS enabled mode.
10682423	There must be at least one host key algorithm associated with the SSH configuration.
10682424	Host key algorithm not supported in FIPS enabled mode.
10682425	Failed to modify Host key algorithms.
10682426	Failed to modify *ssh-rsa* enabled status for publickey algorithms configuration.
10682426	Failed to modify the SSH connection login grace time.
10682428	Cipher not supported in FIPS enabled mode.

Error Code	Description
10682429	Adding 'diffie_hellman_group16_sha512' or 'diffie_hellman_group18_sha512' to the SSH key exchange algorithms list requires an effective cluster version of ONTAP 9.16.1 or later.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

cluster_ssh_server

Name	Type	Description
ciphers	array[string]	Ciphers for encrypting the data.
connections_per_second	integer	Maximum connections allowed per second.
host_key_algorithms	array[string]	Host key algorithms. The host key algorithms 'ssh_ed25519' and 'ssh_rsa' 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.
login_grace_time	integer	The SSH connection login grace time allowed for the connection.
mac_algorithms	array[string]	MAC algorithms.
max_authentication_retry_count	integer	Maximum authentication retries allowed before closing the connection.

Name	Type	Description
max_instances	integer	Maximum possible simultaneous connections.
per_source_limit	integer	Maximum connections from the same client host.

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