Certificados

SANtricity 11.5

NetApp
February 12, 2024

Tabla de contenidos

Certificados

Conceptos

Cómo funcionan los certificados de CA

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.

Cuando se abre un explorador y se intenta una conexión con System Manager a través del puerto de gestión de la controladora, el explorador intenta verificar si la controladora de la cabina de almacenamiento es un origen confiable. Si el explorador no puede localizar un certificado digital para la controladora, alerta que el certificado no está firmado por una autoridad reconocida y pregunta al usuario si desea continuar. Si ya no desea ver esta alerta, debe obtener un certificado digital firmado de una CA.

Si usa un servidor de gestión de claves externo con la función Drive Security, también puede crear certificados para la autenticación entre ese servidor y las controladoras, o puede aceptar los certificados autofirmados de la cabina de almacenamiento.

Debe seguir estos pasos para usar un certificado digital de una autoridad de confianza:

1. Vaya al menú:Configuración[certificados]. Su inicio de sesión de usuario debe incluir permisos de administración de seguridad; de lo contrario, **certificados** no aparecerá en la página.
2. Cree una solicitud de firma de certificación (CSR) para cada controladora o para un servidor de gestión de claves.
3. Envíe el o los archivos .CSR a una CA y espere que la autoridad envíe los certificados.
4. Importe los certificados de confianza (intermedio y raíz) de la CA. Estos certificados establecen un punto de confianza para una jerarquía de CA.
5. Importe los certificados de gestión firmados para cada controladora o el servidor de gestión de claves.

Terminología de certificados

Conozca la forma en que los términos de certificados se aplican a su cabina de almacenamiento.

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.

Duración	Descripción
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.
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 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.
Certificado de gestión	Una entidad de certificación (CA) aprueba un certificado de gestión para permitir el acceso seguro a la aplicación web. También se conoce como "certificado firmado".
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 autofirmado	Los certificados autofirmados se cargan de forma previa en las controladoras. Si la conexión de sitio es autofirmada, se abre un mensaje de advertencia antes de pasar a la aplicación web.
Certificado de confianza	Un certificado de confianza de una entidad de certificación (CA) es un certificado conocido ubicado en la parte superior de la jerarquía de certificados. También se conoce como "certificado raíz".

Procedimientos

Complete una solicitud de firma de certificación (CSR) de una CA para las controladoras

Para recibir un certificado de una entidad de certificación (CA) para las controladoras de la cabina de almacenamiento, primero se debe generar un archivo de solicitud de firma de certificación (CSR) para cada controladora de 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.

Acerca de esta tarea

En esta tarea, se describe cómo generar los archivos .CSR (solicitudes de firma de certificación) que se envían a una CA para recibir certificados de gestión firmados de las controladoras. Se debe proporcionar información sobre la organización, más la dirección IP o el nombre DNS de las controladoras. 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.

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. En el caso de controladoras dobles, se descargan dos archivos .CSR. La ubicación de la carpeta de la descarga depende del explorador.

6. Envíe el o los archivos .CSR a la CA.

Después de terminar

Cuando reciba los certificados digitales, importe los archivos de certificado adecuados que le envió la CA.

Importe certificados de confianza para las controladoras

Después de recibir certificados digitales de una entidad de certificación (CA), puede importar la cadena de certificados (intermedio y raíz) para las controladoras.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Generó una solicitud de firma de certificación (archivo .CSR) y la envió a la CA.
- La CA devolvió archivos de certificado de confianza.
- Los archivos de certificado están instalados en el sistema local.

Acerca de esta tarea

En esta tarea, se describe cómo cargar los certificados de confianza para las controladoras de la cabina de almacenamiento.

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.

Después de terminar

Importe el certificado de gestión.

Importe un certificado de gestión para controladoras

Después de importar la cadena de certificados de confianza, es posible importar un archivo de certificado de gestión (firmado) para cada controladora de 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.
- Se importaron los certificados de confianza.
- La CA devolvió un archivo de certificado de gestión para cada controladora.
- Los archivos de certificado de gestión están disponibles en el sistema local.

Acerca de esta tarea

En esta tarea, se describe cómo cargar archivos de certificado de gestión para la autenticación de la controladora.

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 **examinar** para seleccionar el archivo del controlador A. Si hay dos controladores, haga clic en el segundo botón **examinar** para seleccionar el archivo del controlador B.

   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.

Vea información de certificaciones importadas

Desde la página certificados, es posible ver el tipo de certificado, la entidad de certificación y el rango válido de fechas de certificados importados anteriormente.

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 ver información de certificados instalados por el usuario o instalados previamente.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. Seleccione una de las pestañas para ver información sobre certificados de gestión de controladoras, certificados de confianza y certificados de un servidor de gestión de claves.

Pestaña	Descripción
Gestión de cabinas	Permite ver información sobre todos los certificados de servidor importados de las controladoras.
De confianza	Permite ver información sobre todos los certificados de confianza (raíz) importados de 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 (incluyen certificados de confianza, certificados LDAPS y certificados de la Federación de identidades). • **Preinstalado**. Certificados incluidos en la cabina de almacenamiento.
Gestión de claves	Permite ver información sobre todos los certificados de gestión (firmados) importados para un servidor de gestión de claves externo.

Elimine certificados de confianza

Es posible eliminar cualquiera de los certificados importados por el usuario.

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.

Es posible que pierda acceso al sistema si elimina un certificado utilizado para autenticar los certificados de gestión de la cabina de almacenamiento o el servidor LDAP antes de importar un certificado de reemplazo.

Acerca de esta tarea

Esta tarea describe la manera de eliminar certificados importados por el usuario. Los certificados predefinidos no pueden eliminarse.

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**.

Restablezca los certificados de gestión

Es posible revertir los certificados de gestión en la cabina de almacenamiento a su estado autofirmado 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.
- Los certificados deben haberse importado previamente.

Acerca de esta tarea

Al restablecer los certificados de gestión en la cabina de almacenamiento, se eliminan los certificados de gestión actuales de cada una de las controladoras. Una vez restablecidos los certificados, se revierten las controladoras 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 haga clic en **Restablecer**.

Resultados

Una vez que se actualiza el explorador, se revierten las controladoras al uso de certificados autofirmados. Como resultado, el sistema solicita a los usuarios que acepten manualmente el certificado autofirmado para sus sesiones.

Completar una solicitud de firma de certificación (CSR) de CA para un servidor de claves

Para recibir un certificado de la entidad de certificación (CA) para un servidor de gestión de claves, primero se debe crear un archivo de solicitud de firma de certificación (CSR).

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 los archivos .CSR (solicitudes de firma de certificación) que se envían a una CA para recibir certificados firmados de un servidor de gestión de claves. 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 guarda un archivo .CSR en el sistema local.

5. Envíe el o los archivos .CSR a la CA.

Después de terminar

Cuando obtenga los certificados de cliente y servidor del servidor de gestión de claves, impórtelos para su autenticación con las controladoras de la cabina de almacenamiento.

Importe los certificados del servidor de gestión de claves

Para la gestión de claves externas, debe importar 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. Existen dos tipos de certificados: El certificado de cliente valida a las controladoras, 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.
- Hay un certificado de cliente disponible para la cabina de almacenamiento.

> Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus direcciones IP. Para obtener un certificado de cliente, debe completar una CSR para la cabina de almacenamiento y luego cargarlo al servidor de gestión de claves. Desde el servidor, genere un certificado de cliente.

- El certificado de servidor de gestión de claves está disponible.

Un certificado de servidor de gestión de claves valida el servidor para que la cabina de almacenamiento pueda confiar en su dirección IP. Para obtener un certificado de servidor de gestión de claves, debe generarlo en el 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.

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. Haga clic en los botones **examinar** para seleccionar los archivos.

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

4. 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**.

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

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

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 es posible habilitar la comprobación de revocación en la pestaña 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**.

Resultado

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

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, 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 direcciones IP. Para obtener un certificado de cliente, debe completar una CSR para la cabina de almacenamiento y luego cargarlo al servidor de gestión de claves. Desde el servidor, genere un certificado de cliente y luego use System Manager para importarlo.

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. Para obtener un certificado de servidor de gestión de claves, debe generarlo en el servidor de gestión de claves.

¿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.