Set up SAML authentication

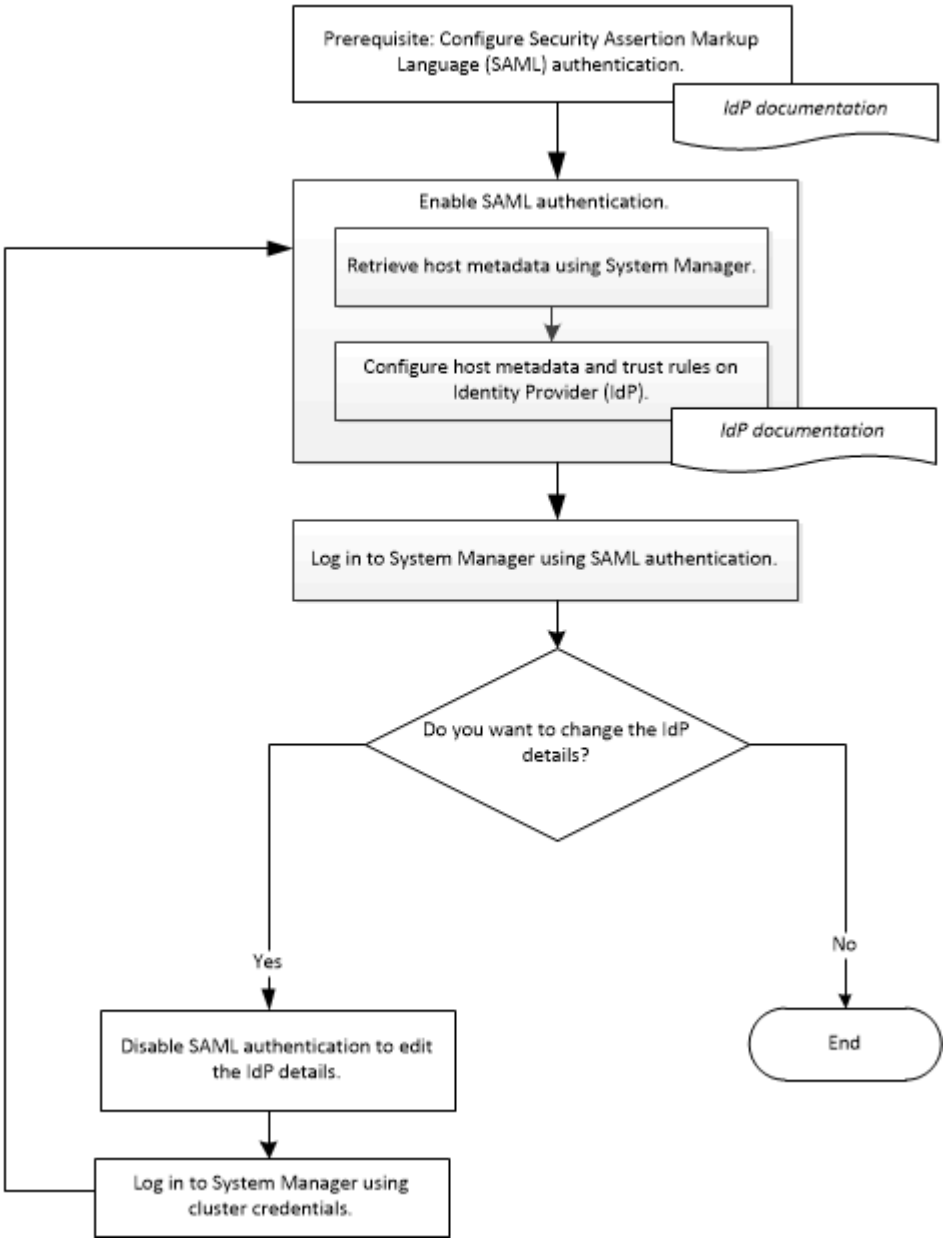
System Manager Classic

NetApp
December 09, 2021

Table of Contents

Setting up SAML authentication

You can set up Security Assertion Markup Language (SAML) authentication so that remote users are authenticated through a secure identity provider (IdP) before they log in to System Manager.



Enabling SAML authentication

You can use System Manager to configure Security Assertion Markup Language (SAML) authentication so that remote users can log in by using a secure identity provider (IdP).

Before you begin

- The IdP that you plan to use for remote authentication must be configured.

See the documentation that is provided by the IdP that you have configured.

- You must have the URI of the IdP.

About this task

The IdPs that have been validated with System Manager are Shibboleth and Active Directory Federation Services.

After SAML authentication is enabled, only remote users can access the System Manager GUI. Local users cannot access the System Manager GUI after SAML authentication is enabled.

Steps

1. Click **Configuration** > **Cluster** > **Authentication**.
2. Select the **Enable SAML authentication** check box.
3. Configure System Manager to use SAML authentication:
   a. Enter the URI of the IdP.
   b. Enter the IP address of the host system.
   c. If required, change the host system certificate.
4. Click **Retrieve Host Metadata** to retrieve the host URI and host metadata information.
5. Copy the host URI or host metadata details, access your IdP, and then specify the host URI or host metadata details and the trust rules in the IdP window.

   See the documentation that is provided by the IdP that you have configured.

6. Click **Save**.

   The IdP login window is displayed.

7. Log in to System Manager by using the IdP login window.

   After the IdP is configured, if the user tries to log in by using the fully qualified domain name (FQDN), IPv6, or a cluster management LIF, then the system automatically changes the IP address to the IP address of the host system that was specified during the IdP configuration.

Related information

Accessing a cluster by using the ONTAP System Manager browser-based graphic interface

Disabling SAML authentication

You can disable Security Assertion Markup Language (SAML) authentication if you want to disable remote access to System Manager, or to edit the SAML configuration.

About this task

Disabling SAML authentication does not delete SAML configuration.

Steps

1. Click **Configuration** > **Cluster** > **Authentication**.
2. Clear the **Enable SAML authentication** check box.
3. Click **Save**.

   System Manager restarts.

4. Log in to System Manager by using the cluster credentials.

Related information

Accessing a cluster by using the ONTAP System Manager browser-based graphic interface