Usar certificados

SANtricity 11.8

NetApp
April 05, 2024

Tabla de contenidos

Usar certificados

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.
- Debe conocer la dirección IP o los nombres DNS de cada controladora.

Acerca de esta tarea

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

Paso 1: Completar los 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.

Acerca de esta tarea

En esta tarea, se describe cómo generar un archivo CSR desde System Manager. La CSR proporciona información sobre la organización y la dirección IP o el nombre DNS de la controladora. Durante esta tarea, se genera un archivo CSR si la cabina de almacenamiento tiene una controladora y dos archivos CSR si posee dos controladoras.

> También puede generar un archivo CSR con una herramienta como OpenSSL y puede saltar a. Paso 2: Envíe los archivos CSR.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. En la ficha Administración 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. El nombre DNS no puede comenzar con un comodín.
   - **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. El nombre DNS no puede comenzar con un comodín. 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. Vaya a. Paso 2: Envíe los archivos CSR.

Paso 2: Envíe los archivos CSR

Después de crear los archivos de solicitud de firma de certificación (CSR), envíe los archivos a una CA. Los sistemas E-Series requieren el formato PEM (codificación ASCII Base64) para certificados firmados, que incluye los siguientes tipos de archivo: pem, .crt, .cer o .key.

Pasos

1. Busque los archivos CSR descargados.
2. Envíe los archivos 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 firmados para las controladoras.

Paso 3: Importar certificados firmados para las controladoras

Después de recibir los certificados firmados de la entidad de certificación (CA), importe los archivos para las controladoras.

Antes de empezar

- La CA devolvió archivos de certificado firmados. Estos archivos incluyen el certificado raíz, uno o varios certificados intermedios y los certificados 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 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 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 accede a System Manager.

Pasos

1. Seleccionar menú:Configuración[certificados]
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 los archivos de certificado raíz e intermedio 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. 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**.

   Los archivos se cargan y validan.

Resultado

La sesión finaliza automáticamente. Debe volver a iniciar sesión para que los certificados entren en vigencia. Cuando inicia sesión nuevamente, se utilizan los nuevos certificados firmados 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 restablecimiento de certificados 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

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.

Pestaña	Descripción
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** — 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** — certificados autofirmados incluidos con la cabina de almacenamiento.
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. 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).

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. 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.

Antes de empezar

- 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 un archivo de certificado del servidor de gestión de claves y, a continuación, copiar ese archivo en el host donde va a acceder 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. Es posible usar un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.

> Si desea obtener más información sobre el certificado de servidor, consulte la documentación del 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. Es posible elegir un certificado raíz, intermedio o de servidor para el servidor de gestión 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**.