



Manage SSH server

ONTAP 9.7 REST API reference

NetApp
August 29, 2024

Table of Contents

- Manage SSH server 1
 - Security SSH endpoint overview 1
 - Retrieve cluster SSH server ciphers, MAC algorithms, key exchange algorithms, and connection limits . . . 3
 - Update the SSH server setting for a cluster 6

Manage SSH server

Security SSH endpoint overview

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 and maximum authentication retry attempts allowed before closing the connection) and SSH connection limits.

The security algorithms include SSH key exchange algorithms, ciphers for payload encryption, and MAC 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", "diffie_hellman_group14_sha1" ],
  "mac_algorithms": [ "hmac_sha2_512_etm", "umac_128_etm" ],
  "max_authentication_retry_count": 3 }'
```

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",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha2_512_etm",
    "umac_128_etm"
  ],
  "max_authentication_retry_count": 3,
  "connections_per_second": 8,
  "max_instances": 10,
  "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

Retrieves the cluster SSH server ciphers, MAC algorithms, key exchange algorithms, and connection limits.

Related ONTAP commands

- `security ssh`
- `security protocol ssh`

Learn more

- [DOC /security/ssh](#)

Response

Status: 200, Ok

| Name | Type | Description |
|---|----------------------------|---|
| <code>_links</code> | <code>_links</code> | |
| <code>ciphers</code> | <code>array[string]</code> | Ciphers for encrypting the data. |
| <code>connections_per_second</code> | <code>integer</code> | Maximum connections allowed per second. |
| <code>key_exchange_algorithms</code> | <code>array[string]</code> | Key exchange algorithms. |
| <code>mac_algorithms</code> | <code>array[string]</code> | MAC algorithms. |
| <code>max_authentication_retry_count</code> | <code>integer</code> | Maximum authentication retries allowed before closing the connection. |
| <code>max_instances</code> | <code>integer</code> | Maximum possible simultaneous connections. |
| <code>per_source_limit</code> | <code>integer</code> | Maximum connections from the same client host. |

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "hmac_sha2_512_etm"
  ]
}
```

Error

Status: Default, Error

| Name | Type | Description |
|-------|-------|-------------|
| error | 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 |

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

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
- `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
- `per_source_limit` - Maximum allowed connections from the same client host

Related ONTAP commands

- `security ssh`
- `security protocol ssh`

Learn more

- [DOC /security/ssh](#)

Parameters

| Name | Type | In | Required | Description |
|-----------------------------|---------|-------|----------|---|
| <code>return_records</code> | boolean | query | False | The default is false. If set to true, the records are returned. |

Request Body

| Name | Type | Description |
|---|------------------------|---|
| <code>_links</code> | _links | |
| <code>ciphers</code> | array[string] | Ciphers for encrypting the data. |
| <code>connections_per_second</code> | integer | Maximum connections allowed per second. |
| <code>key_exchange_algorithms</code> | array[string] | Key exchange algorithms. |
| <code>mac_algorithms</code> | array[string] | MAC algorithms. |
| <code>max_authentication_retry_count</code> | integer | Maximum authentication retries allowed before closing the connection. |
| <code>max_instances</code> | integer | Maximum possible simultaneous connections. |
| <code>per_source_limit</code> | integer | Maximum connections from the same client host. |

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "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. |

| Error Code | Description |
|------------|--|
| 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. |

| Name | Type | Description |
|-------|-------|-------------|
| error | 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 | |

cluster_ssh_server

| Name | Type | Description |
|--------------------------------|------------------------|---|
| _links | _links | |
| ciphers | array[string] | Ciphers for encrypting the data. |
| connections_per_second | integer | Maximum connections allowed per second. |
| 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. |
| 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 |

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

Copyright © 2024 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.