Gestión del acceso

SANtricity 11.5

NetApp
February 12, 2024

Tabla de contenidos

Gestión del acceso

Conceptos

Cómo funciona Access Management

Access Management es un método para establecer la autenticación de usuario en SANtricity System Manager. La autenticación requiere que los usuarios inicien sesión en estos sistemas con sus credenciales asignadas.

La configuración y la autenticación de usuarios de Access Management funciona de la siguiente manera:

1. Un administrador inicia sesión en System Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   > La primera vez que se inicia sesión, el nombre de usuario `admin` se muestra automáticamente y no se puede cambiar. La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. El administrador navega hasta Access Management en la interfaz de usuario. La cabina de almacenamiento está preconfigurada para utilizar roles de usuario local, que son una implementación de capacidades RBAC (control de acceso basado en roles).
3. El administrador configura uno o varios de los siguientes métodos de autenticación:
   - **Roles de usuario local** — la autenticación se gestiona a través de capacidades RBAC aplicadas en la cabina de almacenamiento. Los roles de usuario local incluyen perfiles de usuario predefinidos con permisos de acceso específicos. Los administradores pueden usar estos roles de usuario local como el único método de autenticación o usarlos en combinación con un servicio de directorio. No hace falta configurar nada más allá de las contraseñas de los usuarios.
   - **Servicios de directorio** — la autenticación se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft. Un administrador se conecta con el servidor LDAP y luego asigna los usuarios LDAP a los roles de usuario local integrados en la cabina de almacenamiento.
   - **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) utilizando el lenguaje de marcado de aserción de seguridad (SAML) 2.0. Un administrador establece comunicación entre el sistema IDP y la cabina de almacenamiento, y luego asigna los usuarios IDP a los roles de usuario local integrados en la cabina de almacenamiento.
4. El administrador ofrece credenciales de inicio de sesión en System Manager para los usuarios.
5. Los usuarios inician sesión en el sistema con sus credenciales.

   > Si la autenticación se gestiona con SAML y un SSO (inicio de sesión único), el sistema puede omitir el diálogo de inicio de sesión de System Manager.

   Durante el inicio de sesión, el sistema realiza las siguientes tareas en segundo plano:

   - Autentica el nombre de usuario y la contraseña en relación con la cuenta de usuario.
   - Determina los permisos del usuario según los roles asignados.
   - Ofrece acceso al usuario a las tareas en la interfaz de usuario.

- Muestra el nombre de usuario en la esquina superior derecha de la interfaz.

Tareas disponibles en System Manager

El acceso a las tareas depende de los roles asignados a un usuario, entre los cuales se encuentran los siguientes:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Una tarea no disponible está atenuada o no aparece en la interfaz de usuario. Por ejemplo, un usuario con el rol de supervisión puede ver toda la información sobre los volúmenes, pero no puede acceder a funciones para modificarlos. Las pestañas para funciones como **Servicios de copia** y **Agregar a carga de trabajo** estarán atenuadas; sólo Ver/Editar configuración está disponible.

Acceso de usuarios a SANtricity Storage Manager

Cuando se configuran los roles de usuario local y los servicios de directorio, los usuarios deben introducir credenciales antes de realizar cualquiera de las siguientes funciones en Enterprise Management Window (EMW):

- Cambiar el nombre de la cabina de almacenamiento
- Actualizar el firmware de la controladora
- Cargar una configuración de la cabina de almacenamiento
- Ejecutar un script
- Intentar realizar una operación activa cuando se agotó el tiempo de espera de una sesión no utilizada

Si SAML está configurado para una cabina de almacenamiento, los usuarios no pueden usar EMW para detectar o gestionar almacenamiento para esa cabina.

Terminología de Access Management

Conozca la forma en que los términos de Access Management se aplican a su cabina de almacenamiento.

Duración	Descripción
Active Directory	Active Directory (AD) es un servicio de directorio de Microsoft en el que se utiliza LDAP para redes de dominio de Windows.

Duración	Descripción
Vinculación	Las operaciones de vinculación se usan para autenticar clientes en el servidor de directorio. Por lo general, la vinculación requiere credenciales de cuenta y contraseña, pero algunos servidores aceptan operaciones de vinculación anónimas.
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
IDP	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.
LDAP	El protocolo ligero de acceso a directorios (LDAP) es un protocolo de aplicación para acceder a servicios distribuidos de información de directorio y mantenerlos. Este protocolo permite que varias aplicaciones y servicios se conecten con el servidor LDAP para validar usuarios.
RBAC	El control de acceso basado en funciones (RBAC) es un método para regular el acceso a los recursos informáticos o de red en función de las funciones de los usuarios individuales. Los controles de RBAC se aplican en la cabina de almacenamiento y se componen de roles predefinidos.

Duración	Descripción
SAML	El lenguaje de marcado de aserción de seguridad (SAML) es un estándar basado en XML para fines de autenticación y autorización entre dos entidades. SAML permite utilizar la autenticación multifactor, en la cual los usuarios deben introducir dos o más elementos para validar su identidad (por ejemplo, una contraseña y una huella digital). La función de SAML integrada de la cabina de almacenamiento es compatible con SAML2.0 para autenticación, autorización y confirmación de identidades.
SP	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.
SSO	El inicio de sesión único (SSO) es un servicio de autenticación que permite el uso de un conjunto de credenciales de inicio de sesión para acceder a varias aplicaciones.

Permisos para roles asignados

Las capacidades de RBAC (control de acceso basado en roles) presentes en la cabina de almacenamiento incluyen perfiles de usuario predefinidos con uno o varios roles asignados. Cada rol incluye permisos para acceder a tareas en SANtricity System Manager.

Puede accederse a los perfiles de usuario y a los roles asignados desde el menú:Configuración[Access Management > roles de usuario local] desde la interfaz de usuario de cualquier System Manager.

Los roles permiten que los usuarios accedan a tareas de la siguiente manera:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Si un usuario no tiene permisos para determinada tarea, la tarea aparece atenuada o directamente no aparece en la interfaz de usuario.

Access Management con roles de usuario local

Para Access Management, los administradores pueden usar las capacidades RBAC (control de acceso basado en roles) aplicadas en la cabina de almacenamiento. Estas capacidades se denominan "roles de usuario local".

Flujo de trabajo de configuración

Los roles de usuario local están preconfigurados para la cabina de almacenamiento. Para usar roles de usuario local con fines de autenticación, los administradores pueden hacer lo siguiente:

1. Un administrador inicia sesión en SANtricity System Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. Un administrador revisa los perfiles de usuario, que están predefinidos y no pueden modificarse.
3. De manera opcional, el administrador asigna nuevas contraseñas para cada perfil de usuario.
4. Los usuarios inician sesión en el sistema con las credenciales asignadas.

Gestión

Al utilizar solamente los roles de usuario local para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Cambiar contraseñas.
- Configurar la longitud mínima de las contraseñas.
- Permitir que los usuarios inicien sesión sin contraseñas.

Access Management con servicios de directorio

Para Access Management, los administradores puede usar un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorios, como Active Directory de Microsoft.

Flujo de trabajo de configuración

Si se utilizan un servidor LDAP y un servicio de directorio en la red, la configuración opera de la siguiente manera:

1. Un administrador inicia sesión en SANtricity System Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. El administrador introduce los ajustes de configuración del servidor LDAP. Entre ellas se encuentran el nombre de dominio, la URL y la información de la cuenta vinculada.
3. Si el servidor LDAP utiliza un protocolo seguro (LDAPS), el administrador carga una cadena de certificados de Certificate Authority (CA) para la autenticación entre el servidor LDAP y la cabina de

almacenamiento.

4. Después de establecer la conexión del servidor, el administrador asigna los grupos de usuarios a los roles de la cabina de almacenamiento. Estos roles están predefinidos y no pueden modificarse.
5. El administrador prueba la conexión entre el servidor LDAP y la cabina de almacenamiento.
6. Los usuarios inician sesión en el sistema con las credenciales de LDAP/servicios de directorio asignadas.

Gestión

Al utilizar los servicios de directorio para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Añadir servidor de directorio.
- Editar la configuración del servidor de directorio.
- Asignar usuarios LDAP a roles de usuario local.
- Quitar un servidor de directorio.

Access Management con SAML

Para Access Management, los administradores pueden usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) 2.0 que están integradas en la cabina.

Flujo de trabajo de configuración

La configuración de SAML funciona de la siguiente manera:

1. Un administrador inicia sesión en System Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   La `admin` El usuario tiene acceso completo a todas las funciones en System Manager.

2. El administrador se dirige a la ficha **SAML** de Access Management.
3. Un administrador configura las comunicaciones con el proveedor de identidades (IDP). Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. Para configurar las comunicaciones con la cabina de almacenamiento, el administrador descarga el archivo de metadatos de IDP desde el sistema IDP y luego usa System Manager para cargarlo a la cabina de almacenamiento.
4. Un administrador establece una relación de confianza entre el proveedor de servicios y el IDP. Un proveedor de servicios controla la autorización de usuarios; en este caso, la controladora en la cabina de almacenamiento actúa como proveedor de servicios. Para configurar las comunicaciones, el administrador usa System Manager para exportar el archivo de metadatos del proveedor de servicios en cada controladora. Desde el sistema IDP, el administrador importa estos archivos de metadatos al IDP.

   Los administradores también deben asegurarse de que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.

5. El administrador asigna los roles de la cabina de almacenamiento a los atributos de usuario definidos en el IDP. Para hacerlo, el administrador usa System Manager y crea las asignaciones.

6. El administrador prueba el inicio de sesión de SSO en la URL del IDP. Esta prueba garantiza que la cabina de almacenamiento y el IDP puedan comunicarse.

> Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

7. En System Manager, el administrador del sistema habilita SAML para la cabina de almacenamiento.
8. Los usuarios inician sesión en el sistema con sus credenciales de SSO.

Gestión

Cuando se usa SAML con fines de autenticación, los administradores pueden realizar las siguientes tareas de administración:

- Modifique o cree nuevas asignaciones de roles
- Exporte los archivos del proveedor de servicios

Restricciones de acceso

Cuando se habilita SAML, los siguientes clientes no pueden acceder a los recursos y los servicios de la cabina de almacenamiento:

- Enterprise Management Window (EMW)
- Interfaz de línea de comandos (CLI)
- Clientes de kits de desarrollo de software (SDK)
- Clientes en banda
- Clientes HTTP de la API de REST de autenticación básica
- Inicio de sesión mediante extremo estándar de la API de REST

Procedimientos

Ver los roles de usuario local

Desde la pestaña roles de usuario local, es posible ver las asignaciones de los perfiles de usuario a los roles predeterminados. Estas asignaciones forman parte de los controles de acceso basados en roles (RBAC) aplicados en 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.

Acerca de esta tarea

Los perfiles de usuario y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse.

Pasos

1. Seleccione MENU:Settings[Access Management].

2. Seleccione la ficha **roles de usuario local**.

   Los perfiles de usuario se muestran en la tabla:

   - **Administrador raíz** (admin) — Super administrador que tiene acceso a todas las funciones del sistema. Este perfil de usuario incluye todos los roles.
   - **Administrador de almacenamiento** (almacenamiento) — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este perfil de usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión.
   - **Administración de seguridad** (seguridad): El usuario responsable de la configuración de seguridad, incluidas la administración de acceso, la administración de certificados y las funciones de unidad con seguridad habilitada. Este perfil de usuario incluye los siguientes roles: Administrador de seguridad y Supervisión.
   - **Support admin** (asistencia técnica) — el usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este perfil de usuario incluye los siguientes roles: Support Admin y Supervisión.
   - **Monitor** (monitor) — un usuario con acceso de sólo lectura al sistema. Este perfil de usuario incluye únicamente el rol Supervisión.

Cambiar contraseñas

Es posible cambiar las contraseñas de usuario de cada perfil de usuario desde Access Management.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.
- Debe conocer la contraseña de administrador local.

Acerca de esta tarea

Tenga en cuenta estas directrices al elegir una contraseña:

- Todas las contraseñas de usuarios locales nuevas deben alcanzar o superar la configuración de longitud mínima actual de la contraseña (en Ver/editar configuración).
- Las contraseñas distinguen mayúsculas de minúsculas.
- Los espacios al final de la contraseña no se eliminan, si se los utiliza. Procure incluir espacios si se incluyeron en la contraseña.
- Para mayor seguridad, use al menos 15 caracteres alfanuméricos y cambie la contraseña con frecuencia.

> Cuando se cambia la contraseña en System Manager también se modifica en la interfaz de línea de comandos (CLI). Además, los cambios de contraseña provocan el cierre de la sesión activa del usuario.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione un usuario de la tabla.

   El botón **Cambiar contraseña** estará disponible.

4. Seleccione **Cambiar contraseña**.

   Se abre el cuadro de diálogo **Cambiar contraseña**.

5. Si no se estableció una longitud de contraseña mínima para las contraseñas de usuario local, se puede marcar la casilla para solicitar que el usuario seleccionado introduzca una contraseña para acceder a la cabina de almacenamiento y, a continuación, se puede escribir la contraseña nueva para el usuario seleccionado.
6. Introduzca su contraseña de administrador local y, a continuación, haga clic en **Cambiar**.

Resultado

Si el usuario está conectado, el cambio de contraseña provocará el cierre de la sesión activa del usuario.

Cambie la configuración de contraseña de usuario local

Es posible configurar la longitud mínima requerida para todas las contraseñas de usuario locales nuevas o actualizadas de la cabina de almacenamiento. También es posible permitir a los usuarios locales acceder a la cabina de almacenamiento sin introducir una contraseña.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.

Acerca de esta tarea

Recuerde estas directrices cuando configure la longitud mínima para las contraseñas de usuario local:

- Los cambios en la configuración no afectan a las contraseñas existentes de usuarios locales.
- La configuración de la longitud mínima requerida para las contraseñas de usuario local debe tener entre 0 y 30 caracteres.
- Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración de longitud mínima actual.
- No configure una longitud mínima para la contraseña si no desea que usuarios locales accedan a la cabina de almacenamiento sin introducir una contraseña.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione el botón **Ver/editar configuración**.

   Se abre el cuadro de diálogo **Configuración de contraseña de usuario local**.

4. Debe realizar una de las siguientes acciones:
   - Para permitir a los usuarios locales acceder a la cabina de almacenamiento *sin* introducir una contraseña, desactive la casilla de comprobación "require all local user passwords to be at least".
   - Para configurar una longitud mínima de contraseña para todas las contraseñas de usuarios locales, active la casilla de comprobación "require all local user passwords to be at least" y luego use el cuadro de desplazamiento para configurar la longitud mínima requerida para todas las contraseñas de usuarios locales.

Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración actual.

5. Haga clic en **Guardar**.

Añadir servidor de directorio

Para configurar la autenticación de Access Management, se pueden establecer comunicaciones entre la cabina de almacenamiento y un servidor LDAP, y luego asignar los grupos de usuarios LDAP a los roles predefinidos de la cabina.

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 haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

Acerca de esta tarea

La adición de un servidor de directorio es un proceso que consta de dos pasos. Primero, se debe introducir la URL y el nombre de dominio. Si el servidor utiliza un protocolo seguro, se debe cargar además un certificado de CA para autenticación, si no está firmado por una entidad de firma estándar. Si se poseen credenciales de una cuenta de enlace, también es posible introducir el nombre de cuenta de usuario y la contraseña. Luego, se deben asignar los grupos de usuarios del servidor LDAP a los roles predefinidos de la cabina de almacenamiento.

> Durante el procedimiento para añadir un servidor LDAP, se deshabilitará la interfaz de gestión heredada. La interfaz de gestión heredada (Symbol) es un método de comunicación entre la cabina de almacenamiento y el cliente de gestión. Cuando se encuentra deshabilitada, la cabina de almacenamiento y el cliente de gestión utilizan un método de comunicación más seguro (API DE REST por https).

Pasos

1. Seleccione MENU:Settings[Access Management].
2. En la ficha **Servicios de directorio**, seleccione **Agregar servidor de directorio**.

   Se abre el cuadro de diálogo **Agregar servidor de directorio**.

3. En la ficha **Configuración del servidor**, introduzca las credenciales del servidor LDAP.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Introduzca el nombre de dominio del servidor LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (*username@domain*) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
Introduzca la URL para acceder al servidor LDAP con el formato de `ldap[s]://host:port`.	Cargar certificado (opcional)
Este campo aparece solo si se especifica un protocolo LDAPS en el campo URL del servidor arriba. Haga clic en **examinar** y seleccione un certificado de CA para cargar. Este es el certificado o la cadena de certificados de confianza utilizado para autenticar el servidor LDAP.	Enlazar cuenta (opcional)
Introduzca una cuenta de usuario de solo lectura para realizar consultas de búsqueda en el servidor LDAP y para buscar dentro de los grupos. Introduzca el nombre de cuenta con formato tipo LDAP. Por ejemplo, si el usuario de enlace se denomina "bindacct", puede introducir un valor como el siguiente: "CN=bindacct,CN=Users,DC=cpoc,DC=local".	Enlazar contraseña (opcional)
Este campo aparece cuando introduce una cuenta de enlace arriba. Introduzca la contraseña de la cuenta de enlace.	Probar conexión del servidor antes de añadir

Ajuste	Descripción
Seleccione esta casilla de comprobación si desea asegurarse de que la cabina de almacenamiento pueda comunicarse con la configuración de servidor LDAP que introdujo. La prueba se produce después de hacer clic en **Agregar** en la parte inferior del cuadro de diálogo. Si esta casilla de comprobación está seleccionada y la prueba falla, no se añadirá la configuración. Debe resolver el error o anular la selección de la casilla de comprobación para omitir la comprobación y añadir la configuración.	**Ajustes de privilegios**
DN base de búsqueda	Introduzca el contexto de LDAP para buscar usuarios, generalmente con el formato de `CN=Users, DC=copc, DC=local`.
Atributo de nombre de usuario	Introduzca el atributo vinculado al ID de usuario para los fines de autenticación. Por ejemplo: `sAMAccountName`.
Atributos de grupo	Introduzca una lista de atributos de grupo en el usuario, que se utilizará para la asignación de grupos a roles. Por ejemplo: `memberOf, managedObjects`.

4. Haga clic en la ficha **asignación de roles**.
5. Asigne grupos LDAP a los roles predefinidos. Un grupo puede tener varios roles asignados.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
Especifique el nombre distintivo (DN) del grupo correspondiente al grupo de usuarios LDAP que se asignará.	Funciones

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

6. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
7. Cuando termine de asignar, haga clic en **Agregar**.

El sistema realiza una validación y se asegura de que la cabina de almacenamiento y el servidor LDAP pueden comunicarse. Si aparece un mensaje de error, compruebe las credenciales que introdujo en el cuadro de diálogo y vuelva a introducir la información, de ser necesario.

Editar ajustes y asignaciones de roles del servidor de directorios

Si anteriormente configuró un servidor de directorio en Access Management, es posible cambiar sus ajustes en cualquier momento. Entre estos ajustes se encuentran la información de conexión del servidor y las asignaciones de grupos a roles.

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 definirse un servidor de directorio.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Servicios de directorio**.
3. Si se define más de un servidor, seleccione el servidor que desea editar en la tabla.
4. Seleccione **Ver/editar configuración**.

   Se abre el cuadro de diálogo **Configuración del servidor de directorio**.

5. En la ficha **Configuración del servidor**, cambie la configuración deseada.

Ajuste	Descripción
Ajustes de configuración	Dominios
Los nombres de dominio de los servidores LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (*username@domain*) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
La URL para acceder al servidor LDAP con el formato de `ldap[s]://host:port`.	Enlazar cuenta (opcional)
La cuenta de usuario de solo lectura para realizar consultas en el servidor LDAP y buscar dentro de grupo.	Enlazar contraseña (opcional)
La contraseña de la cuenta vinculada. (Este campo se muestra cuando se introduce una cuenta vinculada.)	Probar conexión del servidor antes de guardar

Ajuste	Descripción
Comprueba que la cabina de almacenamiento pueda comunicarse con la configuración del servidor LDAP. La prueba se produce después de hacer clic en Guardar, en la parte inferior del cuadro de diálogo. Si se selecciona esta casilla de comprobación y la prueba falla, no se modifica la configuración. Debe resolver el error o cancelar la selección de la casilla de comprobación para omitir la prueba y volver a editar la configuración.	**Configuración de privilegios**
DN base de búsqueda	El contexto de LDAP para buscar usuarios, normalmente en la forma de `CN=Users, DC=copc, DC=local`.
Atributo de nombre de usuario	El atributo que está vinculado al ID de usuario para la autenticación. Por ejemplo: `sAMAccountName`.
Atributos de grupo	Lista de atributos de grupo en el usuario, que se utiliza para la asignación de grupos a roles. Por ejemplo: `memberOf, managedObjects`.

6. En la ficha **asignación de roles**, cambie la asignación deseada.

Ajuste	Descripción
Asignaciones	DN de grupo
El nombre de dominio para asignar el grupo de usuarios LDAP.	Funciones

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

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

Resultado

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

Quitar un servidor de directorio

Para interrumpir la conexión entre un servidor de directorio y la cabina de almacenamiento, es posible eliminar la información del servidor de la página Access Management. Se recomienda ejecutar esta tarea si se configuró un servidor nuevo y se

desea eliminar el anterior.

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.

Acerca de esta tarea

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

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Servicios de directorio**.
3. Seleccione el servidor de directorio que desea eliminar de la lista.
4. Haga clic en **Quitar**.

   Se abrirá el cuadro de diálogo **Quitar servidor de directorio**.

5. Tipo `remove` En el campo y, a continuación, haga clic en **Quitar**.

   Se eliminará la configuración del servidor de directorio, la configuración de privilegios y las asignaciones de roles. Los usuarios ya no podrán iniciar sesión con las credenciales de este servidor.

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.

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 System 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
- Paso 2: Exporte los archivos del proveedor de servicios
- Paso 3: Asignar roles
- Paso 4: Probar el inicio de sesión SSO
- Paso 5: Habilite SAML

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 System Manager.

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 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 los relojes del servidor de IDP y de la controladora están sincronizados (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 System Manager.

Acerca de esta tarea

En esta tarea, se carga un archivo de metadatos desde IDP en System Manager. El sistema IDP necesita los metadatos para redirigir las solicitudes de autenticación a la URL correcta y validar las respuestas recibidas. Solamente es necesario cargar un solo archivo de metadatos para la cabina de almacenamiento, incluso si hay dos controladoras.

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.

Antes de empezar

- Conoce la dirección IP o el nombre de dominio de cada controladora de la cabina de almacenamiento.

Acerca de esta tarea

En esta tarea, es posible exportar metadatos de las controladoras (un archivo para cada controladora). IDP necesita estos metadatos para establecer una relación de confianza con las controladoras 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. Si la matriz de almacenamiento incluye dos controladoras, repita este paso con la segunda controladora en el campo **controladora B**.

   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 los archivos de metadatos del proveedor de servicios que exportó.

   Hay un archivo con formato XML por controladora.

4. Desde el servidor IDP, importe los archivos de metadatos del proveedor de servicios para establecer la relación de confianza. Es posible importar los archivos directamente o bien introducir manualmente la información de la controladora desde los archivos.

Paso 3: Asignar roles

Para proporcionar autorización y acceso a System 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 System Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para cada controladora en el sistema IDP.

Acerca de esta tarea

En esta tarea, se deberá usar System Manager para asignar los grupos de IDP a los roles de los usuarios locales.

Pasos

1. Haga clic en el enlace para asignar los roles de System Manager.

   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.	Funciones

   El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System 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 System Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para cada controladora en el sistema IDP.

Pasos

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

   Se abre un 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.
   - Las direcciones de las controladoras en los archivos de metadatos de SP sean correctas.

Paso 5: Habilite SAML

El paso final es habilitar la autenticación de usuario SAML.

Antes de empezar

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

Acerca de esta tarea

En esta tarea, se describe cómo 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.

> **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 activación de 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.

Resultado

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 System 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. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

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

Resultado

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 los archivos 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, es posible exportar metadatos de las controladoras (un archivo para cada controladora). IDP necesita estos metadatos para establecer una relación de confianza con las controladoras 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. Para cada controlador, haga clic en **Exportar** para guardar el archivo de metadatos en el sistema local.

   Los campos de nombre de dominio para cada controladora son de solo lectura.

   Anote en qué lugar se almacena el archivo.

5. Desde el sistema local, busque los archivos de metadatos del proveedor de servicios que exportó.

   Hay un archivo con formato XML por controladora.

6. Desde el servidor IDP, importe los archivos de metadatos del proveedor de servicios. Puede importar los archivos directamente o introducir manualmente la información de la controladora incluida en ellos.
7. Haga clic en **Cerrar**.

Ver actividad de registro de auditoría

Al ver los registros de auditoría, los usuarios que tienen permisos de administrador de seguridad pueden supervisar acciones de usuarios, fallos de autenticación, intentos de inicio de sesión no válidos y la vida útil de la sesión de usuario.

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.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.

   La actividad del registro de auditoría aparece en formato tabular, que incluye las siguientes columnas de información:

   - **Fecha/Hora** — Marca de hora del momento en que la matriz de almacenamiento detectó el evento (en

GMT).

- **Nombre de usuario** — el nombre de usuario asociado al evento. Para cualquier acción sin autenticar en la cabina de almacenamiento, aparece "N/A" como nombre de usuario. El proxy interno o algún otro mecanismo podrían activar acciones sin autenticar.
- **Código de estado** — Código de estado HTTP de la operación (200, 400, etc.) y texto descriptivo asociado al evento.
- **URL visitada** — URL completa (incluido el host) y cadena de consulta.
- **Dirección IP del cliente** — Dirección IP del cliente asociado al evento.
- **Source** — origen de registro asociado al evento, que puede ser System Manager, CLI, Web Services o Support Shell.

3. Use las selecciones de la página Registro de auditoría para ver y gestionar eventos.

Detalles de selección

Selección	Descripción
Mostrar eventos de…	Eventos de límite mostrados por rango de fechas (últimas 24 horas, últimos 7 días, últimos 30 días o un rango de fechas personalizado).
Filtro	Eventos de límite mostrados por los caracteres introducidos en el campo. Utilice comillas ("") para una coincidencia exacta de palabras, introduzca `OR` para devolver una o más palabras, o introduzca un guión (--) para omitir palabras.
Actualice	Seleccione **Actualizar** para actualizar la página a los eventos más recientes.
Ver/editar configuración	Seleccione **Ver/editar configuración** para abrir un cuadro de diálogo que permite especificar una política de registro completo y el nivel de acciones que se registrarán.
Eliminar eventos	Seleccione **Eliminar** para abrir un cuadro de diálogo que le permite eliminar eventos antiguos de la página.
Mostrar/ocultar columnas	Haga clic en el icono de la columna **Mostrar/Ocultar** para seleccionar columnas adicionales para mostrar en la tabla. Las columnas adicionales incluyen: • **Método** — el método HTTP (POR ejemplo, POST, GET, DELETE, etc.). • **Comando CLI ejecutado** — el comando CLI (gramática) ejecutado para solicitudes Secure CLI. • **Estado de devolución de CLI** — un código de estado de CLI o una solicitud de archivos de entrada del cliente. • **Procedimiento de Symbol** — procedimiento de Symbol ejecutado. • **Tipo de evento SSH** — Tipo de eventos Secure Shell (SSH), como inicio de sesión, cierre de sesión y login_fail. • **PID de sesión SSH** — número de ID de proceso de la sesión SSH. • **Duración(s) de sesión de SSH** — el número de segundos en los que el usuario estuvo conectado.
Alternar filtros de columnas	Haga clic en el icono **alternar** para abrir los campos de filtrado de cada columna. Introduzca los caracteres en un campo de columna para limitar los eventos que se muestran con esos caracteres. Vuelva a hacer clic en el icono para cerrar los campos de filtrado.
Deshacer cambios	Haga clic en el icono **Deshacer** para devolver la tabla a la configuración predeterminada.

Selección	Descripción
Exportar	Haga clic en **Exportar** para guardar los datos de la tabla en un archivo de valores separados por comas (CSV).

Defina políticas de registro de auditoría

Es posible cambiar la política de sobrescritura y los tipos de eventos registrados en el registro de auditoría.

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.

Acerca de esta tarea

En esta tarea, se describe la forma de cambiar la configuración del registro de auditoría, lo que incluye la política para sobrescribir eventos anteriores y la política para registrar tipos de eventos.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.
3. Seleccione **Ver/editar configuración**.

   Se abrirá el cuadro de diálogo **Configuración del registro de auditoría**.

4. Cambie la política de sobrescritura o los tipos de eventos registrados.

Detalles del campo

Ajuste	Descripción
Política de sobrescritura	Determine la política para sobrescribir eventos antiguos cuando se alcanza la capacidad máxima: • **Permitir que los eventos más antiguos del registro de auditoría se sobrescriban cuando el registro de auditoría está lleno** — sobrescribe los eventos antiguos cuando el registro de auditoría llega a 50,000 registros. • **Requerir que se eliminen manualmente los eventos del registro de auditoría** — especifica que los eventos no se eliminarán automáticamente; en su lugar, aparecerá una advertencia de umbral en el porcentaje establecido. Los eventos deben eliminarse manualmente. Si se deshabilita la política de sobrescritura y las entradas del registro de auditoría llegan al límite máximo, se deniega el acceso a System Manager para usuarios sin permisos de Administrador de seguridad. Para restaurar el acceso al sistema para usuarios sin permisos de Administrador de seguridad, un usuario asignado al rol Security Admin debe eliminar los registros de eventos anteriores. Las políticas de sobrescritura no se aplican si un servidor de syslog está configurado para archivar registros de auditoría.

Ajuste	Descripción
Nivel de acciones que se registrarán	Determina los tipos de eventos que deben registrarse: • **Grabar sólo eventos de modificación** — muestra sólo los eventos en los que una acción del usuario implica realizar un cambio en el sistema. • **Grabar todos los eventos de modificación y sólo lectura** — muestra todos los eventos, incluyendo una acción del usuario que implica leer o descargar información.

5. Haga clic en **Guardar**.

Elimine eventos del registro de auditoría

Es posible borrar los eventos antiguos del registro de auditoría para que la búsqueda de eventos sea más sencilla. Tiene la opción de guardar los eventos antiguos en un archivo CSV (valores separados por comas) después de su eliminación.

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.

Acerca de esta tarea

En esta tarea, se describe la forma de eliminar eventos antiguos del registro de auditoría.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.
3. Seleccione **Eliminar**.

   Se abre el cuadro de diálogo **Eliminar registro de auditoría**.

4. Seleccione o escriba el número de eventos antiguos que desea eliminar.
5. Si desea exportar los eventos eliminados a un archivo CSV (recomendado), mantenga seleccionada la casilla de comprobación. Se le pedirá que introduzca un nombre de archivo y una ubicación al hacer clic en **Eliminar** en el paso siguiente. De lo contrario, si no desea guardar eventos en un archivo CSV, haga clic en la casilla de comprobación para cancelar la selección.
6. Haga clic en **Eliminar**.

   Se abre un cuadro de diálogo de confirmación.

7. Tipo `delete` En el campo y, a continuación, haga clic en **Eliminar**.

   Los eventos más antiguos se eliminarán de la página Registro de auditoría.

Configurar servidores de syslog para registros de auditoría

Si desea archivar registros de auditoría en un servidor de syslog externo, puede configurar las comunicaciones entre ese servidor y la cabina de almacenamiento. Una vez que se establece la conexión, los registros de auditoría se guardan automáticamente en el servidor de syslog.

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.
- La dirección, el protocolo y el número de puerto del servidor de syslog deben estar disponibles. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si el servidor usa un protocolo seguro (por ejemplo, TLS), debe haber disponible un certificado de entidad de certificación (CA) en el sistema local. Los certificados DE CA identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. En la ficha **Registro de auditoría**, seleccione **Configurar servidores de syslog**.

   Se abre el cuadro de diálogo **Configurar servidores de syslog**.

3. Haga clic en **Agregar**.

   Se abrirá el cuadro de diálogo **Agregar servidor de syslog**.

4. Introduzca la información del servidor y, a continuación, haga clic en **Agregar**.
   - Dirección del servidor — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
   - Protocol — Seleccione un protocolo en la lista desplegable (por ejemplo, TLS, UDP o TCP).
   - Cargar certificado (opcional): Si seleccionó el protocolo TLS y todavía no cargó un certificado de CA firmado, haga clic en examinar para cargar el archivo de certificado. Los registros de auditoría no se archivan en un servidor de syslog si no cuentan con un certificado de confianza.

     Si la certificación ya no es válida en el futuro, el apretón de manos de TSL fallará. Como resultado, se publica un mensaje de error en el registro de auditoría y ya no se envían mensajes al servidor de syslog. Para resolver este problema, debe corregir la certificación en el servidor de syslog y, a continuación, ir a menú:Configuración[Registro de auditoría > Configurar servidores de syslog > probar todo].

   - Puerto — Introduzca el número de puerto para el receptor de syslog. Después de hacer clic en **Agregar**, se abre el cuadro de diálogo **Configurar servidores de syslog** y se muestra el servidor de syslog configurado en la página.
5. Para probar la conexión del servidor con la matriz de almacenamiento, seleccione **probar todo**.

Resultado

Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.

Editar la configuración del servidor de syslog para los registros de auditoría

Es posible modificar la configuración del servidor de syslog utilizada para archivar registros de auditoría, y también cargar un nuevo certificado de una entidad de certificación (CA) para el servidor.

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.
- La dirección, el protocolo y el número de puerto del servidor de syslog deben estar disponibles. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si va a cargar un nuevo certificado de CA, el certificado debe estar disponible en el sistema local.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. En la ficha **Registro de auditoría**, seleccione **Configurar servidores de syslog**.

   Los servidores de syslog configurados se muestran en la página.

3. Para editar la información del servidor, seleccione el icono **Editar** (lápiz) situado a la derecha del nombre del servidor y, a continuación, realice los cambios deseados en los siguientes campos:
   - Dirección del servidor — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
   - Protocol — Seleccione un protocolo en la lista desplegable (por ejemplo, TLS, UDP o TCP).
   - Puerto — Introduzca el número de puerto para el receptor de syslog.
4. Si cambió el protocolo al protocolo TLS seguro (desde UDP o TCP), haga clic en **Importar certificado de confianza** para cargar un certificado de CA.
5. Para probar la nueva conexión con la matriz de almacenamiento, seleccione **probar todo**.

Resultado

Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.

Preguntas frecuentes

¿Por qué no puedo iniciar sesión?

Si recibe un error al intentar iniciar sesión en System Manager, revise estas causas posibles.

Los errores de inicio de sesión en System Manager pueden ocurrir por uno de estos motivos:

- Introdujo un nombre de usuario o contraseña incorrectos.
- No tiene privilegios suficientes.
- El servidor de directorio (si está configurado) puede no estar disponible. Si este es el caso, intente iniciar sesión con un rol de usuario local.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Aguarde 10 minutos y

vuelva a intentarlo.

- Se activó la condición de bloqueo y es posible que el registro de auditoría esté completo. Vaya a Access Management y elimine los eventos anteriores del registro de auditoría.
- La autenticación SAML está habilitada. Actualice el explorador para iniciar sesión.

Los errores de inicio de sesión en una cabina de almacenamiento remota para tareas de mirroring pueden ocurrir por uno de estos motivos:

- Introdujo una contraseña incorrecta.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Aguarde 10 minutos para volver a iniciar sesión.
- Se alcanzó la cantidad máxima de conexiones de clientes en la controladora. Busque clientes o usuarios múltiples.

¿Qué debo saber antes de añadir un servidor de directorio?

Antes de añadir un servidor de directorio en Access Management, asegúrese de cumplir con los siguientes requisitos.

- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

¿Qué debo saber acerca de la asignación de roles de la cabina de almacenamiento?

Antes de asignar grupos a roles, revise las siguientes directrices.

Las funcionalidades de control de acceso basado en roles (RBAC) incorporadas en la cabina de almacenamiento incluyen los siguientes roles:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Servicios de directorio

Si usa un servidor de protocolo ligero de acceso a directorios (LDAP) y servicios de directorio, asegúrese de que:

- Un administrador haya definido grupos de usuarios en el servicio de directorio.
- Conoce los nombres de dominio de los grupos de usuarios LDAP.
- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

SAML

Si usa las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) incorporadas en la cabina de almacenamiento, asegúrese de que:

- Un administrador de proveedor de identidades (IDP) haya configurado atributos de usuario y pertenencia a grupos en el sistema del IDP.
- Conoce los nombres de pertenencia a grupos.
- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

¿A cuáles herramientas de gestión externas puede afectar este cambio?

Cuando se realizan ciertos cambios en System Manager, como el cambio de la interfaz de gestión o el uso de SAML como método de autenticación, puede restringirse el uso de algunas herramientas y funciones externas.

Interfaz de gestión

Las herramientas que se comunican directamente con la interfaz de gestión heredada (Symbol), como SANtricity SMI-S Provider u OnCommand Insight (OCI), no funcionan a menos que la configuración interfaz de gestión heredada esté habilitada. Además, no es posible utilizar comandos de la CLI heredados ni realizar operaciones de mirroring si dicha configuración está deshabilitada.

Póngase en contacto con el soporte técnico para obtener más información.

Autenticación SAML

Cuando se habilita SAML, los siguientes clientes no pueden acceder a los recursos y los servicios de la cabina de almacenamiento:

- Enterprise Management Window (EMW)
- Interfaz de línea de comandos (CLI)
- Clientes de kits de desarrollo de software (SDK)
- Clientes en banda
- Clientes HTTP de la API de REST de autenticación básica
- Inicio de sesión mediante extremo estándar de la API de REST

Póngase en contacto con el soporte técnico para obtener más información.

¿Qué debo saber antes de configurar y habilitar SAML?

Antes de configurar y habilitar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) para la autenticación, asegúrese de cumplir con los siguientes

requisitos y comprender las restricciones de SAML.

Requisitos

Antes de comenzar, compruebe lo siguiente:

- Se configuró un proveedor de identidades (IDP) en la red. Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. El equipo de seguridad es responsable de mantener el IDP.
- Un administrador IDP configuró los atributos y los grupos del usuario en el 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 los relojes del servidor de IDP y de la controladora están sincronizados (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 System Manager.
- Conoce la dirección IP o el nombre de dominio de cada controladora de la cabina de almacenamiento.

Restricciones

Además de los requisitos mencionados más arriba, asegúrese de comprender las siguientes restricciones:

- Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda. Se recomienda que pruebe los inicios de sesión SSO para poder habilitar SAML en el paso final de la configuración. (El sistema también hace una prueba de inicio de sesión SSO antes de habilitar SAML.)
- Si deshabilita SAML en el futuro, el sistema restaura automáticamente la configuración anterior (local User roles o Directory Services).
- Si Directory Services está actualmente configurado para la autenticación de usuario, SAML anula esa configuración.
- Cuando se configura SAML, los siguientes clientes no pueden acceder a los recursos de la cabina de almacenamiento:
  - Enterprise Management Window (EMW)
  - Interfaz de línea de comandos (CLI)
  - Clientes de kits de desarrollo de software (SDK)
  - Clientes en banda
  - Clientes HTTP de la API de REST de autenticación básica
  - Inicio de sesión mediante extremo estándar de la API de REST

¿Qué tipo de eventos se registran en el registro de auditoría?

El registro de auditoría puede incluir eventos de modificación, o bien tanto eventos de modificación como de solo lectura.

Según la configuración de la política, se muestran los siguientes tipos de eventos:

- **Eventos de modificación** — acciones del usuario desde System Manager que involucran cambios en el sistema, como el aprovisionamiento de almacenamiento.
- **Eventos de modificación y de sólo lectura** — acciones del usuario que involucran cambios en el sistema, así como eventos que involucran la visualización o descarga de información, como la visualización de asignaciones de volumen.

¿Qué debo saber antes de configurar un servidor de syslog?

Es posible archivar registros de auditoría en un servidor de syslog externo.

Antes de configurar un servidor de syslog, tenga en cuenta las siguientes directrices.

- Asegúrese de conocer la dirección, el protocolo y el número de puerto del servidor. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si el servidor usa un protocolo seguro (por ejemplo, TLS), debe haber disponible un certificado de entidad de certificación (CA) en el sistema local. Los certificados DE CA identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.
- Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.
- La configuración de **Política de sobrescritura** (disponible en View/Edit Settings) no afecta a la forma en que se gestionan los registros con una configuración de servidor syslog.
- Los registros de auditoría tienen el formato de mensajería RFC 5424.

El servidor de syslog ya no recibe registros de auditoría. ¿Qué debo hacer?

Si configuró un servidor de syslog con un protocolo TLS, el servidor no puede recibir mensajes si la certificación no es válida por algún motivo. Se envía un mensaje de error sobre el certificado no válido al registro de auditoría.

Para resolver este problema, debe corregir la certificación para el servidor de syslog. Una vez que haya una cadena de certificados válida vigente, vaya a menú:Configuración[Registro de auditoría > Configurar servidores de syslog > probar todo].