Conceptos

SANtricity 11.8

NetApp
April 05, 2024

Tabla de contenidos

Conceptos

Cómo funciona Access Management

Utilice Access Management para establecer la autenticación de usuario en Unified Manager.

Flujo de trabajo de configuración

La configuración de Access Management funciona de la siguiente manera:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administrador 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. La contraseña se debe establecer en el primer inicio de sesión.

2. El administrador se desplaza hasta Access Management en la interfaz de usuario, donde se incluyen roles de usuario local preconfigurados. Estos roles son una implementación de las funcionalidades de control de acceso basado en roles (RBAC).
3. El administrador configura uno o varios de los siguientes métodos de autenticación:
   - **Roles de usuario local** — la autenticación se administra mediante capacidades RBAC. Los roles de usuario local incluyen usuarios 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, a continuación, asigna los usuarios LDAP a los roles de usuario local.
   - **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 proporciona credenciales de inicio de sesión en Unified Manager a los usuarios.
5. Los usuarios inician sesión en el sistema con sus credenciales. 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 funciones en la interfaz de usuario.
   - Muestra el nombre de usuario en el banner superior.

Funciones disponibles en Unified Manager

El acceso a las funciones 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 de las matrices, pero sin acceso a la configuración de seguridad.
- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. 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 función no disponible se muestra atenuada o directamente no se muestra en la interfaz de usuario.

Terminología de Access Management

Conozca la forma en que los términos de Access Management se aplican a Unified Manager.

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.
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.
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.

Duración	Descripción
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. Unified Manager incluye roles predefinidos.
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.
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.
Proxy de servicios web	El proxy de servicios web, que proporciona acceso mediante mecanismos HTTPS estándar, permite a los administradores configurar servicios de gestión para las cabinas de almacenamiento. El proxy se puede instalar en hosts Windows o Linux. La interfaz de Unified Manager se encuentra disponible con el proxy de servicios web.

Permisos para roles asignados

Las funcionalidades de control de acceso basado en roles (RBAC) incluyen usuarios predefinidos con uno o varios roles asignados. Cada rol incluye permisos para acceder a tareas en Unified 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 de las matrices, pero sin acceso a la configuración de seguridad.
- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. 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 una función determinada, esa función no se encuentra disponible para selección o no se muestra en la interfaz de usuario.

Access Management con roles de usuario local

Los administradores pueden utilizar las funcionalidades de control de acceso basado en roles (RBAC) que se aplican en Unified Manager. Estas capacidades se denominan

"roles de usuario local".

Flujo de trabajo de configuración

Los roles de usuario local están preconfigurados en el sistema. Para usar roles de usuario local con fines de autenticación, los administradores pueden hacer lo siguiente:

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

Los administradores puede usar un servidor de protocolo ligero de acceso a directorios (LDAP) y un servicio de directorio, 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 Unified Manager con un perfil de usuario que incluye permisos de administrador 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 una entidad de certificación (CA) para la autenticación entre el servidor LDAP y el sistema host donde se instaló el proxy de servicios web.
4. Después de establecer la conexión del servidor, el administrador asigna los grupos de usuarios a los roles de usuario local. Estos roles están predefinidos y no pueden modificarse.
5. El administrador prueba la conexión entre el servidor LDAP y el proxy de servicios web.

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

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 Unified 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 Unified 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 Unified Manager para exportar el archivo de metadatos del proveedor de servicios de la controladora. Desde el sistema IdP, el administrador importa el archivo 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 Unified 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 Unified 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 usuarios no pueden detectar ni gestionar el almacenamiento de esa cabina desde la interfaz de Storage Manager heredada.

Además, los siguientes clientes no pueden obtener acceso 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