Access Management

SANtricity 11.6

NetApp
February 12, 2024

Tabla de contenidos

Access Management

Conceptos

Cómo funciona Access Management

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.
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 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.
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.

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 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. **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 SANtricity 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.

Procedimientos

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 contraseñas

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.

   El botón **Cambiar contraseña** estará disponible.

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.

Cambie la configuración de contraseña de usuario local

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**.

Añadir servidor de directorio

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 **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)

Ajuste	Descripción
Este campo aparece solo si se especific a 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.	**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`.

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.	Funciones

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 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 **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 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=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.

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.

Preguntas frecuentes

¿Por qué no puedo iniciar sesión?

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

Los errores de inicio de sesión en Unified 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.

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, 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.

¿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.