Manage cluster NTP keys

REST API reference

NetApp
September 12, 2025

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9111/cluster_ntp_keys_endpoint_overview.html on September 12, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Manage cluster NTP keys . . . 1
- Cluster NTP keys endpoint overview . . . 1
  - Overview . . . 1
  - Example . . . 1
- Retrieve NTP symmetric authentication keys . . . 1
  - Related ONTAP commands . . . 1
  - Learn more . . . 2
  - Parameters . . . 2
  - Response . . . 3
  - Error . . . 4
  - Definitions . . . 4
- Create an NTP symmetric authentication key entry . . . 6
  - Required properties . . . 6
  - Related ONTAP commands . . . 6
  - Learn more . . . 6
  - Parameters . . . 6
  - Request Body . . . 7
  - Response . . . 7
  - Error . . . 8
  - Definitions . . . 8
- Delete an NTP key . . . 10
  - Related ONTAP commands . . . 10
  - Learn more . . . 10
  - Parameters . . . 10
  - Response . . . 10
  - Error . . . 10
  - Definitions . . . 11
- Retrieve NTP symmetric authentication key details . . . 12
  - Related ONTAP commands . . . 12
  - Learn more . . . 12
  - Parameters . . . 12
  - Response . . . 12
  - Error . . . 13
  - Definitions . . . 14
- Update NTP symmetric authentication key details . . . 15
  - Required properties . . . 15
  - Related ONTAP commands . . . 16
  - Learn more . . . 16
  - Parameters . . . 16
  - Request Body . . . 16
  - Response . . . 16
  - Error . . . 17
  - Definitions . . . 17

Manage cluster NTP keys

Cluster NTP keys endpoint overview

Overview

You can configure NTP to use shared private keys between ONTAP and trusted external NTP time servers.

You acquire the keys from the external NTP time servers and individual entries created for each unique key. You can use the /cluster/ntp/servers API to associate a key with an external NTP time server used by ONTAP and enable authentication.

Fields used for adding an NTP shared key

The required fields are:

- `id`
- `digest_type`
- `secret_key`

Example

```
# Body
create_ntp_key.txt(body):
{
"id": 10,
"digest_type": "sha1",
"value": "da39a3ee5e6b4b0d3255bfef95601890afd80709"
}

# Request
curl -X POST "https://<mgmt-ip>/api/cluster/ntp/keys" -d
"@create_ntp_key.txt"
```

Retrieve NTP symmetric authentication keys

GET `/cluster/ntp/keys`

Introduced In: 9.7

Retrieves the collection of NTP symmetric authentication keys known by ONTAP that are uniquely indexed by an identifier.

Related ONTAP commands

- `cluster time-service ntp key show`

Learn more

- DOC /cluster/ntp/keys

Parameters

Name	Type	In	Required	Description
value	string	query	False	Filter by value
id	integer	query	False	Filter by id • Max value: 65535 • Min value: 1
digest_type	string	query	False	Filter by digest_type
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 1

Name	Type	In	Required	Description
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records.
records	array[ntp_key]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "digest_type": "sha1",
      "id": 10,
      "value": "da39a3ee5e6b4b0d3255bfef95601890afd80709"
    }
  ]
}
```

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
next	href	
self	href	

_links

Name	Type	Description
self	href	

ntp_key

Name	Type	Description
_links	_links	
digest_type	string	The type of cryptographic hash used to create and verify the NTP's message authentication code appended to each NTP packet header.
id	integer	NTP symmetric authentication key identifier or index number (ID). This ID is included in the NTP cryptographic hash encoded header.
value	string	A hexadecimal digit string that represents the cryptographic key that is shared with the remote NTP server. The current expected length is 40 characters. Use the cryptographic key and key ID to create a unique hash value used to authenticate the rest of the NTP data.

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.

Create an NTP symmetric authentication key entry

POST `/cluster/ntp/keys`

Introduced In: 9.7

Creates an NTP symmetric authentication key entry including the type of key using an unused identifier or index number (ID).

Required properties

- `id` - Shared symmetric key number (ID).
- `digest_type` - Shared private key cryptographic hash type.
- `value` - Value of shared private key.

Related ONTAP commands

- `cluster time-service ntp key create`

Learn more

- DOC /cluster/ntp/keys

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
digest_type	string	The type of cryptographic hash used to create and verify the NTP's message authentication code appended to each NTP packet header.
id	integer	NTP symmetric authentication key identifier or index number (ID). This ID is included in the NTP cryptographic hash encoded header.
value	string	A hexadecimal digit string that represents the cryptographic key that is shared with the remote NTP server. The current expected length is 40 characters. Use the cryptographic key and key ID to create a unique hash value used to authenticate the rest of the NTP data.

Example request

```
{
  "digest_type": "sha1",
  "id": 10,
  "value": "da39a3ee5e6b4b0d3255bfef95601890afd80709"
}
```

Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
2097187	Invalid value for an NTP symmetric authentication key. A SHA1 key must be exactly 40 hexadecimal digits.
2097189	Too many NTP keys have been configured.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ntp_key

Name	Type	Description
digest_type	string	The type of cryptographic hash used to create and verify the NTP's message authentication code appended to each NTP packet header.
id	integer	NTP symmetric authentication key identifier or index number (ID). This ID is included in the NTP cryptographic hash encoded header.
value	string	A hexadecimal digit string that represents the cryptographic key that is shared with the remote NTP server. The current expected length is 40 characters. Use the cryptographic key and key ID to create a unique hash value used to authenticate the rest of the NTP data.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete an NTP key

DELETE `/cluster/ntp/keys/{id}`

Introduced In: 9.7

Deletes an NTP key.

Related ONTAP commands

- `cluster time-service ntp key delete`

Learn more

- DOC /cluster/ntp/keys

Parameters

Name	Type	In	Required	Description
id	integer	path	True	Key identifier

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
2097186	The key cannot be deleted because it is being used by an NTP server.

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

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.

Retrieve NTP symmetric authentication key details

GET `/cluster/ntp/keys/{id}`

Introduced In: 9.7

Retrieves the details of a specific NTP symmetric authentication key by numeric identifier or index (ID).

Related ONTAP commands

- `cluster time-service ntp key show`

Learn more

- DOC /cluster/ntp/keys

Parameters

Name	Type	In	Required	Description
id	integer	path	True	Key identifier
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
digest_type	string	The type of cryptographic hash used to create and verify the NTP's message authentication code appended to each NTP packet header.
id	integer	NTP symmetric authentication key identifier or index number (ID). This ID is included in the NTP cryptographic hash encoded header.

Name	Type	Description
value	string	A hexadecimal digit string that represents the cryptographic key that is shared with the remote NTP server. The current expected length is 40 characters. Use the cryptographic key and key ID to create a unique hash value used to authenticate the rest of the NTP data.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "digest_type": "sha1",
  "id": 10,
  "value": "da39a3ee5e6b4b0d3255bfef95601890afd80709"
}
```


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 NTP symmetric authentication key details

PATCH `/cluster/ntp/keys/{id}`

Introduced In: 9.7

Updates the details of a specific NTP symmetric authentication key by numeric identifier or index (ID).

Required properties

- `digest_type` - Shared private key cryptographic hash type.
- `value` - Value of shared private key.

Related ONTAP commands

- `cluster time-service ntp key modify`

Learn more

- DOC /cluster/ntp/keys

Parameters

Name	Type	In	Required	Description
id	integer	path	True	Key identifier

Request Body

Name	Type	Description
digest_type	string	The type of cryptographic hash used to create and verify the NTP's message authentication code appended to each NTP packet header.
value	string	A hexadecimal digit string that represents the cryptographic key that is shared with the remote NTP server. The current expected length is 40 characters. Use the cryptographic key and key ID to create a unique hash value used to authenticate the rest of the NTP data.

Example request

```
{
  "digest_type": "sha1",
  "value": "da39a3ee5e6b4b0d3255bfef95601890afd80709"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
2097187	An invalid SHA1 key was provided.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ntp_key

Name	Type	Description
digest_type	string	The type of cryptographic hash used to create and verify the NTP's message authentication code appended to each NTP packet header.
value	string	A hexadecimal digit string that represents the cryptographic key that is shared with the remote NTP server. The current expected length is 40 characters. Use the cryptographic key and key ID to create a unique hash value used to authenticate the rest of the NTP data.

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

Name	Type	Description
target	string	The target parameter that caused the error.

Copyright information

Copyright © 2025 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.