



# Certificados

## SANtricity 11.7

NetApp  
February 12, 2024

# Tabla de contenidos

- Certificados ..... 1
  - Información general sobre certificados ..... 1
  - Conceptos ..... 1
  - Utilice certificados firmados por CA para el sistema de gestión ..... 4
  - Restablezca los certificados de gestión ..... 6
  - Usar certificados de cabina ..... 7
  - Gestionar certificados ..... 9

# Certificados

## Información general sobre certificados

La gestión de certificados permite crear solicitudes de firma de certificados (CSR), importar certificados y gestionar certificados existentes.

### ¿Qué son los certificados?

*Certificates* son archivos digitales que identifican entidades en línea, como sitios web y servidores, para comunicaciones seguras en Internet. Existen dos tipos de certificados: Un *certificado firmado* es validado por una entidad de certificación (CA) y un *certificado autofirmado* es validado por el propietario de la entidad en lugar de por un tercero.

Obtenga más información:

- ["Cómo funcionan los certificados"](#)
- ["Terminología de certificados"](#)

### ¿Cómo se configuran los certificados?

En Certificate Management, es posible configurar certificados para la estación de gestión donde se aloja Unified Manager e importar también certificados para las controladoras en las cabinas.

Obtenga más información:

- ["Utilice certificados firmados por CA para el sistema de gestión"](#)
- ["Importar certificados para cabinas"](#)

## 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.
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.

Duración	Descripción
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.
Almacén de confianza	Un almacén de confianza es un repositorio que contiene certificados de terceros de confianza, por ejemplo, entidades de certificación.

## Utilice certificados firmados por CA para el sistema de gestión

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 tres pasos.

### Paso 1: Complete un archivo CSR

Primero, se debe generar un archivo de solicitud de firma de certificación (CSR), que identifica a la organización y al sistema host donde están instalados el proxy de servicios web y Unified Manager.



También puede generar un archivo CSR con una herramienta como OpenSSL y saltar a. [Paso 2: Enviar archivo CSR.](#)

### Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha Administración, 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 donde está instalado el proxy de servicios web:
  - **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://. El nombre DNS no puede comenzar con un comodín.
  - **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. El nombre DNS no puede comenzar con un comodín.
5. Asegúrese de que la información del host sea correcta. Si no lo es, los certificados que se devuelven de la CA fallarán cuando intente importarlos.
6. Haga clic en **Finalizar**.
7. Vaya a. [Paso 2: Enviar archivo CSR](#).

## Paso 2: Enviar archivo CSR

Después de crear un archivo de solicitud de firma de certificación (CSR), se lo envía a una entidad de certificación (CA) para recibir certificados de gestión firmados para el sistema donde se aloja Unified Manager y el proxy de servicios web.



Los sistemas E-Series requieren un formato PEM (codificación ASCII Base64) para certificados firmados, que incluye los siguientes tipos de archivo: .Pem, .crt, .cer o .key.

### Pasos

1. Busque el archivo CSR descargado.

La ubicación de la carpeta de la descarga depende del explorador.

2. Envíe el archivo CSR a una CA (por ejemplo, VeriSign o DigiCert) y solicite certificados firmados en formato PEM.



**Después de enviar un archivo CSR a la CA, NO vuelva a generar otro archivo CSR.** cada vez que genere una CSR, el sistema creará un par 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 del sistema. Cuando recibe los certificados firmados e importarlos, el sistema se asegura de que las claves pública y privada sean la pareja original. Si las claves no coinciden, los certificados firmados no funcionarán y debe solicitar certificados nuevos de la CA.

3. Cuando la CA devuelva los certificados firmados, vaya a [Paso 3: Importar certificados de gestión](#).

### Paso 3: Importar certificados de gestión

Después de recibir certificados firmados de la CA, importe los certificados al sistema host donde se instalaron la interfaz de proxy de servicios web y Unified Manager.

#### Antes de empezar

- Recibió certificados firmados de la CA. Estos archivos incluyen el certificado raíz, uno o varios certificados intermedios y el certificado de servidor.
- Si la CA proporcionó un archivo de 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 MENU: todas las tareas[Exportar]). Se recomienda la codificación base-64. Una vez completadas las exportaciones, se mostrará un archivo CER para cada archivo de certificado de la cadena.
- Copió los archivos de certificado en el sistema host donde se ejecuta el proxy de servicios web.

#### 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 los archivos de certificado raíz e intermedio y, a continuación, seleccionar el certificado de servidor. Si generó la CSR desde una herramienta externa, también debe importar el archivo de claves privadas que se creó junto con la CSR.

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. 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 Administración, seleccione **Restablecer**.

Se abre el cuadro de diálogo Confirmar restablecimiento de certificado de gestión.

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.

# Usar certificados de cabina

## 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 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 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 menú:Importar[certificados] 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.

## 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 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 menú:Importar[certificados] 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.

# Gestionar certificados

## 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.

## 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 INTERRUPTIÓN 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.