security ssh commands

ONTAP commands

NetApp
February 03, 2026

Table of Contents

security ssh commands

security ssh add

Add SSH configuration options

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The ` security ssh add ` command adds additional SSH key exchange algorithms or ciphers or MAC algorithms to the existing configurations of the cluster or a Vserver. The added algorithms or ciphers or MAC algorithms are enabled on the cluster or Vserver. If you change the cluster configuration settings, it is used as the default for all newly created Vservers. The existing SSH key exchange algorithms, ciphers, and MAC algorithms remain unchanged in the configuration. If the SSH key exchange algorithms or ciphers or MAC algorithms are already enabled in the current configuration, the command will does not not fail. ONTAP supports the *diffie-hellman-group-exchange-sha256* , *diffie-hellman-group16-sha512* and *diffie-hellman-group18-sha512* key exchange algorithms for SHA-2. ONTAP also supports the *diffie-hellman-group-exchange-sha1* , *diffie-hellman-group14-sha1* , and *diffie-hellman-group1-sha1* SSH key exchange algorithms for SHA-1. The SHA-2 key exchange algorithm is more secure than the SHA-1 key exchange algorithms. ONTAP also supports *ecdh-sha2-nistp256* , *ecdh-sha2-nistp384* , *ecdh-sha2-nistp521* , and *curve25519-sha256* . ONTAP also supports the AES and 3DES symmetric encryptions (also known as ciphers) of the following types: *aes256-ctr* , *aes192-ctr* , *aes128-ctr* , *aes256-cbc* , *aes192-cbc* , *aes128-cbc* , *aes128-gcm* , *aes256-gcm* , and *3des-cbc* . ONTAP supports MAC algorithms of the following types: *hmac-sha1* , *hmac-sha1-96* , *hmac-md5* , *hmac-md5-96* , *umac-64* , *umac-64* , *umac-128* , *hmac-sha2-256* , *hmac-sha2-512* , *hmac-sha1-etm* , *hmac-sha1-96-etm* , *hmac-sha2-256-etm* , *hmac-sha2-512-etm* , *hmac-md5-etm* , *hmac-md5-96-etm* , *umac-64-etm* , and *umac-128-etm* .

Parameters

-vserver <Vserver Name> - Vserver

Identifies the Vserver to which you want to add additional SSH key exchange algorithms or ciphers.

[-key-exchange-algorithms <algorithm name>,…] - List of SSH Key Exchange Algorithms to Add

Adds the specified SSH key exchange algorithm or algorithms to the Vserver.

[-ciphers <cipher name>,…] - List of SSH Ciphers to Add

Adds the specified cipher or ciphers to the Vserver.

[-mac-algorithms <MAC name>,…] - List of SSH MAC Algorithms to Add

Adds the specified MAC algorithm or algorithms to the Vserver.

[-host-key-algorithms <HostKey Algorithms>,…] - List of SSH Host Key Algorithms to Add

Adds the specified host key algorithms to the Vserver.

Examples

The following command adds the *diffie-hellman-group-exchange-sha256* and *diffie-hellman-*

group-exchange-sha1 key exchange algorithms for the cluster1 Vserver. It also adds the *aes256-cbc* and *aes192-cbc* ciphers and the *hmac-sha1* and *hmac-sha2-256* MAC algorithms to the cluster1 Vserver.

```
cluster1::> security ssh add -vserver cluster1 -key-exchange-algorithms
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
-ciphers aes256-cbc,aes192-cbc -mac-algorithms hmac-sha1,hmac-sha2-256
-host-key-algorithms ecdsa-sha2-nistp256,ssh-rsa
```

security ssh modify

Modify SSH configuration options

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security ssh modify` command replaces the existing configurations of the SSH key exchange algorithms, ciphers, MAC algorithms, maximum authentication retry count, host key algorithms and whether *ssh-rsa* signature scheme is enabled for RSA keys in publickey algorithms, for the cluster or a Vserver, with the configuration settings you specify. If you modify the cluster configuration settings, it will be used as the default for all newly created Vservers. ONTAP supports the *diffie-hellman-group-exchange-sha256* , *diffie-hellman-group16-sha512* and *diffie-hellman-group18-sha512* key exchange algorithms for SHA-2. ONTAP also supports the *diffie-hellman-group-exchange-sha1* , *diffie-hellman-group14-sha1* and *diffie-hellman-group1-sha1* SSH key exchange algorithms for SHA-1. The SHA-2 key exchange algorithm is more secure than the SHA-1 key exchange algorithms. ONTAP also supports the AES and 3DES symmetric encryptions (also known as ciphers) of the following types: *aes256-ctr* , *aes192-ctr* , *aes128-ctr* , *aes256-cbc* , *aes192-cbc* , *aes128-cbc* , *aes128-gcm* , *aes256-gcm* and *3des-cbc* . ONTAP supports MAC algorithms of the following types: *hmac-sha1* , *hmac-sha1-96* , *hmac-md5* , *hmac-md5-96* , *umac-64* , *umac-64* , *umac-128* , *hmac-sha2-256* , *hmac-sha2-512* , *hmac-sha1-etm* , *hmac-sha1-96-etm* , *hmac-sha2-256-etm* , *hmac-sha2-512-etm* , *hmac-md5-etm* , *hmac-md5-96-etm* , *umac-64-etm* and *umac-128-etm* . ONTAP supports host key algorithms of the following types: *ecdsa-sha2-nistp256* , *ssh-rsa* and *ssh-ed25519* .

Parameters

-vserver <Vserver Name> - Vserver

Identifies the Vserver for which you want to replace the existing SSH configurations.

[-key-exchange-algorithms <algorithm name>,…] - Key Exchange Algorithms

Enables the specified SSH key exchange algorithm or algorithms for the Vserver. This parameter also replaces all existing SSH key exchange algorithms with the specified settings.

[-ciphers <cipher name>,…] - Ciphers

Enables the specified cipher or ciphers for the Vserver. This parameter also replaces all existing ciphers with the specified settings.

[-mac-algorithms <MAC name>,…] - MAC Algorithms

Enables the specified MAC algorithm or algorithms for the Vserver. This parameter also replaces all existing MAC algorithms with the specified settings.

[-max-authentication-retry-count <integer>] - Max Authentication Retry Count

Modifies the maximum number of authentication retry count for the Vserver.

[-host-key-algorithms <HostKey Algorithms>,…] - Host Key Algorithms

Enables the specified host key algorithm or algorithms for the Vserver. This parameter also replaces all existing host key algorithms with the specified settings.

[-is-rsa-in-publickey-algorithms-enabled {true|false}] - Is ssh-rsa in Publickey Algorithms Enabled

Modifies the flag to enable or disable *ssh-rsa* signature scheme, which is based on SHA-1 hash algorithm, for RSA keys in publickey algorithms.

Examples

The following command enables the *diffie-hellman-group-exchange-sha256* and *diffie-hellman-group14-sha1* key exchange algorithms for the "cluster1" Vserver. It also enables the *aes256-ctr* , *aes192-ctr* and *aes128-ctr* ciphers, *hmac-sha1* and *hmac-sha2-256* MAC algorithms for the "cluster1" Vserver. It also disables *ssh-rsa* signature scheme for RSA keys in publickey algorithms and modifies the maximum authentication retry count to 3 for the "cluster1" Vserver:

```
cluster1::> security ssh modify -vserver cluster1 -key-exchange-algorithms
diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1 -ciphers
aes256-ctr,aes192-ctr,aes128-ctr -mac-algorithms hmac-sha1,hmac-sha2-256
-is-rsa-in-publickey-algorithms-enabled false -max-authentication-retry
-count 3
```

security ssh prepare-to-downgrade

Downgrade the SSH configuration to be compatible with releases earlier than Data ONTAP 9.2.0.

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command downgrades the SSH configurations of all Vservers and the cluster to settings compatible with releases earlier than ONTAP 9.2.0. This command also disables the max-authentication-retry feature. You must run this command in advanced privilege mode when prompted to do so during the release downgrade. Otherwise, the release downgrade process will fail.

Examples

The following command downgrades the SSH security configurations of all Vservers and the cluster to settings compatible with releases earlier than ONTAP 9.2.0.

```
cluster1::*> security ssh prepare-to-downgrade
```

security ssh remove

Remove SSH configuration options

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The ` security ssh remove` command removes the specified SSH key exchange algorithms or ciphers from the existing configurations of the cluster or a Vserver. The removed algorithms or ciphers are disabled on the cluster or Vserver. If you changed the cluster configuration settings, it will be used as the default for all newly created Vservers. If the SSH key exchange algorithms or ciphers that you specify with this command are not currently enabled, the command does not fail. ONTAP supports the *diffie-hellman-group-exchange-sha256* , *diffie-hellman-group16-sha512* and *diffie-hellman-group18-sha512* key exchange algorithms for SHA-2. ONTAP also supports the *diffie-hellman-group-exchange-sha1* , *diffie-hellman-group14-sha1* , and *diffie-hellman-group1-sha1* SSH key exchange algorithms for SHA-1. The SHA-2 key exchange algorithm is more secure than the SHA-1 key exchange algorithms. ONTAP also supports *ecdh-sha2-nistp256* , *ecdh-sha2-nistp384* , *ecdh-sha2-nistp521* , and *curve25519-sha256* . ONTAP also supports the AES and 3DES symmetric encryption (also known as ciphers) of the following types: *aes256-ctr* , *aes192-ctr* , *aes128-ctr* , *aes256-cbc* , *aes192-cbc* , *aes128-cbc* , *aes128-gcm* , *aes256-gcm* and *3des-cbc* . ONTAP supports MAC algorithms of the following types: *hmac-sha1* , *hmac-sha1-96* , *hmac-md5* , *hmac-md5-96* , *umac-64* , *umac-64* , *umac-128* , *hmac-sha2-256* , *hmac-sha2-512* , *hmac-sha1-etm* , *hmac-sha1-96-etm* , *hmac-sha2-256-etm* , *hmac-sha2-512-etm* , *hmac-md5-etm* , *hmac-md5-96-etm* , *umac-64-etm* , and *umac-128-etm* .

Parameters

-vserver <Vserver Name> - Vserver

Identifies the Vserver from which you want to remove the SSH key exchange algorithms or ciphers.

[-key-exchange-algorithms <algorithm name>,…] - List of SSH Key Exchange Algorithms to Remove

Removes the specified key exchange algorithm or algorithms from the Vserver.

[-ciphers <cipher name>,…] - List of SSH Ciphers to Remove

Removes the specified cipher or ciphers from the Vserver.

[-mac-algorithms <MAC name>,…] - List of SSH MAC Algorithms to Remove

Removes the specified MAC algorithm or algorithms from the Vserver.

[-host-key-algorithms <HostKey Algorithms>,…] - List of SSH Host Key Algorithms to Remove

Removes the specified host key algorithms from the Vserver.

Examples

The following command removes the *diffie-hellman-group1-sha1* and *diffie-hellman-group-exchange-sha1* key exchange algorithms from the cluster1 Vserver. It also removes the *aes128-cbc* and *3des-cbc* ciphers and the *hmac-sha1-96* and *hmac-sha2-256* MAC algorithms from the cluster1 Vserver.

```
cluster1::> security ssh remove -vserver cluster1 -key-exchange-algorithms
diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha1 -ciphers
aes128-cbc,3des-cbc -mac-algorithms hmac-sha1-96,hmac-sha2-256
```

security ssh show

Display SSH configuration options

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

```
The ` security ssh show` command displays the configurations of the SSH
key exchange algorithms, ciphers, MAC algorithms, maximum authentication
retry count, host key algorithms and whether ``_ssh-rsa_`` signature
scheme is enabled for RSA keys in publickey algorithms, for the cluster
and Vservers. The SSH protocol uses a Diffie-Hellman based key exchange
method to establish a shared secret key during the SSH negotiation phrase.
The key exchange method specifies how one-time session keys are generated
for encryption and authentication and how the server authentication takes
place. ONTAP supports the ``_diffie-hellman-group-exchange-sha256_`` ,
``_diffie-hellman-group16-sha512_`` and ``_diffie-hellman-group18-
sha512_`` key exchange algorithms for SHA-2. ONTAP also supports the
``_diffie-hellman-group-exchange-sha1_`` , ``_diffie-hellman-group14-
sha1_`` , and ``_diffie-hellman-group1-sha1_`` key exchange algorithms for
SHA-1. ONTAP also supports ``_ecdh-sha2-nistp256_`` , ``_ecdh-sha2-
nistp384_`` , ``_ecdh-sha2-nistp521_`` and ``_curve25519-sha256_`` . ONTAP
also supports the AES and 3DES symmetric encryptions (also known as
ciphers) of the following types: ``_aes256-ctr_`` , ``_aes192-ctr_`` ,
``_aes128-ctr_`` , ``_aes256-cbc_`` , ``_aes192-cbc_`` , ``_aes128-cbc_``
, ``_aes128-gcm_`` , ``_aes256-gcm_`` and ``_3des-cbc_`` . ONTAP supports
MAC algorithms of the following types: ``_hmac-sha1_`` , ``_hmac-sha1-
96_`` , ``_hmac-md5_`` , ``_hmac-md5-96_`` , ``_umac-64_`` , ``_umac-
128_`` , ``_hmac-sha2-256_`` , ``_hmac-sha2-512_`` , ``_hmac-sha1-etm_`` ,
``_hmac-sha1-96-etm_`` , ``_hmac-sha2-256-etm_`` , ``_hmac-sha2-512-etm_``
, ``_hmac-md5-etm_`` , ``_hmac-md5-96-etm_`` , ``_umac-64-etm_`` and
``_umac-128-etm_`` . ONTAP supports host key algorithms of the following
types: ``_ecdsa-sha2-nistp256_`` , ``_ssh-rsa_`` and ``_ssh-ed25519_`` .
```

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Identifies the Vserver for which you want to display the SSH key exchange algorithms, ciphers, MAC algorithms, maximum authentication retry count, host key algorithms and whether *ssh-rsa* signature scheme is enabled for RSA keys in publickey algorithms.

[-key-exchange-algorithms <algorithm name>,…] - Key Exchange Algorithms

Displays the Vserver or Vservers that have the specified key exchange algorithms enabled.

[-ciphers <cipher name>,…] - Ciphers

Displays the Vserver or Vservers that have the specified ciphers enabled.

[-mac-algorithms <MAC name>,…] - MAC Algorithms

Displays the Vserver or Vservers that have the specified MAC algorithm or algorithms.

[-max-authentication-retry-count <integer>] - Max Authentication Retry Count

Displays Vservers with a matching maximum authentication retry count value. The default value of this parameter is *6* .

[-host-key-algorithms <HostKey Algorithms>,…] - Host Key Algorithms

Displays Vservers with matching host key algorithms.

[-is-rsa-in-publickey-algorithms-enabled {true|false}] - Is ssh-rsa in Publickey Algorithms Enabled

Identifies whether *ssh-rsa* signature scheme, which uses the SHA-1 hash algorithm, is enabled or disabled for RSA keys in publickey algorithms. The default value of this parameter is *true* .

Examples

The following command displays the enabled SSH ciphers, key exchange algorithms, MAC algorithms, host key algorithms, whether *ssh-rsa* signature scheme is enabled for RSA keys in publickey algorithms and maximum number of authentication retry count for the cluster and all Vservers. The cluster settings are used as the default for all newly created Vservers:

```
cluster1::> security ssh show

Is ssh-rsa   Max

in Publickey Auth
                            Key Exchange   MAC            Host Key
Algorithms   Retry
Vserver        Ciphers      Algorithms     Algorithms     Algorithms
Enabled      Count
-------------- ------------ -------------- -------------- --------------
------------ -----
cluster1       aes256-ctr,  curve25519-    hmac-sha1-etm, ecdsa-sha2-
false            4
               3des-cbc     sha256,        hmac-sha2-256- nistp256
                            diffie-        etm,
                            hellman-       hmac-sha2-512
                            group16-sha512
Is ssh-rsa   Max

in Publickey Auth
                            Key Exchange   MAC            Host Key
Algorithms   Retry
Vserver        Ciphers      Algorithms     Algorithms     Algorithms
Enabled      Count
-------------- ------------ -------------- -------------- --------------
------------ -----
vs1            aes256-ctr,  diffie-        hmac-sha2-256, ecdsa-sha2-
true             6
               aes192-ctr,  hellman-group- hmac-sha2-512, nistp256,
               aes128-ctr,  exchange-      hmac-sha2-256- ssh-rsa,
               aes128-gcm,  sha256,        etm,           ssh-ed25519
               aes256-gcm   ecdh-sha2-     hmac-sha2-512-
                            nistp256,      etm, umac-64,
                            ecdh-sha2-     umac-128,
                            nistp384,      umac-64-etm,
                            ecdh-sha2-     umac-128-etm
                            nistp521,
                            curve25519-
                            sha256
2 entries were displayed.
```

Copyright information

Trademark information