Configure SAML authentication for web services
ONTAP 9
NetApp
November 28, 2022
# Table of Contents

Configure SAML authentication for web services ....................................................... 1
  Configure SAML authentication ................................................................. 1
  Disable SAML authentication .................................................................. 3
  Troubleshoot issues with SAML configuration ...................................... 4
Configure SAML authentication for web services

Configure SAML authentication

Beginning with ONTAP 9.3, you can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

What you'll need

• You must have configured the IdP for SAML authentication.
• You must have the IdP URI.

About this task

• SAML authentication applies only to the http and ontapi applications.

  The http and ontapi applications are used by the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

• SAML authentication is applicable only for accessing the admin SVM.

Steps

1. Create a SAML configuration so that ONTAP can access the IdP metadata:

   `security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name`

   `idp_uri` is the FTP or HTTP address of the IdP host from where the IdP metadata can be downloaded.

   `ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the IP address of the cluster-management LIF is used.

   You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.
cluster_12::> security saml-sp create -idp-uri https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify -metadata-server false

Warning: This restarts the web server. Any HTTP/S connections that are active will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL: https://10.63.56.150/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

The URL to access the ONTAP host metadata is displayed.

2. From the IdP host, configure the IdP with the ONTAP host metadata.

For more information about configuring the IdP, see the IdP documentation.

3. Enable SAML configuration:

   security saml-sp modify -is-enabled true

   Any existing user that accesses the http or ontapi application is automatically configured for SAML authentication.

4. If you want to create users for the http or ontapi application after SAML is configured, specify SAML as the authentication method for the new users.

   a. Create a login method for new users with SAML authentication: +security login create -user -or-group-name user_name -application [http | ontapi] -authentication-method saml -vserver svm_name

      cluster_12::> security login create -user-or-group-name admin1 -application http -authentication-method saml -vserver cluster_12

   b. Verify that the user entry is created:

      security login show
Related information

ONTAP 9 Commands

Disable SAML authentication

You can disable SAML authentication when you want to stop authenticating web users by using an external Identity Provider (IdP). When SAML authentication is disabled, the configured directory service providers such as Active Directory and LDAP are used for authentication.

What you'll need
You must be logged in from the console.

Steps
1. Disable SAML authentication:

   ```bash
   security saml-sp modify -is-enabled false
   ```

2. If you no longer want to use SAML authentication or if you want to modify the IdP, delete the SAML configuration:

   ```bash
   security saml-sp delete
   ```
Troubleshoot issues with SAML configuration

If configuring Security Assertion Markup Language (SAML) authentication fails, you can manually repair each node on which the SAML configuration failed and recover from the failure. During the repair process, the web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

About this task
When you configure SAML authentication, ONTAP applies SAML configuration on a per-node basis. When you enable SAML authentication, ONTAP automatically tries to repair each node if there are configuration issues. If there are issues with SAML configuration on any node, you can disable SAML authentication and then reenable SAML authentication. There can be situations when SAML configuration fails to apply on one or more nodes even after you reenable SAML authentication. You can identify the node on which SAML configuration has failed and then manually repair that node.

Steps
1. Log in to the advanced privilege level:
   ```
   set -privilege advanced
   ```
2. Identify the node on which SAML configuration failed:
   ```
   security saml-sp status show -instance
   ```

   ```
   cluster_12::*> security saml-sp status show -instance
   Node: node1
   Update Status: config-success
   Database Epoch: 9
   Database Transaction Count: 997
   Error Text:
   SAML Service Provider Enabled: false
   ID of SAML Config Job: 179
   
   Node: node2
   Update Status: config-failed
   Database Epoch: 9
   Database Transaction Count: 997
   Failed to receive the SAML IDP Metadata file.
   SAML Service Provider Enabled: false
   ID of SAML Config Job: 180
   2 entries were displayed.
   ```
3. Repair the SAML configuration on the failed node:
   ```
   security saml-sp repair -node node_name
   ```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are active will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.

The web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

4. Verify that SAML is successfully configured on all of the nodes:

   security saml-sp status show -instance

cluster_12::*> security saml-sp status show -instance

       Node: node1
       Update Status: config-success
       Database Epoch: 9
       Database Transaction Count: 997
       Error Text:
       SAML Service Provider Enabled: false
       ID of SAML Config Job: 179

       Node: node2
       Update Status: **config-success**
       Database Epoch: 9
       Database Transaction Count: 997
       Error Text:
       SAML Service Provider Enabled: false
       ID of SAML Config Job: 180
2 entries were displayed.