Use SAML

SANtricity 11.8

NetApp
April 05, 2024

Tabla de contenidos

Use SAML

Configure SAML

Para configurar la autenticación de Access Management, puede usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) que están integradas en la cabina de almacenamiento. Esta configuración establece una conexión entre un proveedor de identidades y el proveedor de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe conocer la dirección IP o el nombre de dominio de la controladora de la cabina de almacenamiento.
- Un administrador de IDP configuró un sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.
- Un administrador comprobó que el reloj del servidor de IdP y de la controladora está sincronizado (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IdP del sistema de IdP y ese archivo está disponible en el sistema local que se usa para acceder a Unified Manager.

Acerca de esta tarea

Un proveedor de identidades (IDP) es un sistema externo que se usa para solicitar credenciales a un usuario y para determinar si el usuario se autentica correctamente. El IDP se puede configurar para ofrecer autenticación multifactor y para usar cualquier base de datos de usuario, como Active Directory. El equipo de seguridad es responsable de mantener el IDP. Un proveedor de servicios (SP) es un sistema que controla la autenticación y el acceso de usuario. Cuando se configura Access Management con SAML, la cabina de almacenamiento actúa como proveedor de servicios, ya que solicita la autenticación del proveedor de identidades. Para establecer una conexión entre el IDP y la cabina de almacenamiento, se deben compartir archivos de metadatos entre estas dos entidades. A continuación, se deben asignar las entidades de usuario de IDP con los roles de la cabina de almacenamiento. Y, finalmente, se debe probar la conexión y los inicios de sesión SSO antes de habilitar SAML.

> **SAML y Directory Services**. Si SAML se habilita cuando Directory Services está configurado como método de autenticación, SAML sustituye a Directory Services en Unified Manager. Si se deshabilita SAML posteriormente, la configuración de Directory Services se establece en los valores anteriores.

> **Edición y desactivación.** una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

La configuración de la autenticación SAML es un procedimiento de varios pasos.

Paso 1: Cargue el archivo de metadatos de IDP

Para brindar información de conexión de IdP a la cabina de almacenamiento, se deben importar los metadatos de IdP en Unified Manager. El sistema IDP necesita los metadatos para redirigir las solicitudes de

autenticación a la URL correcta y validar las respuestas recibidas.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.

   La página muestra información general de los pasos de configuración.

3. Haga clic en el enlace **Import Identity Provider (IDP) file**.

   Se abre el cuadro de diálogo Importar archivo del proveedor de identidades.

4. Haga clic en **examinar** para seleccionar y cargar el archivo de metadatos IDP que copió en el sistema local.

   Una vez seleccionado el archivo, se muestra el ID de entidad IDP.

5. Haga clic en **Importar**.

Paso 2: Exporte los archivos del proveedor de servicios

Para establecer una relación de confianza entre IDP y la cabina de almacenamiento, se deben importar los metadatos del proveedor de servicios en IDP. IDP necesita estos metadatos para establecer una relación de confianza con la controladora y procesar las solicitudes de autorización. El archivo incluye información, como el nombre de dominio de la controladora o la dirección IP, por lo que IDP se puede comunicar con los proveedores de servicios.

Pasos

1. Haga clic en el enlace **Exportar archivos del proveedor de servicios**.

   Se abre el cuadro de diálogo Exportar archivos del proveedor de servicios.

2. Introduzca la dirección IP del controlador o el nombre DNS en el campo **controladora A** y, a continuación, haga clic en **Exportar** para guardar el archivo de metadatos en el sistema local.

   Después de hacer clic en **Exportar**, los metadatos del proveedor de servicios se descargan en el sistema local. Anote en qué lugar se almacena el archivo.

3. Desde el sistema local, busque el archivo de metadatos del proveedor de servicios con formato XML que exportó.
4. Desde el servidor IdP, importe el archivo de metadatos del proveedor de servicios para establecer la relación de confianza. Es posible importar el archivo directamente o bien introducir manualmente la información de la controladora desde el archivo.

Paso 3: Asignar roles

Para proporcionar autorización y acceso a Unified Manager a los usuarios, se deben asignar los atributos de usuario IdP y las membresías de grupo a los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- Se importó el archivo de metadatos de IdP a Unified Manager.

- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.

Pasos

1. Haga clic en el enlace para **mapping Unified Manager** roles.

   Se abre el cuadro de diálogo asignación de roles.

2. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

   Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=	Funciones

   El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

3. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.

   Es posible modificar las asignaciones de roles después de haber habilitado SAML.

4. Cuando termine de asignar, haga clic en **Guardar**.

Paso 4: Probar el inicio de sesión SSO

Para garantizar la comunicación entre el sistema IDP y la cabina de almacenamiento, de manera opcional, se puede probar un inicio de sesión SSO. Esa prueba también se puede llevar a cabo durante el paso final para

habilitar SAML.

Antes de empezar

- Se importó el archivo de metadatos de IdP a Unified Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.

Pasos

1. Seleccione el enlace **probar inicio de sesión SSO**.

   Se abre un cuadro de diálogo para introducir las credenciales de SSO.

2. Introduzca las credenciales de inicio de sesión para un usuario, tanto con permisos de administración de seguridad como de supervisión.

   Se abre un cuadro de diálogo mientras el sistema prueba el inicio de sesión.

3. Busque el mensaje Test Successful. Si el análisis se realiza correctamente, vaya al siguiente paso para habilitar SAML.

   Si el análisis no se realiza correctamente, se muestra un mensaje de error con más información. Asegúrese de que:

   - El usuario pertenezca a un grupo con permisos de administración de seguridad y supervisión.
   - Los metadatos cargados para el servidor IDP sean correctos.
   - La dirección de la controladora en los archivos de metadatos de SP sea correcta.

Paso 5: Habilite SAML

El paso final es completar la configuración de SAML para la autenticación de usuarios. Durante este proceso, el sistema también le indica que pruebe un inicio de sesión SSO. El proceso de prueba de inicio de sesión con SSO se describe en el paso anterior.

Antes de empezar

- Se importó el archivo de metadatos de IdP a Unified Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.
- Se debe configurar al menos una asignación de rol de administración de seguridad y una de rol de supervisión.

> **Edición y desactivación.** una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

Pasos

1. En la ficha **SAML**, seleccione el enlace **Habilitar SAML**.

   Se abre el cuadro de diálogo Confirmar acción de habilitar SAML.

2. Tipo `enable`Y, a continuación, haga clic en **Activar**.
3. Introduzca las credenciales de usuario para llevar a cabo una prueba de inicio de sesión SSO.

Resultados

Una vez que el sistema habilita SAML, se cierran todas las sesiones activas y se inicia la autenticación de usuarios a través de SAML.

Cambiar las asignaciones de roles SAML

Si anteriormente configuró SAML para Access Management, puede cambiar las asignaciones de roles entre los grupos IDP y los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- SAML debe estar configurado y habilitado.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.
3. Seleccione **asignación de roles**.

   Se abre el cuadro de diálogo asignación de roles.

4. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

   Tenga cuidado de no quitar los permisos mientras SAML está habilitado; de lo contrario, perderá el acceso a Unified Manager.

   Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado.	Funciones

> El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

5. Opcionalmente, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
6. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Exporte los archivos de proveedor de servicios SAML

Si es necesario, se pueden exportar metadatos de proveedor de servicios para la cabina de almacenamiento y volver a importar el archivo en el sistema del proveedor de identidades (IdP).

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- SAML debe estar configurado y habilitado.

Acerca de esta tarea

En esta tarea, se exportan metadatos de la controladora. IDP necesita estos metadatos para establecer una relación de confianza con la controladora y procesar solicitudes de autenticación. El archivo incluye información, como el nombre de dominio o la dirección IP de la controladora, que IDP puede usar para enviar solicitudes.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.
3. Seleccione **Exportar**.

   Se abre el cuadro de diálogo Exportar archivos del proveedor de servicios.

4. Haga clic en **Exportar** para guardar el archivo de metadatos en su sistema local.

   > El campo de nombre de dominio es de sólo lectura.

   Anote en qué lugar se almacena el archivo.

5. Desde el sistema local, busque el archivo de metadatos del proveedor de servicios con formato XML que exportó.
6. Desde el servidor IdP, importe el archivo de metadatos del proveedor de servicios. Es posible importar el archivo directamente o introducir manualmente la información de la controladora.
7. Haga clic en **Cerrar**.