security saml-sp commands

ONTAP commands

NetApp
February 03, 2026

Table of Contents

security saml-sp commands

security saml-sp create

Configure SAML service provider for authentication

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

Description

The `security saml-sp create` command configures ONTAP with Security Assertion Markup Language (SAML) Service Provider (SP) for single sign-on authentication. This command does not enable SAML SP, it just configures it. Configuring and enabling SAML SP is a two-step process:

- Create a SAML SP configuration using `security saml-sp create` command.
- Enable SAML SP by using security saml-sp modify`-is-enabled` *`true`*

After the SAML SP configuration is created, it cannot be modified. It must be deleted and created again to change any settings.

This restarts the web server. Any HTTP/S connections that are active will be disrupted.

Parameters

`-idp-uri {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…}` - Identity Provider (IdP) Metadata Location

This is the URI of the desired identity provider's (IdP) metadata.

`[-sp-host <Remote InetAddress>]` - SAML Service Provider Host

This specifies the SAML service provider host IP address.

`{ -cert-ca <text>` - Server Certificate Issuing CA

This specifies the service provider's certificate issuing CA.

`-cert-serial <text>` - Server Certificate Serial Number

This specifies the service provider's certificate's serial number.

`| [-cert-common-name <FQDN or Custom Common Name>]` - Server Certificate Common Name `}`

This specifies the service provider certificate's common name.

`[-verify-metadata-server {true|false}]` - Verify IdP Metadata Server Identity

When the IdP metadata is downloaded, the identity of the server hosting the metadata is verified using Transport Layer Security (TLS), validating the server's X.509 certificate against the list of certificate authorities (CAs) in ONTAP, and verifying that the host in the server certificate matches the host in the URI (the `idp-uri` field). This verification can be bypassed by setting this field to *`false`* . Bypassing the server verification is not recommended as the server can not be trusted that way, but will be necessary to use non-TLS URIs, e.g. with the "http" scheme, or when the server certificates are self-signed. If the server's certificate was signed by a CA that is not installed in ONTAP, the security certificate install -type server-ca command can be used to install it.

[-foreground {true|false}] - Foreground Process

When this parameter is set to *false* the command runs in the background as a job. The default is *true*, which causes the command to return after the operation completes.

Examples

The following example configures ONTAP with SAML SP IdP information:

```
cluster1::> security saml-sp create -idp-uri http://public-idp-uri -sp
-host 1.1.1.1
    [Job 9] Job succeeded.
    cluster1::>
```

Related Links

- security saml-sp modify
- security certificate install

security saml-sp delete

Delete SAML service provider for authentication

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

Description

The `security saml-sp delete` command is used to remove the Security Access Markup Language (SAML) Service Provider (SP). Running this command frees resources used by the SP. SAML SP services will no longer be available after the SP is removed.

If the SAML SP is currently enabled, it is necessary to first use security saml-sp modify`-is-enabled` *false* prior to `security saml-sp delete`. The security saml-sp modify`-is-enabled` *false* command must be issued by a password authenticated console application user or from a SAML authenticated command interface.

This restarts the web server. Any HTTP/S connections that are active will be disrupted.

Examples

The following example unconfigures SAML SP:

```
cluster1::> security saml-sp delete
    cluster1::>
```

Related Links

- security saml-sp modify

security saml-sp modify

Modify SAML service provider authentication

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

Description

The `security saml-sp modify` command modifies the Security Assertion Markup Language (SAML) Service Provider (SP) configuration for single sign-on authentication. This command is used to enable or disable an existing SAML SP, `security saml-sp modify-is-enabled` *true* `or` *false*`` respectively.

This command will check the validity of the current SAML SP configuration before enabling the SP. Also, it is necessary to use this command with the `-is-enabled` *false* parameter prior to deleting an existing SAML SP configuration. SAML SP can only be disabled in this way by a password authenticated console application user or from a SAML authenticated command interface. The delete command must be used if the SAML configuration settings are to be changed, as only the `is-enabled` parameter can be modified.

This may restart the web server. Any HTTP/S connections that are active may be disrupted.

Parameters

`[-is-enabled {true|false}]` - SAML Service Provider Enabled

Use this parameter to enable or disable the SAML SP.

Examples

The following example enables SAML SP:

```
cluster1::> security saml-sp modify -is-enabled true
    cluster1::>
```

security saml-sp repair

Repair a failed SAML SP configuation

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

Description

The `security saml-sp repair` command attempts to repair a failed SAML SP configuration on a given node. The status of the individual nodes can be viewed using the security saml-sp status show command.

This restarts the web server. Any active HTTP/S requests to the web server will be disrupted.

Parameters

`-node {<nodename>|local}` - Node (privilege: advanced)

This identifies a single node that matches the input. The repair job will run on this node.

`[-foreground {true|false}]` - Foreground Process (privilege: advanced)

When this parameter is set to *`false`* the command runs in the background as a job. The default is *`true`*, which causes the command to return after the operation completes.

Examples

The following example repairs a failed SAML SP configuration:

```
cluster1:> security saml-sp repair -node node-2
Warning: This restarts the web server. Any active HTTP/S requests to the
web
               server will be disrupted
Do you want to continue? {y|n}: y
      [Job 1321] Job succeeded.
cluster1:>
```

Related Links

- security saml-sp status show

security saml-sp show

Display SAML service provider for authentication

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

Description

The `security saml-sp show` command displays the Security Assertion Markup Language (SAML) Service Provider (SP) configuration.

The `Identity Provider (IdP) URI` indicates the URI of the desired IdP's metadata.

The `Service Provider (SP) host` indicates the IP address containing SAML SP metadata.

The `Certificate Common Name` indicates the SAML SP certificate's common name.

The `Certificate Serial` indicates the SAML SP certificate's serial number.

Examples

The following example displays the SAML SP configuration:

```
cluster1::> security saml-sp show
Identity Provider URI: https://www.my.idp.com
       Service Provider Host: 1.1.1.1
            Certificate Name: mycert
         Certificate Serial: 1234abcd
            Is SAML Enabled: false
```

security saml-sp status show

Display SAML service provider configuration status

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

Description

The `security saml-sp status show` command displays the SAML Service Provider (SP) status for all nodes in the cluster.

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 ]` (privilege: advanced) }

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

`[-node {<nodename>|local}]` - Node (privilege: advanced)

This identifies the node in the cluster.

`[-status {not-configured|config-in-progress|config-failed|config-success}]` - Update Status (privilege: advanced)

This identifies the SAML SP status on the specified node.

`[-error-text <text>]` - Error Text (privilege: advanced)

This identifies the error text associated with the latest saml SP update for this node.

`[-is-enabled {true|false}]` - SAML Service Provider Enabled (privilege: advanced)

When this parameter is set to *`true`* it indicates that the SAML SP is enabled on this node. Similarly, when this parameter is set to *`false`* , it indicates that the SAML SP is not enabled on this node.

Examples

The following example displays the SAML SP status information for all nodes in the cluster.

```
cluster::security saml-sp status> show
Node                            SAML SP Status          Enabled
------------------------------  ----------------------  ----------
cluster-node1                   not-configured          false
cluster-node2                   not-configured          false
2 entries were displayed.

cluster::*>
```

Copyright information

Trademark information