Gestión del acceso

SANtricity software

NetApp
November 03, 2025

This PDF was generated from https://docs.netapp.com/es-es/e-series-santricity/um-certificates/overview-access-management-um.html on November 03, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestión del acceso . . . 1
- Obtenga más información sobre la gestión de acceso de SANtricity Unified Manager . . . 1
  - ¿Qué métodos de autenticación están disponibles? . . . 1
  - ¿Cómo se configura Access Management? . . . 1
- Conceptos . . . 1
  - Cómo funciona la gestión de acceso en SANtricity Unified Manager . . . 1
  - Conozca la terminología de gestión de acceso de SANtricity Unified Manager . . . 3
  - Permisos para roles asignados . . . 4
  - Gestión de acceso con roles de usuarios locales en SANtricity Unified Manager . . . 4
  - Gestión de acceso con servicios de directorio en SANtricity Unified Manager . . . 5
  - Gestión de acceso con SAML en SANtricity Unified Manager . . . 6
- Use los roles de usuario local . . . 7
  - Ver los roles de usuario local . . . 7
  - Cambiar las contraseñas de los perfiles de usuarios locales en SANtricity Unified Manager . . . 8
  - Cambiar la configuración de la contraseña del usuario local en SANtricity Unified Manager . . . 9
- Uso de los servicios de directorio . . . 9
  - Agregar servidor de directorio en SANtricity Unified Manager . . . 9
  - Editar la configuración del servidor de directorio y las asignaciones de roles en SANtricity Unified Manager . . . 16
  - Quitar un servidor de directorio . . . 19
- Use SAML . . . 20
  - Configurar SAML en SANtricity Unified Manager . . . 20
  - Cambiar las asignaciones de roles SAML en SANtricity Unified Manager . . . 24
  - Exportar archivos del proveedor de servicios SAML en SANtricity Unified Manager . . . 25
- Preguntas frecuentes sobre la gestión de acceso de usuarios para SANtricity Unified Manager . . . 26
  - ¿Por qué no puedo iniciar sesión? . . . 26
  - ¿Qué debo saber antes de añadir un servidor de directorio? . . . 26
  - ¿Qué debo saber acerca de la asignación de roles de la cabina de almacenamiento? . . . 26
  - ¿Qué debo saber antes de configurar y habilitar SAML? . . . 27
  - ¿De qué se tratan los usuarios locales? . . . 28

Gestión del acceso

Obtenga más información sobre la gestión de acceso de SANtricity Unified Manager

Access Management es un método para configurar la autenticación de usuario en SANtricity Unified Manager.

¿Qué métodos de autenticación están disponibles?

Están disponibles los siguientes métodos de autenticación:

- **Roles de usuario local** — la autenticación se administra mediante funciones RBAC (control de acceso basado en roles). Los roles de usuario local incluyen perfiles de usuario predefinidos con permisos de acceso específicos.
- **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.
- **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) que utiliza SAML 2.0.

Obtenga más información:

- "Cómo funciona Access Management"
- "Terminología de Access Management"
- "Permisos para roles asignados"
- "SAML"

¿Cómo se configura Access Management?

El software SANtricity está preconfigurado para usar roles de usuario local. Si desea utilizar LDAP, puede configurarlo en la página Access Management.

Obtenga más información:

- "Access Management con roles de usuario local"
- "Access Management con servicios de directorio"
- "Configure SAML"

Conceptos

Cómo funciona la gestión de acceso en SANtricity Unified Manager

Utilice Access Management para establecer la autenticación de usuario en SANtricity 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.

Conozca la terminología de gestión de acceso de SANtricity Unified Manager

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

Duración	Descripción
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 SANtricity 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.

Gestión de acceso con roles de usuarios locales en SANtricity Unified Manager

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

Gestión de acceso con servicios de directorio en SANtricity Unified Manager

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.

Gestión de acceso con SAML en SANtricity Unified Manager

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

Use los roles de usuario local

Ver los roles de usuario local

Desde la pestaña roles de usuario local, es posible ver las asignaciones de los usuarios a los roles predeterminados. Estas asignaciones forman parte de los RBAC aplicados en el proxy de servicios web de Unified Manager de SANtricity.

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 usuarios y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.

   Los usuarios se muestran en la tabla:

   - **Admin** — Super administrador que tiene acceso a todas las funciones del sistema. Este usuario incluye todos los roles.
   - **Almacenamiento** — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión.
   - **Security**: El usuario responsable de la configuración de seguridad, incluidos Access Management y Certificate Management. Este usuario incluye los siguientes roles: Administrador de seguridad y Supervisión.
   - **Soporte**: El usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este usuario incluye los siguientes roles: Administrador de soporte y Supervisión.
   - **Monitor** — un usuario con acceso de sólo lectura al sistema. Este usuario incluye únicamente el rol Supervisión.

- **rw** (lectura/escritura): Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y monitor.
- **Ro** (sólo lectura) — este usuario incluye sólo la función Monitor.

Cambiar las contraseñas de los perfiles de usuarios locales en SANtricity Unified Manager

Es posible cambiar las contraseñas de usuario de cada 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.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione un usuario de la tabla.

   Se habilita el botón Cambiar contraseña.

4. Seleccione **Cambiar contraseña**.

   Se abre el cuadro de diálogo Cambiar contraseña.

5. Si no existe una longitud mínima de contraseña establecida para las contraseñas de usuario local, puede seleccionar la casilla de comprobación para requerir que el usuario introduzca una contraseña para acceder al sistema.
6. Introduzca la contraseña nueva para el usuario seleccionado en los dos campos.
7. Introduzca su contraseña de administrador local para confirmar esta operación y, a continuación, haga clic en **Cambiar**.

Resultados

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

Cambiar la configuración de la contraseña del usuario local en SANtricity Unified Manager

Es posible configurar la longitud mínima requerida para todas las contraseñas de usuario local nuevas o actualizadas. También es posible permitir a los usuarios locales que accedan al sistema 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 desea que los usuarios locales accedan al sistema sin introducir una contraseña.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione **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 que accedan al sistema *without* password, desactive la casilla de verificación "requerir que todas las contraseñas de usuario local tengan al menos…".
   - Si desea configurar una longitud mínima de contraseña para todas las contraseñas de usuario local, active la casilla de comprobación "requerir que todas las contraseñas de usuario local tengan al menos…" y luego use el cuadro de desplazamiento para configurar la longitud mínima requerida para todas las contraseñas de usuario local

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

5. Haga clic en **Guardar**.

Uso de los servicios de directorio

Agregar servidor de directorio en SANtricity Unified Manager

Para configurar la autenticación de Access Management, se debe establecer la comunicación entre un servidor LDAP y el host donde se ejecuta el proxy de servicios web para Unified Manager de SANtricity. A continuación, se deben asignar los grupos de usuarios LDAP a los roles de usuario local.

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 también un certificado de CA para autenticación si no se encuentra firmado por una entidad de firma estándar. Si se poseen credenciales de una cuenta de enlace, es posible introducir también el nombre de cuenta de usuario y la contraseña. Luego, se deben asignar los grupos de usuarios del servidor LDAP a los roles de usuario local.

Pasos

1. Seleccione **Access Management**.
2. En la ficha **Servicios de directorio**, seleccione **Agregar servidor de directorio**.

   Se abre el cuadro de diálogo Añadir 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)

Ajuste	Descripción
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", es posible introducir un valor como el siguiente `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Enlazar contraseña (opcional)

Ajuste	Descripción
Este campo se muestra cuando se introduce una cuenta de enlace. Introduzca la contraseña de la cuenta de enlace.	Probar conexión del servidor antes de añadir
Seleccione esta casilla de comprobación si desea asegurarse de que el sistema 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.	**Configuración de privilegios**
DN base de búsqueda	Introduzca el contexto de LDAP para buscar usuarios, generalmente con el formato de `CN=Users, DC=cpoc, DC=local`.
Atributo de nombre de usuario	Introduzca el atributo vinculado al ID de usuario para los fines de autenticación. Por ejemplo: `sAMAccountName`.

Ajuste	Descripción
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. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra diagonal inversa (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=?<$	
Funciones	Haga clic en el campo y seleccione uno de los roles de usuario local que se asignará al DN del grupo. Debe seleccionar individualmente cada rol que desee incluir en este grupo. Se requiere el rol de supervisión junto con los demás roles para iniciar sesión en SANtricity Unified Manager. Los roles asignados incluyen los siguientes permisos: • **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.

El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

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 la configuración del servidor de directorio y las asignaciones de roles en SANtricity Unified Manager

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 **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.

Detalles del campo

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 el sistema pueda comunicarse con la configuración del servidor LDAP. La prueba se produce después de hacer clic en **Guardar**. Si se selecciona esta casilla de comprobación y la prueba falla, no se modifica la configuración. Debe resolver el error o desmarcar 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=cpoc, 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.

Detalles del campo

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

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

Quitar un servidor de directorio

Para interrumpir la conexión entre un servidor de directorio y el proxy de servicios web, es posible quitar 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 **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.

Use SAML

Configurar SAML en SANtricity Unified Manager

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 en SANtricity Unified Manager

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.

Exportar archivos del proveedor de servicios SAML en SANtricity Unified Manager

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**.

Preguntas frecuentes sobre la gestión de acceso de usuarios para SANtricity Unified Manager

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

¿Por qué no puedo iniciar sesión?

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

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

- Introdujo un nombre de usuario o contraseña incorrectos.
- No tiene privilegios suficientes.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Aguarde 10 minutos y vuelva a intentarlo.
- La autenticación SAML está habilitada. Actualice el explorador para iniciar sesión.

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

Antes de añadir un servidor de directorio en Access Management, debe cumplir ciertos 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 directrices.

Las funcionalidades de RBAC incluyen los siguientes roles:

- **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.

El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

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.

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.
- Conoce 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:

```
\.[]{}()<>*+-=!?^$|
```

- 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.

¿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 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.
- Conoce la dirección IP o el nombre de dominio de la 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

¿De qué se tratan los usuarios locales?

Los usuarios locales están predefinidos en el sistema e incluyen permisos específicos.

Entre ellos, se incluyen:

- **Admin** — Super administrador que tiene acceso a todas las funciones del sistema. Este usuario incluye todos los roles. La contraseña se debe establecer en el primer inicio de sesión.
- **Almacenamiento** — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Security**: El usuario responsable de la configuración de seguridad, incluidos Access Management y Certificate Management. Este usuario incluye los siguientes roles: Administrador de seguridad y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Soporte**: El usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este usuario incluye los siguientes roles: Administrador de soporte y Supervisión. Esta cuenta está

deshabilitada hasta que se defina una contraseña.

- **Monitor** — un usuario con acceso de sólo lectura al sistema. Este usuario incluye únicamente el rol Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **rw** (lectura/escritura): Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Ro** (sólo lectura) — este usuario incluye sólo la función Monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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