



Manage SAML service

ONTAP 9.14.1 REST API reference

NetApp
May 23, 2024

Table of Contents

- Manage SAML service 1
 - Security authentication cluster saml-sp endpoint overview 1
 - Delete a SAML service provider configuration 3
 - Retrieve a SAML service provider configuration 4
 - Update a SAML service provider configuration 9
 - Create a SAML service provider configuration 13

Manage SAML service

Security authentication cluster saml-sp endpoint overview

Overview

This API is used to retrieve and display relevant information pertaining to the SAML service provider configuration in the cluster. The POST request creates a SAML service provider configuration if there is none present. The DELETE request removes the SAML service provider configuration. The PATCH request enables and disables SAML in the cluster. Various responses are shown in the examples below.

Examples

Retrieving the SAML service provider configuration in the cluster

The following output shows the SAML service provider configuration in the cluster.

```
# The API:
/api/security/authentication/cluster/saml-sp

# The call:
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp" -H "accept: application/hal+json"

# The response:
{
  "idp_uri": "https://examplelab.customer.com/idp/Metadata",
  "enabled": true,
  "host": "172.21.74.181",
  "certificate": {
    "ca": "cluster1",
    "serial_number": "156F10C3EB4C51C1",
    "common_name": "cluster1"
  },
  "_links": {
    "self": {
      "href": "/api/security/authentication/cluster/saml-sp"
    }
  }
}
```

Creating the SAML service provider configuration

The following output shows how to create a SAML service provider configuration in the cluster.

```
# The API:
/api/security/authentication/cluster/saml-sp

# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp?return_records=true" -H "accept: application/hal+json" -d '{ "idp_uri": "https://examplelab.customer.com/idp/Metadata", "host": "172.21.74.181", "certificate": { "ca": "cluster1", "serial_number": "156F10C3EB4C51C1" } }'
```

Updating the SAML service provider configuration

The following output shows how to enable a SAML service provider configuration in the cluster.

Disabling the configuration requires the client to be authenticated through SAML prior to performing the operation.

```
# The API:
/api/security/authentication/cluster/saml-sp

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp/" -d '{ "enabled": true }'
```

Deleting the SAML service provider configuration

```
# The API:
/api/security/authentication/cluster/saml-sp

# The call:
curl -X DELETE "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp/"
```

Delete a SAML service provider configuration

DELETE /security/authentication/cluster/saml-sp

Introduced In: 9.6

Deletes a SAML service provider configuration.

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|------------|--|
| 12320803 | SAML must be disabled before the configuration can be removed. |

Also see the table of common errors in the [Response body](#) overview section of this documentation.

| 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

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. |

Retrieve a SAML service provider configuration

GET /security/authentication/cluster/saml-sp

Introduced In: 9.6

Retrieves a SAML service provider configuration.

Parameters

| Name | Type | In | Required | Description |
|----------------|--------|-------|----------|---|
| certificate.ca | string | query | False | Filter by certificate.ca <ul style="list-style-type: none">• maxLength: 256• minLength: 1• Introduced in: 9.7 |

| Name | Type | In | Required | Description |
|---------------------------|---------------|-------|----------|---|
| certificate.serial_number | string | query | False | Filter by certificate.serial_number <ul style="list-style-type: none"> • maxLength: 40 • minLength: 1 • Introduced in: 9.7 |
| certificate.common_name | string | query | False | Filter by certificate.common_name <ul style="list-style-type: none"> • Introduced in: 9.7 |
| host | string | query | False | Filter by host <ul style="list-style-type: none"> • Introduced in: 9.7 |
| enabled | boolean | query | False | Filter by enabled <ul style="list-style-type: none"> • Introduced in: 9.7 |
| idp_uri | string | query | False | Filter by idp_uri <ul style="list-style-type: none"> • Introduced in: 9.7 |
| fields | array[string] | query | False | Specify the fields to return. |

Response

Status: 200, Ok

| Name | Type | Description |
|-------------|-----------------------------|--|
| _links | _links | |
| certificate | certificate | |
| enabled | boolean | The SAML service provider is enabled. Valid for PATCH and GET operations only. |

| Name | Type | Description |
|---------|--------|--|
| host | string | The SAML service provider host. |
| idp_uri | string | The identity provider (IdP) metadata location. Required for POST operations. |

Example response

```

{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-06/FederationMetadata.xml"
}

```

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 | |

certificate

| Name | Type | Description |
|---------------|--------|---|
| ca | string | Server certificate issuing certificate authority (CA). This cannot be used with the server certificate common name. |
| common_name | string | Server certificate common name. This cannot be used with the certificate authority (CA) or serial_number. |
| serial_number | string | Server certificate serial number. This cannot be used with the server certificate common name. |

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 |

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

Update a SAML service provider configuration

PATCH /security/authentication/cluster/saml-sp

Introduced In: 9.6

Updates a SAML service provider configuration.

Request Body

| Name | Type | Description |
|-------------|-----------------------------|--|
| _links | _links | |
| certificate | certificate | |
| enabled | boolean | The SAML service provider is enabled. Valid for PATCH and GET operations only. |
| host | string | The SAML service provider host. |
| idp_uri | string | The identity provider (IdP) metadata location. Required for POST operations. |

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-06/FederationMetadata.xml"
}
```

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|--|
| 12320791 | SAML can only be disabled using the console or a SAML-authenticated application. |

Also see the table of common errors in the [Response body](#) overview section of this documentation.

| 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 | |

certificate

| Name | Type | Description |
|---------------|--------|---|
| ca | string | Server certificate issuing certificate authority (CA). This cannot be used with the server certificate common name. |
| common_name | string | Server certificate common name. This cannot be used with the certificate authority (CA) or serial_number. |
| serial_number | string | Server certificate serial number. This cannot be used with the server certificate common name. |

security_saml_sp

| Name | Type | Description |
|-------------|-----------------------------|--|
| _links | _links | |
| certificate | certificate | |
| enabled | boolean | The SAML service provider is enabled. Valid for PATCH and GET operations only. |
| host | string | The SAML service provider host. |
| idp_uri | string | The identity provider (IdP) metadata location. Required for POST operations. |

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. |

Create a SAML service provider configuration

POST /security/authentication/cluster/saml-sp

Introduced In: 9.6

Creates a SAML service provider configuration. Note that "common_name" is mutually exclusive with "serial_number" and "ca" in POST. SAML will initially be disabled, requiring a patch to set "enabled" to "true", so that the user has time to complete the setup of the IdP.

Required properties

- idp_uri

Optional properties

- certificate
- enabled
- host

Parameters

| Name | Type | In | Required | Description |
|------------------------|---------|-------|----------|--|
| verify_metadata_server | boolean | query | False | Verify IdP metadata server identity. <ul style="list-style-type: none"> • Default value: 1 |
| return_timeout | integer | query | False | The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0 |

Request Body

| Name | Type | Description |
|-------------|-----------------------------|--|
| _links | _links | |
| certificate | certificate | |
| enabled | boolean | The SAML service provider is enabled. Valid for PATCH and GET operations only. |

| Name | Type | Description |
|---------|--------|--|
| host | string | The SAML service provider host. |
| idp_uri | string | The identity provider (IdP) metadata location. Required for POST operations. |

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-06/FederationMetadata.xml"
}
```

Response

Status: 202, Accepted

| Name | Type | Description |
|------|--------------------------|-------------|
| job | job_link | |

Example response

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
```

Headers

| Name | Description | Type |
|----------|---|--------|
| Location | Useful for tracking the resource location | string |

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|---|
| 12320789 | Failed to download data file from specified URI. |
| 12320794 | The host parameter provided must be the cluster management interface's IP address. If the cluster management interface is not available, the node management interface's IP address must be used. |
| 12320795 | A valid cluster or node management interface IP address must be provided. |
| 12320805 | The certificate information provided does not match any installed certificates. |
| 12320806 | The certificate information entered does not match any installed certificates. |

| Error Code | Description |
|------------|--|
| 12320814 | An invalid IDP URI has been entered. |
| 12320815 | An IDP URI must be an HTTPS or FTPS URI. |

Also see the table of common errors in the [Response body](#) overview section of this documentation.

| 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 | |

certificate

| Name | Type | Description |
|---------------|--------|---|
| ca | string | Server certificate issuing certificate authority (CA). This cannot be used with the server certificate common name. |
| common_name | string | Server certificate common name. This cannot be used with the certificate authority (CA) or serial_number. |
| serial_number | string | Server certificate serial number. This cannot be used with the server certificate common name. |

security_saml_sp

| Name | Type | Description |
|-------------|-----------------------------|--|
| _links | _links | |
| certificate | certificate | |
| enabled | boolean | The SAML service provider is enabled. Valid for PATCH and GET operations only. |
| host | string | The SAML service provider host. |
| idp_uri | string | The identity provider (IdP) metadata location. Required for POST operations. |

job_link

| Name | Type | Description |
|------------------------|------------------------|---|
| _links | _links | |
| uuid | string | The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation. |

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

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.