security ssh commands

ONTAP commands

NetApp
February 04, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-95/security-ssh-add.html on February 04, 2026. Always check docs.netapp.com for the latest.

Table of Contents

security ssh commands . . . 1
- security ssh add . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 1
- security ssh modify . . . 2
  - Description . . . 2
  - Parameters . . . 2
  - Examples . . . 3
- security ssh prepare-to-downgrade . . . 3
  - Description . . . 3
  - Examples . . . 3
- security ssh remove . . . 3
  - Description . . . 3
  - Parameters . . . 4
  - Examples . . . 4
- security ssh show . . . 4
  - Description . . . 4
  - Parameters . . . 5
  - Examples . . . 6

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. Data ONTAP supports the *diffie-hellman-group-exchange-sha256* key exchange algorithm for SHA-2. Data 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. Data ONTAP also supports *ecdh-sha2-nistp256* , *ecdh-sha2-nistp384* , *ecdh-sha2-nistp521* , and *curve25519-sha256* . Data 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* . Data ONTAP supports MAC algorithms of the following types: *hmac-sha1* , *hmac-sha1-96* , *hmac-md5* , *hmac-md5-96* , *hmac-ripemd160* , *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* , *hmac-ripemd160-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.

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
```

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 or ciphers or MAC 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. Data ONTAP supports the *diffie-hellman-group-exchange-sha256* key exchange algorithm for SHA-2. Data 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. Data 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* . Data ONTAP supports MAC algorithms of the following types: *hmac-sha1* , *hmac-sha1-96* , *hmac-md5* , *hmac-md5-96* , *hmac-ripemd160* , *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* , *hmac-ripemd160-etm* , *umac-64-etm* , and *umac-128-etm* .

Parameters

-vserver <Vserver Name> - Vserver

Identifies the Vserver for which you want to replace the existing SSH key exchange algorithm and cipher 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.

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 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
-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 Data 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 Data 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 is 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 will notdoes not fail. Data ONTAP supports the *diffie-hellman-group-exchange-sha256* key exchange algorithm for SHA-2. Data 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. Data ONTAP also supports *ecdh-sha2-nistp256* , *ecdh-sha2-nistp384* , *ecdh-sha2-nistp521* , and *curve25519-sha256* . Data 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* . Data ONTAP supports MAC algorithms of the following types: *hmac-sha1* , *hmac-sha1-96* , *hmac-md5* , *hmac-md5-96* , *hmac-ripemd160* , *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* , *hmac-ripemd160-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.

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 and maximum
authentication retry count 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. Data ONTAP
supports the ``_diffie-hellman-group-exchange-sha256_`` key exchange
algorithm for SHA-2. Data ONTAP also supports the ``_diffie-hellman-group-
exchange-sha1_`` , ``_diffie-hellman-group14-sha1_`` , and ``_diffie-
hellman-group1-sha1_`` key exchange algorithms for SHA-1. Data ONTAP also
supports ``_ecdh-sha2-nistp256_`` , ``_ecdh-sha2-nistp384_`` , ``_ecdh-
sha2-nistp521_`` , ``_curve25519-sha256_`` . Data 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_`` . Data ONTAP supports MAC algorithms
of the following types: ``_hmac-sha1_`` , ``_hmac-sha1-96_`` , ``_hmac-
md5_`` , ``_hmac-md5-96_`` , ``_hmac-ripemd160_`` , ``_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_`` ,
``_hmac-ripemd160-etm_`` , ``_umac-64-etm_`` , ``_umac-128-etm_``
```

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 algorithm, cipher, and MAC algorithm configurations.

[-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.

Examples

The following command displays the enabled SSH key exchange algorithms, ciphers, MAC 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:

```
cluster-1::> security ssh show
                            Key Exchange  MAC              Max
Authentication
Vserver        Ciphers     Algorithms    Algorithms              Retry
Count
-------------- ----------  ------------  --------------
------------------
cluster-1      3des-cbc    diffie-       hmac-sha1
4
                           hellman-
                           group-
                           exchange-
                           sha256
vs1            aes256-     diffie-       hmac-sha1,
6
               ctr,        hellman-      hmac-sha1-96,
               aes192-     group-        hmac-sha2-256,
               ctr,        exchange-     hmac-sha2-512,
               aes128-     sha256,       hmac-sha1-etm,
               ctr,        diffie-       hmac-sha1-96-
               aes256-     hellman-      etm,
               cbc,        group-        hmac-sha2-256-
               aes192-     exchange-     etm,
               cbc,        sha1,         hmac-sha2-512-
               aes128-     diffie-       etm, hmac-md5,
               cbc,        hellman-      hmac-md5-96,
               3des-cbc,   group14-      hmac-
               aes128-     sha1,         ripemd160,
               gcm,        ecdh-sha2-    umac-64,
               aes256-gcm  nistp256,     umac-128,
                           ecdh-sha2-    hmac-md5-etm,
                           nistp384,     hmac-md5-96-
                           ecdh-sha2-    etm,
                           nistp521,     hmac-
                           curve25519-   ripemd160-etm,
                           sha256        umac-64-etm,
                                         umac-128-etm
2 entries were displayed.
```

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.