Gestionar certificados

E-Series Systems

NetApp
June 14, 2024

Tabla de contenidos

Gestionar certificados

Información general sobre certificados

La gestión de certificados en el complemento de almacenamiento para vCenter permite crear solicitudes de firma de certificados (CSR), importar certificados y gestionar certificados existentes.

¿Qué son los certificados?

Los certificados son archivos digitales que identifican entidades en línea, como sitios web y servidores, para poder establecer comunicaciones seguras en Internet. Garantizan que solo se transmitan comunicaciones web en formato cifrado, de forma privada y sin alternaciones, entre el servidor especificado y el cliente. Mediante el complemento de almacenamiento para vCenter, puede 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.

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 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 exploradores. 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.

Certificado de gestión

Al abrir el plugin, el explorador intenta verificar si el host de gestión es un origen de confianza mediante la comprobación de un certificado digital. Si el explorador no encuentra un certificado firmado por CA, abre un mensaje de advertencia. Desde allí, podrá continuar al sitio web para aceptar el certificado autofirmado en esa sesión. También es posible obtener certificados digitales firmados de una CA para que ya no se vea el mensaje de advertencia.

Certificados de confianza

Durante una sesión del plugin, 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 plugin pueda autenticar las solicitudes de cliente entrantes procedentes de estas controladoras.

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 el complemento de almacenamiento para vCenter.

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

- Paso 1: Complete un archivo CSR.
- Paso 2: Enviar archivo CSR.
- Paso 3: Importar certificados de gestión.

Paso 1: Complete un archivo CSR

Primero, debe generar un archivo de solicitud de firma de certificación (CSR), que identifica a la organización y al sistema host donde se ejecuta el plugin. 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 **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 donde se ejecuta el plugin:
   - **Nombre común** — la dirección IP o el nombre DNS del sistema host donde se ejecuta el plugin. Asegúrese de que esta dirección es correcta; debe coincidir exactamente con lo que escribe para acceder al plugin 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**.

Paso 2: Enviar archivo CSR

Después de crear un archivo de solicitud de firma de certificación (CSR), se envía el archivo CSR generado a una CA para recibir certificados de gestión firmados para el sistema donde se aloja el plugin.

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 se genera 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 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.

Paso 3: Importar certificados de gestión

Después de recibir certificados firmados de la entidad de certificación (CA), importe los certificados en el sistema host donde se instaló el plugin.

Antes de empezar

- Debe tener los 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. También puede usar la utilidad certmgr de Windows para desempaquetar los archivos (haga clic con el botón derecho y seleccione MENU:All Tasks[Export]). Se recomienda la codificación base-64. Una vez completadas las exportaciones, se mostrará un archivo CER para cada archivo de certificado de la cadena.
- Se deben copiar los archivos de certificado en el sistema host donde se ejecuta el plugin.

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**.

Resultado

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

Restablezca los certificados de gestión

Para el sistema de gestión que aloja el complemento de almacenamiento para vCenter, puede revertir el certificado de gestión a su estado autofirmado original de fábrica.

Acerca de esta tarea

Esta tarea elimina el certificado de gestión actual del sistema host donde se ejecuta el complemento de almacenamiento para vCenter. 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 de certificado de gestión.

3. Escriba reset en el campo y 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.

Resultado

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 el complemento de almacenamiento para vCenter. Los certificados pueden estar firmados por una entidad de certificación (CA) o ser autofirmados.

Antes de empezar

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.
4. 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.
5. 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).

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione una de las siguientes pestañas:
   - **Administración** — muestra el certificado para el sistema que aloja el plugin. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro al plugin.
   - **Trusted** — muestra certificados a los que el plugin 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 plugin. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro al plugin.
   - **Trusted** — muestra certificados a los que el plugin 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

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

Si tiene pensado importar un certificado firmado por una CA, asegúrese de que:

- 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

Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una conexión con el plugin, pero no se confirma que la conexión sea segura. 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 o 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.
4. 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.
5. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

   El certificado se carga y se valida.

Información de copyright

Información de la marca comercial