Certificados

SANtricity 11.6

NetApp
February 12, 2024

Tabla de contenidos

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.

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 System Manager, puede gestionar los certificados entre el explorador en un sistema de gestión host (que actúa como cliente) y las controladoras en un sistema de almacenamiento (que actúan como servidores).

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.

Certificados firmados

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 se encuentra el certificado raíz, que 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.
- Intermedio: Como una rama del certificado raíz, se encuentran 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 la entidad específica del usuario, 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. Sin embargo, un certificado autofirmado no utiliza la misma cadena de confianza que un certificado firmado por CA.

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 usados para el servidor de gestión de claves

Si usa un servidor de gestión de claves externo con la función Drive Security, también puede gestionar los certificados para la autenticación entre ese servidor y las 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.

Duración	Descripción
Certificado de cliente	En la gestión de claves de seguridad, un certificado de cliente valida las controladoras de la cabina de almacenamiento a fin de que el servidor de gestión de claves pueda confiar en sus direcciones IP.
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.
Certificado de servidor de gestión de claves	En la gestión de claves de seguridad, un certificado de servidor de gestión de claves valida el servidor a fin de que la cabina de almacenamiento pueda confiar en su dirección IP.
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.
Servidor OCSP	El servidor de protocolo de estado de certificado en línea (OCSP) determina si la entidad de certificación (CA) ha revocado algún certificado antes de su fecha de vencimiento programada y bloquea el acceso del usuario a un servidor si se ha revocado el certificado.
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".

Duración	Descripción
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.

Procedimientos

Use certificados firmados por CA para las controladoras

Es posible obtener certificados firmados por CA para establecer comunicaciones seguras entre las controladoras y el explorador que se utiliza para acceder a System 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 y envíe una CSR para las controladoras

Primero, es necesario generar un archivo de solicitud de firma de certificación (CSR) para cada controladora de la cabina de almacenamiento y, a continuación, enviar los archivos a la entidad de certificación (CA).

Antes de empezar

- Debe conocer la dirección IP o el nombre DNS de cada controladora.

Acerca de esta tarea

La CSR proporciona información sobre su organización, la dirección IP o el nombre DNS de la controladora, y una pareja de claves para identificar el servidor web de la controladora. Durante esta tarea, se genera un archivo CSR si solo existe una controladora en la cabina de almacenamiento y dos archivos CSR si existen dos controladoras.

> 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 **MENU:Settings[Certificates]**.
2. En la ficha **Gestión de matrices**, seleccione **completar CSR**.

> Si aparece un cuadro de diálogo que le pide que acepte un certificado autofirmado para el segundo controlador, haga clic en **Aceptar certificado autofirmado** para continuar.

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** — Ciudad en la que se encuentra la matriz de almacenamiento o el negocio.
   - **Estado/Región (opcional)** — el estado o región donde está ubicada la matriz de almacenamiento o el negocio.
   - **Código ISO de país**: Código ISO (Organización Internacional de Normalización) de dos dígitos de su país, por ejemplo, US.

     Algunos campos pueden autocompletarse con la información adecuada, como la dirección IP de la controladora. No cambie los valores autocompletados a menos que esté seguro de que son incorrectos. Por ejemplo, si todavía no ha completado una CSR, la dirección IP de la controladora se establecerá en "'localhost'". En ese caso, deberá cambiar «'localhost'» por el nombre DNS o la dirección IP del controlador.

4. Verifique o introduzca la siguiente información acerca de la controladora A en su cabina de almacenamiento:
   - **Controller un nombre común** — la dirección IP o el nombre DNS del controlador A se muestran de manera predeterminada. Compruebe que la dirección sea correcta; debe coincidir exactamente con lo que escribe para acceder a System Manager en el explorador.
   - **Controller a Alternate IP address** — Si el nombre común es una dirección IP, puede opcionalmente escribir cualquier dirección IP adicional o alias para el controlador A. Si va a introducir varios datos, use un formato delimitado por comas.
   - **Nombre DNS alternativo del controlador a** — Si el nombre común es un nombre DNS, introduzca cualquier nombre DNS adicional para el controlador A. 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. Si la cabina de almacenamiento sólo tiene una controladora, el botón **Finalizar** estará disponible. Si la cabina de almacenamiento tiene dos controladores, el botón **Siguiente** estará disponible.

     No haga clic en el enlace **Omitir este paso** cuando cree inicialmente una solicitud CSR. El enlace se proporciona para situaciones de recuperación de errores. En raras ocasiones, una solicitud CSR puede generar errores en una controladora, pero no en la otra. Este enlace permite omitir el paso para crear una solicitud CSR en la controladora A si ya está definida, y continuar hacia el siguiente paso para volver a crear una solicitud CSR en la controladora B.

5. Si sólo hay un controlador, haga clic en **Finalizar**. Si hay dos controladores, haga clic en **Siguiente** para introducir información para el controlador B (igual que el anterior) y, a continuación, haga clic en **Finalizar**.

   Para una sola controladora, se descarga un archivo CSR en el sistema local. Para controladoras dobles, se descargan dos archivos CSR. La ubicación de la carpeta de la descarga depende del explorador.

6. Busque los archivos CSR descargados. La ubicación de la carpeta depende del explorador.
7. Envíe los archivos CSR a una CA y solicite certificados firmados en formato PEM.
8. Espere a que la CA devuelva los certificados y vaya a. Paso 2: Importe los certificados firmados para las controladoras.

Paso 2: Importe los certificados firmados para las controladoras

Después de recibir los certificados firmados, es necesario importar los archivos para las controladoras.

Antes de empezar

- La CA devolvió archivos de certificado firmados.
- Los archivos se encuentran disponibles 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 los certificados de servidor que identifican a las controladoras. 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.

Acerca de esta tarea

En esta tarea, se describe la manera de cargar los archivos de certificado.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Administración de matrices**, seleccione **Importar**.

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

3. Haga clic en los botones **examinar** para seleccionar primero el archivo raíz y los archivos intermedios y, a continuación, seleccionar cada certificado de servidor para los controladores. El archivo raíz y los archivos intermedios son los mismos para ambas controladoras. Solo los certificados de servidor son únicos para cada controladora.

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

4. Haga clic en **Importar**.

   Los archivos se cargan y validan.

Resultados

La sesión finaliza automáticamente. Debe volver a iniciar sesión para que los certificados entren en vigencia. Cuando inicia sesión nuevamente, se utiliza el nuevo certificado firmado por la CA en la sesión.

Restablezca los certificados de gestión

Es posible revertir los certificados que se usan en las controladoras de los certificados firmados por CA a los certificados autofirmados 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.
- Se deben importar de forma previa los certificados firmados por CA.

Acerca de esta tarea

La función Restablecer elimina los archivos de certificados firmados por CA actuales de cada controladora. A continuación, las controladoras revierten al uso de certificados autofirmados.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Administración de matrices**, seleccione **Restablecer**.

   Se abre el cuadro de diálogo Confirmar **Restablecer certificados 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

Las controladoras revierten al uso de certificados autofirmados. Como resultado, el sistema solicita a los usuarios que acepten manualmente el certificado autofirmado para sus sesiones.

Vea información de certificaciones importadas

Desde la página certificados, es posible ver el tipo de certificado, la entidad emisora y el rango válido de fechas de los certificados para la cabina de almacenamiento.

Antes de empezar

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

Pasos

1. Seleccione MENU:Settings[Certificates].
2. Seleccione una de las pestañas para ver información sobre los certificados.

Pestaña	Descripción
Gestión de cabinas	Vea información sobre los certificados firmados por CA importados para cada controladora, incluido el archivo raíz, los archivos intermedios y los archivos de servidor.
De confianza	Vea información sobre los otros tipos de certificados importados para las controladoras. Utilice el campo de filtro en **Mostrar certificados…** para ver certificados instalados por el usuario o instalados previamente. • **Instalado por el usuario**. Los certificados que un usuario cargó en la cabina de almacenamiento, los cuales pueden incluir certificados de confianza cuando la controladora funciona como cliente (en lugar de servidor), certificados LDAPS y certificados de la Federación de identidades. • **Preinstalado**. Los certificados autofirmados incluidos con la cabina de almacenamiento.

Pestaña	Descripción
Gestión de claves	Vea información sobre los certificados firmados por CA importados para un servidor de gestión de claves externo.

Importar certificados para las controladoras cuando funcionan como clientes

Si la controladora rechaza una conexión debido a que no puede validar la cadena de confianza de un servidor de red, es posible importar un certificado de la pestaña de confianza con el que la controladora (actuando como cliente) pueda aceptar comunicaciones de ese servidor.

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.
- Los archivos de certificado están instalados en el sistema local.

Acerca de esta tarea

Es posible que sea necesario importar certificados de la pestaña de confianza para permitir que otro servidor se comunique con las controladoras (por ejemplo, un servidor de syslog o un servidor LDAP que utiliza TLS).

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Trusted**, seleccione **Importar**.

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

3. Haga clic en **examinar** para seleccionar los archivos de certificado para los controladores.

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

4. Haga clic en **Importar**.

Resultados

Los archivos se cargan y validan.

Habilite la comprobación de revocación de certificados

Es posible habilitar comprobaciones automáticas de certificados revocados para que el servidor de protocolo de estado de certificado en línea (OCSP) bloquee los usuarios y no permita que realicen conexiones no seguras.

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.
- Existe un servidor DNS configurado en las dos controladoras, lo que permite usar un nombre de dominio completo para el servidor OCSP. Esta tarea está disponible en la página hardware.
- Si desea especificar su propio servidor OCSP, debe conocer la URL de ese servidor.

Acerca de esta tarea

La comprobación de revocación automática es útil cuando la CA emite de manera incorrecta un certificado o cuando la clave privada está en riesgo.

Durante esta tarea, es posible configurar un servidor OCSP o usar el servidor especificado en el archivo de certificado. El servidor OCSP determina si la CA revocó algún certificado antes de su fecha de vencimiento programada y, a continuación, bloquea al usuario para que no acceda al sitio si se ha revocado el certificado.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. Seleccione la ficha **Trusted**.

   > También puede habilitar la comprobación de revocación en la ficha **Gestión de claves**.

3. Haga clic en **tareas no comunes** y seleccione **Activar comprobación de revocación** en el menú desplegable.
4. Seleccione **deseo habilitar la comprobación de revocación**, de modo que aparezca una Marca de verificación en la casilla de verificación y aparecerán campos adicionales en el cuadro de diálogo.
5. En el campo **Dirección de respondedor OCSP**, puede especificar opcionalmente una URL para un servidor de respuesta OCSP. Si no se especifica ninguna dirección, el sistema utiliza la URL del servidor OCSP incluida en el archivo de certificado.
6. Haga clic en **Dirección de prueba** para asegurarse de que el sistema pueda abrir una conexión a la URL especificada.
7. Haga clic en **Guardar**.

Resultados

Si la cabina de almacenamiento intenta conectarse a un servidor que posee un certificado revocado, la conexión se rechaza y se registra un evento.

Elimine certificados de confianza

Es posible eliminar los certificados instalados por el usuario que se importaron anteriormente desde la pestaña de confianza.

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 actualiza a una nueva versión de certificado de confianza, el certificado actualizado debe importarse antes de eliminar el anterior.

> Si elimina un certificado que se utiliza para autenticar las controladoras y otro servidor, como un servidor LDAP, antes de importar un certificado de reemplazo, puede perder el acceso al sistema.

Acerca de esta tarea

En esta tarea, se describe la manera de eliminar certificados instalados por el usuario. No se pueden eliminar los certificados autofirmados preinstalados.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. Seleccione la ficha **Trusted**.

   En la tabla, se muestran los certificados de confianza de la cabina de almacenamiento.

3. En la tabla, seleccione el certificado que desea eliminar.
4. Haga clic en **menú:tareas no comunes[Eliminar]**

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

5. Tipo `delete` En el campo y, a continuación, haga clic en **Eliminar**.

Use certificados firmados por CA para la autenticación con un servidor de gestión de claves

Para establecer comunicaciones seguras entre un servidor de gestión de claves y las controladoras de la cabina de almacenamiento, debe configurar los conjuntos de certificados adecuados.

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

La autenticación entre las controladoras y un servidor de gestión de claves es un procedimiento de dos pasos.

Paso 1: Complete y envíe una CSR para la autenticación con un servidor de gestión de claves

Primero, debe generar un archivo de solicitud de firma de certificación (CSR) y utilizar la CSR para solicitar un certificado de cliente firmado de una entidad de certificación (CA) que confía en el servidor de gestión de claves. También es posible crear y descargar un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado.

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 cómo generar el archivo CSR, el cual se utilizará para solicitar un certificado de cliente firmado de una CA de confianza en el servidor de gestión de claves. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP). Durante esta tarea, debe brindar información acerca de su organización.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Gestión de claves**, seleccione **completar CSR**.
3. Introduzca la siguiente información:
   - **Nombre común** — un nombre que identifica a esta CSR, como el nombre de la matriz de almacenamiento, que se mostrará en los archivos de certificado.

- **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 o localidad donde está ubicada su organización.
- **Estado/Región (opcional)** — el estado o región donde está ubicada su organización.
- **Código ISO de país** — el código ISO (Organización Internacional de Normalización) de dos dígitos, como US, en el que se encuentra su organización.

4. Haga clic en **Descargar**.

   Se guardará un archivo CSR en el sistema local.

5. Solicite un certificado de cliente firmado de una CA a la que confíe el servidor de gestión de claves.
6. Cuando tenga un certificado de cliente, vaya a. Paso 2: Importar certificados para el servidor de gestión de claves.

Paso 2: Importar certificados para el servidor de gestión de claves

Como paso siguiente, debe importar certificados para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Existen dos tipos de certificados: El certificado de cliente valida las controladoras de la cabina de almacenamiento, mientras que el certificado de servidor de gestión de claves valida al servidor.

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.
- Tiene un archivo de certificado de cliente firmado (consulte Paso 1: Complete y envíe una CSR para la autenticación con un servidor de gestión de claves), y copió ese archivo en el host donde se accede a System Manager. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP).
- Debe recuperar el archivo de certificado del servidor desde el servidor de gestión de claves y, a continuación, copiar ese archivo en el host donde se accede a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP.

> Si desea obtener más información sobre el certificado de servidor, consulte la documentación del servidor de gestión de claves.

Acerca de esta tarea

En esta tarea, se describe cómo cargar archivos de certificado para la autenticación entre las controladoras de la cabina de almacenamiento y el servidor de gestión de claves. Debe cargar tanto el archivo de certificado de cliente para las controladoras como el archivo de certificado de servidor para el servidor de gestión de claves.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Gestión de claves**, seleccione **Importar**.

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

3. Junto a **Seleccionar certificado de cliente**, haga clic en el botón **examinar** para seleccionar el archivo de certificado de cliente para los controladores de la matriz de almacenamiento.

   Se muestra el nombre del archivo en el cuadro de diálogo.

4. Junto a **Seleccionar certificado de servidor del servidor de administración de claves**, haga clic en el botón **examinar** para seleccionar el archivo de certificado de servidor del servidor de administración de claves.

   Se muestra el nombre del archivo en el cuadro de diálogo.

5. Haga clic en **Importar**.

   Los archivos se cargan y validan.

Exportar certificados del servidor de gestión de claves

Es posible guardar un certificado para un servidor de gestión de claves en una máquina 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 certificación.
- Los certificados deben haberse importado previamente.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. Seleccione la ficha **Gestión de claves**.
3. En la tabla, seleccione el certificado que desea exportar y, a continuación, haga clic en **Exportar**.

   Se abre el cuadro de diálogo Guardar.

4. Introduzca un nombre de archivo y haga clic en **Guardar**.

Preguntas frecuentes

¿Por qué se muestra el cuadro de diálogo no se puede acceder a otra controladora?

Cuando se realizan ciertas operaciones relacionadas con los certificados de CA (por ejemplo, la importación de un certificado), es posible que aparezca un cuadro de diálogo que le solicite aceptar un certificado autofirmado para la segunda controladora.

En las cabinas de almacenamiento con dos controladoras (configuraciones dúplex), este cuadro de diálogo aparece en ocasiones si System Manager de SANtricity no puede comunicarse con la segunda controladora, o bien si el explorador no puede aceptar el certificado durante un determinado punto en una operación.

Si se abre este cuadro de diálogo, haga clic en **Aceptar certificado autofirmado** para continuar. Si otro cuadro de diálogo le solicita una contraseña, introduzca la contraseña de administrador que utiliza para acceder a System Manager.

En caso de que este cuadro de diálogo se muestre nuevamente y no pueda completar una tarea de certificado, intente uno de los procedimientos a continuación:

- Utilice un tipo de explorador diferente para acceder a esta controladora, acepte el certificado y continúe.
- Acceda a la segunda controladora con System Manager, acepte el certificado autofirmado y luego regrese a la primera controladora y continúe.

¿Cómo saber qué certificados deben cargarse en System Manager para la gestión de claves externas?

Para la gestión de claves externas, debe importar dos tipos de certificados para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves, de forma tal que exista confianza mutua entre las dos entidades.

Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP). Para obtener un certificado de cliente, se usa System Manager para completar una CSR para la cabina de almacenamiento. Luego, puede cargar la CSR en un servidor de gestión de claves y generar un certificado de cliente a partir de ese punto. Una vez que tenga un certificado de cliente, copie ese archivo en el host donde acceda a System Manager.

Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Recupere el archivo de certificado de servidor del servidor de gestión de claves y copie ese archivo en el host donde va a acceder a System Manager.

¿Qué debo saber acerca de la comprobación de revocación de certificados?

System Manager permite verificar certificados revocados mediante un servidor de protocolo de estado de certificado en línea (OCSP), en lugar de cargar listas de revocación de certificados (CRL).

Los certificados revocados ya no deberán considerarse de confianza. Un certificado puede ser revocado por varios motivos; por ejemplo, si la entidad de certificación (CA) emitió el certificado incorrectamente, una clave privada quedó en riesgo o la entidad identificada no cumplió con los requisitos de la política.

Después de establecer una conexión con un servidor OCSP en System Manager, la cabina de almacenamiento realiza la verificación de revocación cada vez que se conecta a un servidor de AutoSupport, un servidor de gestión de claves externo (EKMS), un servidor de protocolo ligero de acceso a directorios por SSL (LDAPS) o un servidor de syslog. La cabina de almacenamiento intenta validar los certificados de tales servidores para asegurarse de que no se hayan revocado. A continuación, el servidor obtiene los valores "good", "revoked" o "unknown" para ese certificado. Si el certificado se revoca o la cabina no puede conectarse al servidor de OCSP, la conexión se rechaza.

> La especificación de una dirección de respuesta de OCSP en System Manager o en la interfaz de línea de comandos (CLI) anula la dirección de OCSP que se encontró en el archivo de certificado.

¿Para qué tipos de servidores se habilitará la comprobación de revocación?

La cabina de almacenamiento realiza la verificación de revocación cada vez que se conecta a un servidor AutoSupport, un servidor de gestión de claves externo (EKMS), un

servidor de protocolo ligero de acceso a directorios por SSL (LDAPS) o un servidor de syslog.