



Gestión de la configuración de autenticación SAML

Active IQ Unified Manager 9.7

NetApp
April 17, 2024

Tabla de contenidos

- Gestión de la configuración de autenticación SAML 1
 - Requisitos del proveedor de identidades 1
 - Habilitación de la autenticación SAML 2
 - Cambiar el proveedor de identidades utilizado para la autenticación SAML 4
 - Actualizar la configuración de autenticación SAML después de cambiar el certificado de seguridad de Unified Manager 4
 - Deshabilitación de la autenticación SAML 6
 - Deshabilitar la autenticación SAML de la consola de mantenimiento 7

Gestión de la configuración de autenticación SAML

Después de configurar la configuración de autenticación remota, puede habilitar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para que los usuarios remotos estén autenticados por un proveedor de identidades (IDP) seguro antes de que puedan acceder a la interfaz de usuario web de Unified Manager.

Tenga en cuenta que solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager después de habilitar la autenticación SAML. Los usuarios locales y los usuarios de mantenimiento no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento.

Requisitos del proveedor de identidades

Al configurar Unified Manager para que utilice un proveedor de identidades (IDP) para realizar la autenticación SAML de todos los usuarios remotos, debe tener en cuenta algunos ajustes de configuración necesarios para que la conexión a Unified Manager se haya realizado correctamente.

Debe introducir el URI y los metadatos de Unified Manager en el servidor IDP. Puede copiar esta información desde la página autenticación de Unified Manager SAML. Unified Manager se considera el proveedor de servicios (SP) en el estándar de lenguaje de marcado de aserción de seguridad (SAML).

Estándares de cifrado compatibles

- Estándar de cifrado avanzado (AES): AES-128 y AES-256
- Secure Hash Algorithm (SHA): SHA-1 y SHA-256

Proveedores de identidades validados

- Shibboleth
- Servicios de Federación de Active Directory (ADFS).

Requisitos de configuración de ADFS

- Debe definir tres reglas de reclamación en el siguiente orden que se requieren para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de parte confiable.

Regla de reclamación	Valor
SAM-account-name	ID del nombre
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Grupos de token — Nombre no cualificado	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Debe establecer el método de autenticación en "autenticación de formularios" o los usuarios pueden recibir un error al cerrar sesión en Unified Manager . Siga estos pasos:
 - a. Abra la Consola de administración de ADFS.
 - b. Haga clic en la carpeta Directivas de autenticación de la vista de árbol izquierda.
 - c. En acciones a la derecha, haga clic en Editar directiva de autenticación primaria global.
 - d. Establezca el método de autenticación de la intranet en "autenticación de formularios" en lugar del valor predeterminado "autenticación de Windows".
- En algunos casos, se rechaza iniciar sesión mediante el IDP cuando el certificado de seguridad de Unified Manager está firmado por CA. Existen dos soluciones alternativas para resolver este problema:
 - Siga las instrucciones identificadas en el vínculo para deshabilitar la comprobación de revocación en el servidor ADFS para la parte de confianza asociada al certificado de CA encadenada:

<http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/>
 - Haga que el servidor de CA resida en el servidor ADFS para firmar la solicitud de certificado del servidor Unified Manager.

Otros requisitos de configuración

- La desviación del reloj de Unified Manager se establece en 5 minutos, por lo que la diferencia de hora entre el servidor IDP y el servidor Unified Manager no puede ser superior a 5 minutos o se producirá un error en la autenticación.

Habilitación de la autenticación SAML

Puede habilitar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para que los usuarios remotos se autenticquen mediante un proveedor de identidad seguro (IDP) antes de poder acceder a la interfaz de usuario web de Unified Manager.

Antes de empezar

- Debe haber configurado la autenticación remota y verificado que la autenticación se ha realizado correctamente.
- Debe haber creado al menos un usuario remoto, o un grupo remoto, con la función Administrador de aplicaciones.
- El proveedor de identidades (IDP) debe ser compatible con Unified Manager y debe configurarse.
- Debe tener la URL y los metadatos de IDP.
- Debe tener acceso al servidor IDP.

Acerca de esta tarea

Después de habilitar la autenticación SAML de Unified Manager, los usuarios no pueden acceder a la interfaz gráfica de usuario hasta que el IDP se haya configurado con la información de host del servidor de Unified Manager. Por lo tanto, debe estar preparado para completar ambas partes de la conexión antes de iniciar el proceso de configuración. El IDP se puede configurar antes o después de configurar Unified Manager.

Solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager después de

habilitar la autenticación SAML. Los usuarios locales y los usuarios de mantenimiento no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento, los comandos de Unified Manager o las ZAPI.



Unified Manager se reinicia automáticamente después de completar la configuración de SAML en esta página.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > autenticación SAML**.
2. Seleccione la casilla de verificación **Habilitar autenticación SAML**.

Se mostrarán los campos necesarios para configurar la conexión IDP.

3. Introduzca el URI de IDP y los metadatos de IDP necesarios para conectar el servidor de Unified Manager al servidor de IDP.

Si se puede acceder al servidor IDP directamente desde el servidor de Unified Manager, puede hacer clic en el botón **Fetch IDP Metadata** después de introducir el URI IDP para rellenar el campo IDP Metadata automáticamente.

4. Copie el URI de metadatos de host de Unified Manager o guarde los metadatos del host en un archivo de texto XML.

Ahora es posible configurar el servidor IDP con esta información.

5. Haga clic en **Guardar**.

Aparece un cuadro de mensaje para confirmar que desea completar la configuración y reiniciar Unified Manager.

6. Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.

Resultados

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la página de inicio de sesión de IDP en lugar de en la página de inicio de sesión de Unified Manager.

Después de terminar

Si no se ha completado todavía, acceda a IDP e introduzca el URI del servidor de Unified Manager y los metadatos para completar la configuración.



Cuando se utiliza ADFS como proveedor de identidades, la interfaz gráfica de usuario de Unified Manager no cumple el tiempo de espera de ADFS y continúa funcionando hasta que se alcanza el tiempo de espera de la sesión de Unified Manager. Cuando Unified Manager se pone en marcha en Windows, Red Hat o CentOS, puede cambiar el tiempo de espera de sesión de la interfaz gráfica de usuario mediante el siguiente comando CLI de Unified Manager: `um option set absolute.session.timeout=00:15:00` Este comando configura el tiempo de espera de sesión de la interfaz gráfica de usuario de Unified Manager en 15 minutos.

Cambiar el proveedor de identidades utilizado para la autenticación SAML

Es posible cambiar el proveedor de identidades (IDP) que Unified Manager utiliza para autenticar usuarios remotos.

Antes de empezar

- Debe tener la URL y los metadatos de IDP.
- Debe tener acceso al IDP.

Acerca de esta tarea

El nuevo IDP se puede configurar antes o después de configurar Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > autenticación SAML**.
2. Introduzca el URI nuevo de IDP y los metadatos de IDP necesarios para conectar el servidor de Unified Manager al IDP.

Si se puede acceder al IDP directamente desde el servidor de Unified Manager, puede hacer clic en el botón **Fetch IDP Metadata** después de introducir la URL del IDP para rellenar el campo IDP Metadata automáticamente.

3. Copie el URI de metadatos de Unified Manager o guarde los metadatos en un archivo de texto XML.
4. Haga clic en **Guardar configuración**.

Aparece un cuadro de mensaje para confirmar que desea cambiar la configuración.

5. Haga clic en **Aceptar**.

Después de terminar

Acceda al nuevo IDP e introduzca el URI del servidor de Unified Manager y los metadatos para completar la configuración.

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la nueva página de inicio de sesión de IDP en lugar de en la página de inicio de sesión de IDP anterior.

Actualizar la configuración de autenticación SAML después de cambiar el certificado de seguridad de Unified Manager

Cualquier cambio en el certificado de seguridad HTTPS instalado en Unified Manager Server requiere actualizar los ajustes de configuración de la autenticación SAML. El certificado se actualiza si cambia el nombre del sistema host, asigna una dirección IP nueva al sistema host o cambia manualmente el certificado de seguridad del sistema.

Acerca de esta tarea

Después de modificar el certificado de seguridad y se reinicia el servidor de Unified Manager, la autenticación SAML no funcionará y los usuarios no podrán acceder a la interfaz gráfica de Unified Manager. Debe actualizar la configuración de autenticación SAML tanto en el servidor IDP como en el servidor de Unified Manager para volver a habilitar el acceso a la interfaz de usuario.

Pasos

1. Inicie sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduzca el número de la opción **Desactivar autenticación SAML**.

Aparece un mensaje para confirmar que desea deshabilitar la autenticación SAML y reiniciar Unified Manager.

3. Inicie la interfaz de usuario de Unified Manager con el FQDN o la dirección IP actualizados, acepte el certificado de servidor actualizado en el explorador e inicie sesión con las credenciales de usuario de mantenimiento.
4. En la página **Configuración/autenticación**, seleccione la ficha **autenticación SAML** y configure la conexión IDP.
5. Copie el URI de metadatos de host de Unified Manager o guarde los metadatos del host en un archivo de texto XML.
6. Haga clic en **Guardar**.

Aparece un cuadro de mensaje para confirmar que desea completar la configuración y reiniciar Unified Manager.

7. Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.
8. Acceda al servidor IDP e introduzca el URI del servidor de Unified Manager y los metadatos para completar la configuración.

Proveedor de identidades	Pasos de configuración
ADFS	<ol style="list-style-type: none">a. Elimine la entrada de confianza de la parte de confianza existente en la GUI de administración de ADFS.b. Agregue una nueva entrada de confianza de parte de confianza mediante el <code>saml_sp_metadata.xml</code> Desde el servidor de Unified Manager actualizado.c. Defina las tres reglas de reclamación necesarias para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de parte fiable.d. Reinicie el servicio de Windows de ADFS.

Proveedor de identidades	Pasos de configuración
Shibboleth	<ol style="list-style-type: none"> Actualice el nuevo FQDN del servidor Unified Manager en el <code>attribute-filter.xml</code> y <code>relying-party.xml</code> archivos. Reinicie el servidor Web Apache Tomcat y espere a que el puerto 8005 se vuelva a conectar.

- Inicie sesión en Unified Manager y verifique que la autenticación SAML funcione como se espera en el IDP.

Deshabilitación de la autenticación SAML

Es posible deshabilitar la autenticación SAML cuando se desea dejar de autenticar usuarios remotos a través de un proveedor de identidad segura (IDP) para poder iniciar sesión en la interfaz de usuario web de Unified Manager. Cuando se deshabilita la autenticación SAML, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión.

Acerca de esta tarea

Después de deshabilitar la autenticación SAML, los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario además de los usuarios remotos configurados.

También puede deshabilitar la autenticación SAML con la consola de mantenimiento de Unified Manager si no tiene acceso a la interfaz gráfica de usuario.



Unified Manager se reinicia automáticamente después de deshabilitar la autenticación de SAML.

Pasos

- En el panel de navegación izquierdo, haga clic en **General > autenticación SAML**.
- Desactive la casilla de verificación **Activar autenticación SAML**.
- Haga clic en **Guardar**.

Aparece un cuadro de mensaje para confirmar que desea completar la configuración y reiniciar Unified Manager.

- Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.

Resultados

La próxima vez que los usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la página de inicio de sesión de Unified Manager en lugar de en la página de inicio de sesión de IDP.

Después de terminar

Acceda a IDP y elimine el URI del servidor de Unified Manager y los metadatos.

Deshabilitar la autenticación SAML de la consola de mantenimiento

Es posible que deba deshabilitar la autenticación SAML desde la consola de mantenimiento cuando no existe acceso a la interfaz gráfica de usuario de Unified Manager. Esto puede suceder en casos de configuración errónea o si no se puede acceder al IDP.

Antes de empezar

Debe tener acceso a la consola de mantenimiento como usuario de mantenimiento.

Acerca de esta tarea

Cuando se deshabilita la autenticación SAML, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión. Los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario además de los usuarios remotos configurados.

También se puede deshabilitar la autenticación SAML desde la página Setup/Authentication en la interfaz de usuario.



Unified Manager se reinicia automáticamente después de deshabilitar la autenticación de SAML.

Pasos

1. Inicie sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduzca el número de la opción **Desactivar autenticación SAML**.

Aparece un mensaje para confirmar que desea deshabilitar la autenticación SAML y reiniciar Unified Manager.

3. Escriba **y** y, a continuación, pulse Intro y se reiniciará Unified Manager.

Resultados

La próxima vez que los usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la página de inicio de sesión de Unified Manager en lugar de en la página de inicio de sesión de IDP.

Después de terminar

Si se requiere, acceda a IDP y elimine la URL del servidor de Unified Manager y los metadatos.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.