



# **Certificados y autenticación**

SANtricity 11.6

NetApp  
February 12, 2024

# Tabla de contenidos

- Certificados y autenticación ..... 1
  - Gestión de certificados..... 1
  - Access Management ..... 9

# Certificados y autenticación

## Gestión de certificados

### Conceptos

#### Cómo funcionan los certificados

Los certificados son archivos digitales que identifican entidades en línea, como sitios web y servidores, para poder establecer comunicaciones seguras en Internet.

#### Certificados firmados

Los certificados garantizan que solo se transmitan comunicaciones web en formato cifrado, de forma privada y sin alternaciones, entre el servidor especificado y el cliente. Con Unified Manager, es posible gestionar los certificados para el explorador en un sistema de gestión host y las controladoras en las cabinas de almacenamiento detectadas.

Un certificado puede estar firmado por una autoridad de confianza o puede ser autofirmado. La firma simplemente implica que alguien validó la identidad del propietario y determinó que sus dispositivos son de confianza. Las cabinas de almacenamiento se entregan con un certificado autofirmado generado automáticamente en cada controladora. Puede continuar usando el certificado autofirmado o puede obtener certificados firmados por CA para establecer conexiones más seguras entre las controladoras y los sistemas host.



Si bien los certificados firmados por CA aumentan la protección de seguridad (por ejemplo, evitan los ataques de tipo "man in the middle"), también aplican tarifas que pueden ser costosas si la red es extensa. En cambio, los certificados autofirmados son menos seguros, pero son gratuitos. Por lo tanto, los certificados autofirmados se utilizan con mayor frecuencia para entornos de prueba internos, no en entornos de producción.

Un certificado firmado es validado por una entidad de certificación (CA), que es una organización de terceros de confianza. Los certificados firmados incluyen detalles sobre el propietario de la entidad (generalmente, un servidor o sitio web), la fecha de emisión y de vencimiento del certificado, los dominios válidos de la entidad, y una firma digital compuesta por letras y números.

Al abrir un explorador y escribir una dirección web, el sistema ejecuta un proceso de comprobación de certificados en segundo plano para determinar si el usuario se está conectando a un sitio web que incluye un certificado válido firmado por una CA. Generalmente, un sitio que está protegido con un certificado firmado incluye un icono de candado y una designación https en la dirección. Si el usuario intenta conectarse a un sitio web que no contiene un certificado firmado por CA, el explorador mostrará una advertencia para indicar que el sitio no es seguro.

La CA toma las medidas necesarias para verificar las identidades durante el proceso de solicitud. La entidad puede enviar un correo electrónico a la empresa registrada, verificar la dirección empresarial, y realizar una verificación de HTTP o DNS. Una vez completado el proceso de solicitud, la CA envía los archivos digitales para cargar en el sistema de gestión host. Normalmente, estos archivos contienen una cadena de confianza como la siguiente:

- **Raíz** — en la parte superior de la jerarquía está el certificado raíz, que contiene una clave privada utilizada para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.

- **Intermediate** — ramificándose desde la raíz son los certificados intermedios. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
- **Servidor** — en la parte inferior de la cadena se encuentra el certificado de servidor, que identifica su entidad específica, como un sitio web u otro dispositivo. Cada controladora de una cabina de almacenamiento requiere un certificado de servidor aparte.

### Certificados autofirmados

Cada controladora de la cabina de almacenamiento incluye un certificado autofirmado preinstalado. Un certificado autofirmado es similar a un certificado firmado por CA, excepto que es validado por el propietario de la entidad y no por un tercero. Al igual que un certificado firmado por CA, un certificado autofirmado contiene su propia clave privada, y también garantiza que los datos se cifren y se envíen a través de una conexión HTTPS entre un servidor y un cliente.

Los certificados autofirmados no son «'de confianza'» por parte de los navegadores. Cada vez que intente conectarse a un sitio web que solo contiene un certificado autofirmado, el explorador mostrará un mensaje de advertencia. Deberá hacer clic en un enlace del mensaje de advertencia para continuar al sitio web; al hacer eso, estará aceptando básicamente el certificado autofirmado.

### Certificados para Unified Manager

La interfaz de Unified Manager se instala con el proxy de servicios web en un sistema host. Al abrir un explorador y intentar una conexión con Unified Manager, el explorador intenta verificar si el host es un origen de confianza mediante la comprobación de un certificado digital. Si el explorador no encuentra un certificado firmado por CA para el servidor, abrirá un mensaje de advertencia. Desde allí, podrá continuar al sitio web para aceptar el certificado autofirmado en esa sesión. También puede obtener certificados digitales firmados de una CA para que ya no vea el mensaje de advertencia.

### Certificados para controladoras

Durante una sesión de Unified Manager, es posible que vea mensajes de seguridad adicionales al intentar acceder a una controladora que no tiene un certificado firmado por CA. En este caso, puede confiar de forma permanente en el certificado autofirmado o puede importar los certificados firmados por CA de las controladoras para que el proxy de servicios web pueda autenticar las solicitudes de cliente entrantes procedentes de estas controladoras.

### Terminología de certificados

Los siguientes términos se utilizan en la gestión de certificados.

Duración	Descripción
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.
CSR	Una solicitud de firma de certificación (CSR) es un mensaje que envía un solicitante a una entidad de certificación (CA). La CSR valida la información que requiere la CA para emitir un certificado.

<b>Duración</b>	<b>Descripción</b>
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.
Cadena de certificados	La cadena de certificados es una jerarquía de archivos que suma una capa de seguridad a los certificados. Normalmente, la cadena incluye un certificado raíz en la parte superior de la jerarquía, uno o varios certificados intermedios y los certificados de servidor que identifican a las entidades.
Certificado intermedio	Uno o varios certificados intermedios se extienden como una rama del certificado raíz en la cadena de certificados. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
Almacén de claves	Un almacén de claves es un repositorio en el sistema de gestión host que contiene claves privadas, junto con sus correspondientes claves públicas y certificados. Estas claves y certificados identifican a las entidades propias como, por ejemplo, las controladoras.
Certificado raíz	El certificado raíz se encuentra en la parte superior de la jerarquía de la cadena de certificados y contiene una clave privada que se utiliza para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.
Certificado firmado	Un certificado que ha validado una entidad de certificación (CA). Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. Además, un certificado firmado incluye detalles sobre el propietario de la entidad (normalmente, un servidor o sitio web) y una firma digital compuesta por letras y números. Un certificado firmado usa una cadena de certificados y, por consiguiente, se utiliza con mayor frecuencia en los entornos de producción. También se conoce como "certificado firmado por CA" o "certificado de gestión".
Certificado autofirmado	Un certificado autofirmado es validado por el propietario de la entidad. Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. También incluye una firma digital compuesta por letras y números. Un certificado autofirmado no usa la misma cadena de confianza que un certificado firmado por CA y, por consiguiente, se utiliza con mayor frecuencia en los entornos de prueba. También se conoce como certificado "preinstalado".
Certificado de servidor	El certificado de servidor se encuentra en la parte inferior de la cadena de certificados. Este certificado identifica la entidad específica del usuario, por ejemplo, un sitio web u otro dispositivo. Cada controladora de un sistema de almacenamiento requiere un certificado de servidor aparte.

Duración	Descripción
Almacén de confianza	Un almacén de confianza es un repositorio que contiene certificados de terceros de confianza, por ejemplo, entidades de certificación.
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 incluye en el bundle con el proxy de servicios web.

## Procedimientos

### Usar certificados firmados por CA

Es posible obtener e importar certificados firmados por CA para establecer un acceso seguro al sistema de gestión donde se aloja Unified Manager.

#### Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

#### Acerca de esta tarea

El uso de certificados firmados por CA implica un procedimiento de dos pasos.

#### Paso 1: Complete y envíe una CSR

Primero, debe generar un archivo de solicitud de firma de certificación (CSR) y enviarlo a la entidad de certificación (CA).

#### 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 certificación.

#### Acerca de esta tarea

En esta tarea, se describe la forma de generar un archivo CSR y enviarlo a una CA a fin de recibir certificados de gestión firmados para el sistema donde se aloja Unified Manager y el proxy de servicios web. Se debe proporcionar información sobre la organización, más la dirección IP o el nombre DNS del sistema host.



No genere una nueva CSR después de enviar una a la CA. Al generar una CSR, el sistema crea una pareja de claves pública y privada. La clave pública se incluye en la CSR, mientras que la clave privada se conserva en el almacén de claves. Al recibir los certificados firmados e importarlos al almacén de claves, el sistema se asegura de que las claves pública y privada sean la pareja original. Por lo tanto, no debe generar una nueva CSR después de enviar una a la CA. Si lo hace, las controladoras generarán claves nuevas y los certificados que reciba de la CA no funcionarán.

#### Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha **Gestión**, seleccione **completar CSR**.

3. Introduzca la siguiente información y, a continuación, haga clic en **Siguiente**:

- **Organización** — el nombre completo y legal de su empresa u organización. Incluya sufijos, como Inc. O Corp
- **Unidad organizativa (opcional)** — la división de su organización que maneja el certificado.
- **Ciudad/localidad** — la ciudad donde se encuentra su sistema anfitrión o negocio.
- **Estado/Región (opcional)** — el estado o región donde está ubicado el sistema o negocio anfitrión.
- **Código ISO de país**: Código ISO (Organización Internacional de Normalización) de dos dígitos de su país, por ejemplo, US.

4. Introduzca la siguiente información sobre el sistema host:

- **Nombre común** — la dirección IP o el nombre DNS del sistema host donde está instalado Web Services Proxy. Compruebe que la dirección sea correcta; esta debe coincidir exactamente con lo que se escribe para acceder a Unified Manager en el explorador. No incluya http:// ni https://.
- **Direcciones IP alternativas** — Si el nombre común es una dirección IP, opcionalmente puede escribir cualquier dirección IP adicional o alias para el sistema host. Si va a introducir varios datos, use un formato delimitado por comas.
- **Nombres DNS alternativos** — Si el nombre común es un nombre DNS, introduzca cualquier nombre DNS adicional para el sistema host. Si va a introducir varios datos, use un formato delimitado por comas. Si no hay nombres DNS alternativos, pero especificó un nombre DNS en el primer campo, copie ese nombre aquí.

5. Haga clic en **Finalizar**.

Se descarga un archivo CSR en el sistema local. La ubicación de la carpeta de la descarga depende del explorador.

6. Envíe el archivo CSR a una CA y solicite certificados firmados en formato PEM o DER.

## Después de terminar

Espere a que la CA devuelva los archivos de certificado y vaya a. "[Paso 2: Importar certificados de gestión](#)".

## Paso 2: Importar certificados de gestión

Después de recibir los certificados firmados, importe la cadena de certificados para el sistema host donde se instaló la interfaz de Unified Manager.

## Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Generó una solicitud de firma de certificación (archivo .CSR) y la envió a la CA.
- La CA devolvió archivos de certificado de confianza.
- Los archivos de certificado están instalados en el sistema local.
- Si la CA proporcionó un certificado encadenado (por ejemplo, un archivo .p7b), debe desempaquetar el archivo encadenado en archivos individuales: El certificado raíz, el o los certificados intermedios y el certificado de servidor. Puede utilizar Windows `certmgr` Utilidad para desempaquetar los archivos (haga clic con el botón derecho y seleccione **menú: todas las tareas[Exportar]**). Una vez completadas las exportaciones, se mostrará un archivo CER para cada archivo de certificado de la cadena.

## Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha **Administración**, seleccione **Importar**.

Se abre un cuadro de diálogo para importar los archivos de certificado.

3. Haga clic en **examinar** para seleccionar primero el archivo raíz y los archivos intermedios y, a continuación, seleccionar el certificado de servidor.

Se muestran los nombres de los archivos en el cuadro de diálogo.

4. Haga clic en **Importar**.

## Resultados

Los archivos se cargan y validan. La información del certificado aparece en la página Gestión de certificados.

## Restablezca los certificados de gestión

Es posible revertir el certificado de gestión a su estado autofirmado original de fábrica.

### 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 certificación.

### Acerca de esta tarea

Esta tarea elimina el certificado de gestión actual del sistema host donde están instalados el proxy de servicios web y Unified Manager de SANtricity. Una vez restablecido el certificado, el sistema host se revierte al uso del certificado autofirmado.

### Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha **Gestión**, seleccione **Restablecer**.

Se abre el cuadro de diálogo **Confirmar restablecimiento del certificado de administración**.

3. Tipo `reset` En el campo y, a continuación, haga clic en **Restablecer**.

Una vez que se actualiza el explorador, es posible que el explorador bloquee el acceso al sitio de destino e informe de que el sitio utiliza HTTP estricto Transport Security. Esta condición surge cuando se cambia a certificados autofirmados. Para borrar la condición que bloquea el acceso al destino, debe borrar los datos de navegación del explorador.

## Resultados

El sistema se revierte al uso del certificado autofirmado del servidor. Como resultado, el sistema solicita a los usuarios que acepten manualmente el certificado autofirmado para sus sesiones.

## Importar certificados para cabinas

Si es necesario, puede importar certificados para las cabinas de almacenamiento de modo que estas se puedan autenticar con el sistema donde se aloja SANtricity Unified Manager. Los certificados pueden estar firmados por una entidad de certificación (CA) o ser autofirmados.



### 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 certificación.
- Si desea importar certificados de confianza, es necesario importar los certificados para las controladoras de las cabinas de almacenamiento mediante SANtricity System Manager.

### Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.

Esta página muestra todos los certificados notificados para las cabinas de almacenamiento.

3. Seleccione **MENU:Importar[certificados]** para importar un certificado de CA o **MENU:Importar[certificados de matriz de almacenamiento autofirmados]** para importar un certificado autofirmado.

Para limitar la vista, puede utilizar el campo de filtrado **Mostrar certificados...** o puede ordenar las filas de certificados haciendo clic en uno de los encabezados de columna.

4. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

El certificado se carga y se valida.

### Ver certificados

Es posible ver información resumida de un certificado, incluida la organización que utiliza el certificado, la entidad que lo emite, el periodo de validez y las huellas digitales (identificadores únicos).

### 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 certificación.

### Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione una de las siguientes pestañas:
  - **Administración** — muestra el certificado para el sistema que aloja el proxy de servicios web. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro a Unified Manager.
  - **Trusted**: Muestra los certificados a los que Unified Manager puede acceder para matrices de almacenamiento y otros servidores remotos, como un servidor LDAP. Los certificados pueden emitirse mediante una CA o estar autofirmados.
3. Para ver más información sobre un certificado, seleccione la fila correspondiente, seleccione las tres puntos al final de la fila y haga clic en **Ver** o **Exportar**.

### Exportar certificados

Es posible exportar un certificado para ver todos sus detalles.

### Antes de empezar

Para abrir el archivo exportado, debe contar con una aplicación para visualización de certificados.

### Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione una de las siguientes pestañas:
  - **Administración** — muestra el certificado para el sistema que aloja el proxy de servicios web. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro a Unified Manager.
  - **Trusted**: Muestra los certificados a los que Unified Manager puede acceder para matrices de almacenamiento y otros servidores remotos, como un servidor LDAP. Los certificados pueden emitirse mediante una CA o estar autofirmados.
3. Seleccione un certificado de la página y, a continuación, haga clic en los tres puntos al final de la fila.
4. Haga clic en **Exportar** y guarde el archivo de certificado.
5. Abra el archivo en la aplicación para visualización de certificados.

### Elimine certificados de confianza

Puede eliminar uno o varios certificados que ya no sean necesarios, por ejemplo, un certificado caducado.

#### Antes de empezar

Importe el certificado nuevo antes de eliminar el antiguo.



Tenga en cuenta que la eliminación de un certificado intermedio o de raíz puede afectar a varias cabinas de almacenamiento, ya que es posible que estas cabinas compartan los mismos archivos de certificado.

### Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.
3. Seleccione uno o varios certificados de la tabla y, a continuación, haga clic en **Eliminar**.



La función **Eliminar** no está disponible para los certificados preinstalados.

Se abrirá el cuadro de diálogo Confirmar eliminación de certificado de confianza.

4. Confirme la eliminación y haga clic en **Eliminar**.

El certificado se eliminará de la tabla.

### Resuelva los certificados que no son de confianza

Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una conexión con SANtricity Unified Manager, pero no se confirma que la conexión sea segura. En la página Certificado, puede resolver certificados que no son de confianza al importar un certificado autofirmado de la cabina de almacenamiento o al importar un certificado de una entidad de certificación (CA) que emitió un tercero de

confianza.

### Antes de empezar

- Inició sesión con un perfil de usuario que cuenta con permisos de administración de seguridad.
- Si tiene pensado importar un certificado firmado por una CA:
  - Generó una solicitud de firma de certificación (archivo .CSR) para cada controladora en la cabina de almacenamiento y la envió a la CA.
  - La CA devolvió archivos de certificado de confianza.
  - Los archivos de certificado están disponibles en el sistema local.

### Acerca de esta tarea

Es posible que necesite instalar otros certificados de CA de confianza si se da alguna de las siguientes condiciones:

- Añadió recientemente una cabina de almacenamiento.
- Uno o ambos certificados caducaron.
- Uno o ambos certificados fueron revocados.
- Falta un certificado raíz o intermedio en uno o ambos certificados.

### Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.

Esta página muestra todos los certificados notificados para las cabinas de almacenamiento.

3. Seleccione **MENU:Import[Certificates]**. Para importar un certificado de CA o **menú:Importar[certificados de la cabina de almacenamiento autofirmados]** para importar un certificado autofirmado.

Para limitar la vista, puede utilizar el campo de filtrado **Mostrar certificados...** o puede ordenar las filas de certificados haciendo clic en uno de los encabezados de columna.

4. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

El certificado se carga y se valida.

## 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.
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
<b>Ajustes de configuración</b>	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 ( <i>username@domain</i> ) 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 <code>ldap[s]://host:port</code> .	Cargar certificado (opcional)

Ajuste	Descripción
<div data-bbox="245 363 302 415"></div> <p data-bbox="362 170 480 611">Este campo aparece solo si se especifica a un protocolo LDAPS en el campo URL del servidor arriba.</p> <p data-bbox="212 659 509 961">Haga clic en <b>examinar</b> 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.</p>	<p data-bbox="529 159 846 191">Enlazar cuenta (opcional)</p>
<p data-bbox="212 1014 505 1598">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 <code>CN=bindacct,CN=Users,DC=cpoc,DC=local</code>.</p>	<p data-bbox="529 1014 899 1045">Enlazar contraseña (opcional)</p>

Ajuste		Descripción
 <p>Este campo se muestra cuando se introduce una cuenta de enlace.</p>	<p>Introduzca la contraseña de la cuenta de enlace.</p>	Probar conexión del servidor antes de añadir
	<p>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 <b>Agregar</b> 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.</p>	<b>Ajustes de privilegios</b>
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: <code>memberOf</code> , <code>managedObjects</code> .

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

#### Detalles del campo

Ajuste	Descripción
<b>Asignaciones</b>	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.

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

- Seleccione **Access Management**.
- Seleccione la ficha **Servicios de directorio**.
- 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
<b>Ajustes de configuración</b>	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 ( <i>username@domain</i> ) 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 <code>ldap[s]://host:port</code> .	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 <b>Guardar</b> . 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.	<b>Configuración de privilegios</b>
DN base de búsqueda	El contexto de LDAP para buscar usuarios, normalmente en la forma de <code>CN=Users, DC=copc, DC=local</code> .
Atributo de nombre de usuario	El atributo que está vinculado al ID de usuario para la autenticación. Por ejemplo: <code>sAMAccountName</code> .
Atributos de grupo	Lista de atributos de grupo en el usuario, que se utiliza para la asignación de grupos a roles. Por ejemplo: <code>memberOf, managedObjects</code> .

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

Ajuste	Descripción
<b>Asignaciones</b>	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. Espere 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. Espere 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.

## Información de copyright

Copyright © 2024 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.