



Gestionar certificados

StorageGRID software

NetApp

February 12, 2026

Tabla de contenidos

- Gestionar certificados 1
 - Gestionar certificados de seguridad 1
 - Acceda a los certificados de seguridad 2
 - Detalles del certificado de seguridad 5
 - Ejemplos de certificados 11
 - Tipos de certificado de servidor admitidos 12
 - Configure los certificados de interfaz de gestión 12
 - Añada un certificado de interfaz de gestión personalizado 13
 - Restaurar el certificado de interfaz de gestión predeterminado 16
 - Use un script para generar un nuevo certificado de interfaz de gestión autofirmado 16
 - Descargue o copie el certificado de la interfaz de gestión 17
 - Configure los certificados de API S3 18
 - Agregue un certificado API S3 personalizado 19
 - Restaurar el certificado API S3 predeterminado 22
 - Descargue o copie el certificado API S3 22
 - Copie el certificado de la CA de cuadrícula 23
 - Configure los certificados StorageGRID para FabricPool 24
 - Configurar certificados de cliente 25
 - Añada certificados de cliente 26
 - Editar certificados de cliente 29
 - Adjunte un nuevo certificado de cliente 29
 - Descargar o copiar certificados de cliente 32
 - Quite certificados de cliente 33

Gestionar certificados

Gestionar certificados de seguridad

Los certificados de seguridad son archivos de datos pequeños que se utilizan para crear conexiones seguras y de confianza entre componentes de StorageGRID y entre componentes de StorageGRID y sistemas externos.

StorageGRID utiliza dos tipos de certificados de seguridad:

- **Se requieren certificados de servidor** cuando se utilizan conexiones HTTPS. Los certificados de servidor se utilizan para establecer conexiones seguras entre clientes y servidores, autenticar la identidad de un servidor a sus clientes y proporcionar una ruta de comunicación segura para los datos. Cada servidor y el cliente tienen una copia del certificado.
- **Los certificados de cliente** autentican una identidad de cliente o usuario al servidor, proporcionando una autenticación más segura que las contraseñas solamente. Los certificados de cliente no cifran datos.

Cuando un cliente se conecta al servidor mediante HTTPS, el servidor responde con el certificado del servidor, que contiene una clave pública. El cliente compara la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión con el servidor utilizando la misma clave pública.

StorageGRID funciona como servidor para algunas conexiones (como el extremo de equilibrio de carga) o como cliente para otras conexiones (como el servicio de replicación de CloudMirror).

Certificado de CA de cuadrícula predeterminado

StorageGRID tiene una autoridad de certificación (CA) incorporada que genera un certificado CA de Grid interno durante la instalación del sistema. El certificado CA de Grid se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una autoridad de certificación (CA) externa puede emitir certificados personalizados que cumplan totalmente con las políticas de seguridad de la información de su organización.

Utilice el certificado CA de Grid para entornos que no sean de producción. Para la producción, utilice certificados personalizados firmados por una autoridad de certificación externa. Se admiten conexiones no seguras sin certificado, pero no se recomiendan.

- Los certificados de CA personalizados no eliminan los certificados internos; sin embargo, los certificados personalizados deben ser los especificados para verificar las conexiones del servidor.
- Todos los certificados personalizados deben cumplir con el ["directrices de fortalecimiento del sistema para los certificados de servidor"](#).
- StorageGRID admite la agrupación de certificados de una CA en un único archivo (conocido como paquete de certificados de CA).



StorageGRID también incluye certificados de CA del sistema operativo que son los mismos en todos los entornos Grid. En los entornos de producción, asegúrese de especificar un certificado personalizado firmado por una entidad de certificación externa en lugar del certificado de CA del sistema operativo.

Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Es necesario tener preparados todos los certificados necesarios para la configuración específica de StorageGRID antes de configurar el sistema.

Acceda a los certificados de seguridad

Puede acceder a información sobre todos los certificados de StorageGRID en una única ubicación, junto con enlaces al flujo de trabajo de configuración de cada certificado.

Pasos

1. Desde Grid Manager, seleccione **Configuración > Seguridad > Certificados**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

[Global](#) [Grid CA](#) [Client](#) [Load balancer endpoints](#) [Tenants](#) [Other](#)

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ?	Expiration date ? ↕
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Seleccione una ficha en la página certificados para obtener información sobre cada categoría de certificado y para acceder a la configuración de certificado. Puede acceder a una pestaña si tiene el "permiso apropiado".
 - **Global:** Protege el acceso a StorageGRID desde navegadores web y clientes API externos.
 - **Grid CA:** Protege el tráfico interno de StorageGRID.
 - **Cliente:** Protege las conexiones entre clientes externos y la base de datos Prometheus de StorageGRID.
 - **Puntos Finales de Equilibrador de Carga:** Asegura las conexiones entre los clientes S3 y el Equilibrador de Carga StorageGRID.
 - **Arrendatarios:** Protege las conexiones a servidores de federación de identidades o desde extremos de servicio de plataforma a recursos de almacenamiento S3.
 - **Otros:** Protege las conexiones StorageGRID que requieren certificados específicos.

Cada una de las pestañas se describe a continuación con enlaces a detalles de certificados adicionales.

Global

Los certificados globales protegen el acceso a StorageGRID desde exploradores web y clientes API S3 externos. La autoridad de certificados StorageGRID genera inicialmente dos certificados globales durante la instalación. La práctica recomendada para un entorno de producción es usar certificados personalizados firmados por una entidad de certificación externa.

- [Certificado de interfaz de gestión](#): Protege las conexiones del navegador web del cliente a las interfaces de administración de StorageGRID.
- [Certificado API S3](#): Protege las conexiones de API del cliente a los nodos de almacenamiento, nodos de administración y nodos de gateway, que las aplicaciones cliente S3 utilizan para cargar y descargar datos de objetos.

Entre la información sobre los certificados globales instalados se incluyen:

- **Nombre**: Nombre del certificado con enlace a la administración del certificado.
- **Descripción**
- **Tipo**: Personalizado o predeterminado. + debe usar siempre un certificado personalizado para mejorar la seguridad de la cuadrícula.
- **Fecha de vencimiento**: Si se utiliza el certificado predeterminado, no se muestra ninguna fecha de vencimiento.

Podrá:

- Sustituya los certificados predeterminados por certificados personalizados firmados por una autoridad de certificado externa para mejorar la seguridad de la cuadrícula:
 - ["Reemplace el certificado de interfaz de gestión generado por StorageGRID predeterminado"](#)
Se utiliza para las conexiones de Grid Manager y de Tenant Manager.
 - ["Reemplace el certificado API S3"](#) Se utiliza para las conexiones de extremo del balanceador de carga y del nodo de almacenamiento (opcional).
- ["Restaure el certificado de interfaz de gestión predeterminado"](#).
- ["Restaure el certificado API S3 predeterminado"](#).
- ["Use un script para generar un nuevo certificado de interfaz de gestión autofirmado"](#).
- Copie o descargue el ["certificado de interfaz de gestión"](#) o ["Certificado API S3"](#).

CA de grid

El [Certificado de CA de grid](#), generado por la autoridad de certificación de StorageGRID durante la instalación de StorageGRID, protege todo el tráfico interno de StorageGRID.

La información del certificado incluye la fecha de caducidad del certificado y el contenido del mismo.

Puedes ["Copie o descargue el certificado de Grid CA"](#), pero no puedes cambiarlo.

Cliente

[Certificados de cliente](#), Generado por una autoridad de certificación externa, asegure las conexiones entre las herramientas de monitoreo externo y la base de datos de StorageGRID Prometheus.

La tabla de certificados tiene una fila para cada certificado de cliente configurado e indica si el certificado se puede utilizar para el acceso a la base de datos Prometheus, junto con la fecha de caducidad del certificado.

Podrá:

- "Cargar o generar un nuevo certificado de cliente."
- Seleccione un nombre de certificado para mostrar los detalles del certificado, donde podrá:
 - "Cambie el nombre del certificado de cliente."
 - "Establezca el permiso de acceso Prometheus."
 - "Cargue y reemplace el certificado de cliente."
 - "Copie o descargue el certificado de cliente."
 - "Quite el certificado de cliente."
- Seleccione **Acciones** para rápidamente "editar", "asociar" o "quitar" un certificado de cliente. Puede seleccionar hasta 10 certificados de cliente y eliminarlos a la vez utilizando **acciones** > **Quitar**.

Puntos finales del equilibrador de carga

[Certificados de punto final de equilibrador de carga](#) Proteja las conexiones entre los clientes S3 y el servicio de equilibrador de carga de StorageGRID en los nodos de la puerta de enlace y los nodos de administración.

La tabla de puntos finales de equilibrio de carga tiene una fila para cada punto final de equilibrio de carga configurado e indica si se está utilizando el certificado de API global S3 o un certificado de punto final de equilibrio de carga personalizado para el punto final. También se muestra la fecha de caducidad de cada certificado.



Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Podrá:

- "Ver un punto final de equilibrio de carga", incluyendo sus detalles de certificado.
- "Especifique un certificado de extremo de equilibrio de carga para FabricPool."
- "Utilice el certificado API global S3" en lugar de generar un nuevo certificado de punto final del equilibrador de carga.

Clientes

Los inquilinos pueden usar [certificados de servidor de federación de identidades](#) o [certificados de extremo de servicio de plataforma](#) para proteger sus conexiones con StorageGRID.

La tabla de arrendatarios tiene una fila para cada arrendatario e indica si cada arrendatario tiene permiso para utilizar su propio origen de identidad o servicios de plataforma.

Podrá:

- "Seleccione un nombre de inquilino para iniciar sesión en el Administrador de inquilinos"
- "Seleccione un nombre de inquilino para ver los detalles de la federación de identidades del inquilino"
- "Seleccione el nombre de un inquilino para ver los detalles de los servicios de la plataforma de inquilino"
- "Especifique un certificado de extremo de servicio de plataforma durante la creación del extremo"

Otros

StorageGRID utiliza otros certificados de seguridad con fines específicos. Estos certificados se enumeran por su nombre funcional. Otros certificados de seguridad incluyen:

- [Certificados de Cloud Storage Pool](#)
- [Certificados de notificación de alertas por correo electrónico](#)
- [Certificados de servidor de syslog externos](#)
- [Certificados de conexión de federación de grid](#)
- [Certificados de federación de identidades](#)
- [Certificados de servidor de gestión de claves \(KMS\)](#)
- [Certificados de inicio de sesión único](#)

La información indica el tipo de certificado que una función utiliza y sus fechas de vencimiento del certificado de servidor y cliente, según corresponda. Al seleccionar un nombre de función, se abre una pestaña del navegador en la que puede ver y editar los detalles del certificado.



Solo puede ver y acceder a la información de otros certificados si tiene el ["permiso apropiado"](#).

Podrá:

- ["Especifique un certificado de Cloud Storage Pool para S3, C2S S3 o Azure"](#)
- ["Especifique un certificado para notificaciones de alertas por correo electrónico"](#)
- ["Use un certificado para un servidor de syslog externo"](#)
- ["Rotar certificados de conexión de federación de cuadrícula"](#)
- ["Ver y editar un certificado de federación de identidades"](#)
- ["Cargar certificados de servidor de gestión de claves \(KMS\) y de cliente"](#)
- ["Especifique manualmente un certificado SSO para una confianza de parte de confianza"](#)

Detalles del certificado de seguridad

Cada tipo de certificado de seguridad se describe a continuación, con enlaces a las instrucciones de implementación.

Certificado de interfaz de gestión

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	<p>Autentica la conexión entre los exploradores web del cliente y la interfaz de gestión de StorageGRID, lo que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin advertencias de seguridad.</p> <p>Este certificado también autentica las conexiones API de gestión de grid y API de gestión de inquilinos.</p> <p>Puede usar el certificado predeterminado creado durante la instalación o cargar un certificado personalizado.</p>	Configuración > Seguridad > Certificados , seleccione la pestaña Global y luego seleccione Certificado de interfaz de administración	"Configure los certificados de interfaz de gestión"

Certificado API S3

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica las conexiones de clientes S3 seguras a un nodo de almacenamiento y a los extremos del balanceador de carga (opcional).	Configuración > Seguridad > Certificados , seleccione la pestaña Global y luego seleccione Certificado API S3	"Configure los certificados de API S3"

Certificado de CA de grid

Consulte la [Descripción de certificado de CA de cuadrícula predeterminada](#).

Certificado de cliente de administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	<p>Instalado en cada cliente, lo que permite que StorageGRID autentique el acceso de los clientes externos.</p> <ul style="list-style-type: none"> • Permite a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID. • Permite una supervisión segura de StorageGRID mediante herramientas externas. 	<p>Configuración > Seguridad > Certificados y luego seleccione la pestaña Cliente</p>	<p>"Configurar certificados de cliente"</p>

Certificado de punto final de equilibrador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	<p>Autentica la conexión entre clientes S3 y el servicio de equilibrador de carga de StorageGRID en los nodos de puerta de enlace y los nodos de administración. Puede cargar o generar un certificado de equilibrador de carga al configurar un extremo de equilibrador de carga. Las aplicaciones cliente utilizan el certificado de equilibrador de carga al conectarse a StorageGRID para guardar y recuperar datos de objeto.</p> <p>También puede usar una versión personalizada del certificado global Certificado API S3 para autenticar las conexiones al servicio de Equilibrador de Carga. Si el certificado global se utiliza para autenticar las conexiones del equilibrador de carga, no es necesario cargar ni generar un certificado independiente para cada punto final del equilibrador de carga.</p> <p>Nota: el certificado utilizado para la autenticación del equilibrador de carga es el certificado más utilizado durante el funcionamiento normal de StorageGRID.</p>	Configuración > Red > Puntos finales del balanceador de carga	<ul style="list-style-type: none"> • "Configurar puntos finales del equilibrador de carga" • "Cree un extremo de equilibrador de carga para FabricPool"

Certificado de extremo de Cloud Storage Pool

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión de un pool de almacenamiento en cloud de StorageGRID a una ubicación de almacenamiento externa, como S3 Glacier o el almacenamiento blob de Microsoft Azure. Se necesita un certificado diferente para cada tipo de proveedor de cloud.	ILM > piscinas de almacenamiento	" Cree un pool de almacenamiento en el cloud "

Certificado de notificación de alertas por correo electrónico

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	<p>Autentica la conexión entre un servidor de correo electrónico SMTP y una StorageGRID que se usa para notificaciones de alerta.</p> <ul style="list-style-type: none"> • Si las comunicaciones con el servidor SMTP requieren Transport Layer Security (TLS), debe especificar el certificado de CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo SMTP requiere certificados de cliente para la autenticación. 	Alertas > Configuración de correo electrónico	" Configure notificaciones por correo electrónico para las alertas "

Certificado de servidor de syslog externo

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	<p>Autentica la conexión TLS o RELP/TLS entre un servidor syslog externo que registra eventos en StorageGRID.</p> <p>Nota: no se requiere un certificado de servidor syslog externo para conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.</p>	Configuración > Monitoreo > Servidor de auditoría y syslog	"Use un servidor de syslog externo"

Certificado de conexión de la federación de cuadrícula

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autenticar y cifrar la información enviada entre el sistema de StorageGRID actual y otro grid en una conexión de federación de grid.	Configuración > Sistema > Federación de red	<ul style="list-style-type: none"> • "Crear conexiones de federación de grid" • "Rotar certificados de conexión"

Certificado de federación de identidades

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre StorageGRID y un proveedor de identidades externo, como Active Directory, OpenLDAP u Oracle Directory Server. Se utiliza para la federación de identidades, lo que permite que los grupos de administración y los usuarios sean gestionados por un sistema externo.	Configuración > Control de acceso > Federación de identidades	"Usar la federación de identidades"

Certificado de servidor de gestión de claves (KMS)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor de gestión de claves (KMS) externo, que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID.	Configuración > Seguridad > Servidor de administración de claves	"Añadir servidor de gestión de claves (KMS)"

Certificado de extremo de servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde el servicio de plataforma StorageGRID a un recurso de almacenamiento S3.	Administrador de inquilinos > ALMACENAMIENTO (S3) > terminales de servicios de plataforma	"Cree un extremo de servicios de plataforma" "Editar extremo de servicios de plataforma"

Certificado de inicio de sesión único (SSO)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los servicios de federación de identidades, como Active Directory Federation Services (AD FS), y StorageGRID, que se utilizan para solicitudes de inicio de sesión único (SSO).	Configuración > Control de acceso > Inicio de sesión único	"Configurar el inicio de sesión único"

Ejemplos de certificados

Ejemplo 1: Servicio de equilibrador de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Se configura un extremo de equilibrador de carga y se carga o genera un certificado de servidor en StorageGRID.
2. Debe configurar una conexión de cliente S3 al extremo del equilibrador de carga y cargar el mismo certificado al cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al extremo de equilibrio de carga mediante

HTTPS.

4. StorageGRID responde con el certificado de servidor, que contiene una clave pública y una firma basada en la clave privada.
5. El cliente compara la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión utilizando la misma clave pública.
6. El cliente envía datos de objeto a StorageGRID.

Ejemplo 2: Servidor de gestión de claves externo (KMS)

En este ejemplo, StorageGRID actúa como cliente.

1. Con el software de servidor de gestión de claves externo, configura StorageGRID como un cliente KMS y obtiene un certificado de servidor firmado por CA, un certificado de cliente público y la clave privada del certificado de cliente.
2. Con el Administrador de grid, configura un servidor KMS y carga los certificados de servidor y cliente y la clave privada de cliente.
3. Cuando un nodo StorageGRID necesita una clave de cifrado, realiza una solicitud al servidor KMS que incluye datos del certificado y una firma basada en la clave privada.
4. El servidor KMS valida la firma del certificado y decide que puede confiar en StorageGRID.
5. El servidor KMS responde mediante la conexión validada.

Tipos de certificado de servidor admitidos

El sistema StorageGRID admite certificados personalizados cifrados con RSA o ECDSA (algoritmo de firma digital de curva elíptica).



El tipo de cifrado de la política de seguridad debe coincidir con el tipo de certificado del servidor. Por ejemplo, los cifrados RSA requieren certificados RSA y los cifrados ECDSA requieren certificados ECDSA. Consulte "[Gestionar certificados de seguridad](#)". Si configura una política de seguridad personalizada que no es compatible con el certificado del servidor, puede "[vuelva temporalmente a la política de seguridad predeterminada](#)".

Para obtener más información sobre cómo StorageGRID protege las conexiones de cliente, consulte "[Seguridad para clientes S3](#)".

Configure los certificados de interfaz de gestión

Puede reemplazar el certificado de interfaz de gestión predeterminado por un único certificado personalizado que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin tener que encontrar advertencias de seguridad. También puede revertir al certificado de interfaz de gestión predeterminado o generar una nueva.

Acerca de esta tarea

De manera predeterminada, cada nodo del administrador se envía un certificado firmado por la CA de grid. Estos certificados firmados por CA pueden sustituirse por una sola clave privada correspondiente y un certificado de interfaz de gestión personalizado común.

Dado que se utiliza un único certificado de interfaz de gestión personalizado para todos los nodos de

administración, debe especificar el certificado como un comodín o certificado de varios dominios si los clientes necesitan verificar el nombre de host al conectarse a Grid Manager y al Gestor de inquilinos. Defina el certificado personalizado de modo que coincida con todos los nodos de administrador de la cuadrícula.

Debe completar la configuración en el servidor y, en función de la entidad emisora de certificados raíz (CA) que esté utilizando, los usuarios también pueden necesitar instalar el certificado de la CA de cuadrícula en el explorador Web que utilizarán para acceder a Grid Manager y al gestor de inquilinos.



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración del certificado de servidor para la interfaz de administración** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **Configuración > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado de la interfaz de administración en la pestaña Global.



Si accede a Grid Manager o a Intenant Manager utilizando un nombre de dominio en lugar de una dirección IP, el explorador mostrará un error de certificado sin una opción para omitir si se produce alguna de las siguientes situaciones:

- El certificado de la interfaz de gestión personalizada caduca.
- Usted [revertir de un certificado de interfaz de gestión personalizado al certificado de servidor predeterminado](#).

Añada un certificado de interfaz de gestión personalizado

Para agregar un certificado de interfaz de gestión personalizado, puede proporcionar su propio certificado o generar uno mediante el Gestor de cuadrícula.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor:** El archivo de certificado de servidor personalizado (codificado con PEM).
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado (.key).



Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

- **Paquete CA:** Un único archivo opcional que contiene los certificados de cada entidad emisora de certificados intermedia (CA). El archivo debe contener cada uno de los archivos de certificado de CA codificados con PEM, concatenados en el orden de la cadena de certificados.

c. Expanda **Detalles del certificado** para ver los metadatos de cada certificado que haya cargado. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem.

Por ejemplo: storagegrid_certificate.pem

- Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

d. Seleccione **Guardar**. + el certificado de interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a la API de Grid Manager, de arrendatario Manager, de Grid Manager o de arrendatario Manager.

Generar certificado

Genere los archivos de certificado de servidor.



La práctica recomendada para un entorno de producción es usar un certificado de interfaz de gestión personalizado firmado por una entidad de certificación externa.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.

Campo	Descripción
IP	Una o más direcciones IP que se incluirán en el certificado.
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

- Seleccione **Descargar certificado** para guardar el archivo de certificado.

Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

e. Seleccione **Guardar**. + el certificado de interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a la API de Grid Manager, de arrendatario Manager, de Grid Manager o de arrendatario Manager.

5. Actualice la página para garantizar que se actualice el explorador web.



Tras cargar o generar un nuevo certificado, permita que se borren las alertas de caducidad de los certificados relacionados.

6. Después de añadir un certificado de interfaz de gestión personalizado, la página de certificado de interfaz de gestión muestra información detallada sobre certificados que están en uso. + puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado de interfaz de gestión predeterminado

Puede volver a utilizar el certificado de interfaz de gestión predeterminado para las conexiones de Grid Manager y de arrendatario Manager.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **utilizar certificado predeterminado**.

Cuando restaura el certificado de interfaz de gestión predeterminado, los archivos de certificado del servidor personalizados que configuró se eliminan y no pueden recuperarse del sistema. El certificado de la interfaz de gestión predeterminado se utiliza para todas las conexiones de clientes nuevas subsiguientes.

4. Actualice la página para garantizar que se actualice el explorador web.

Use un script para generar un nuevo certificado de interfaz de gestión autofirmado

Si se requiere una validación estricta del nombre de host, puede usar un script para generar el certificado de la interfaz de gestión.

Antes de empezar

- Tienes "[permisos de acceso específicos](#)".
- Tiene el `Passwords.txt` archivo.

Acerca de esta tarea

La práctica recomendada para un entorno de producción es usar un certificado firmado por una entidad de certificación externa.

Pasos

1. Obtenga el nombre de dominio completo (FQDN) de cada nodo de administrador.
2. Inicie sesión en el nodo de administración principal:
 - a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a raíz: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Al iniciar sesión como root, la petición de datos cambia de \$ a #.

3. Configure StorageGRID con un certificado autofirmado nuevo.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Para `--domains`, utilice comodines para representar los nombres de dominio completos de todos los nodos de administración. Por ejemplo, `*.ui.storagegrid.example.com` utiliza el comodín `*` para representar `admin1.ui.storagegrid.example.com` y `admin2.ui.storagegrid.example.com`.

- Establezca esta opción `--type management` para configurar el certificado de interfaz de gestión, que utiliza Grid Manager y Tenant Manager.
- De forma predeterminada, los certificados generados son válidos durante un año (365 días) y deben volver a crearse antes de que expiren. Puede utilizar `--days` el argumento para sustituir el período de validez por defecto.



El período de validez de un certificado comienza cuando `make-certificate` se ejecuta. Debe asegurarse de que el cliente de gestión esté sincronizado con el mismo origen de hora que StorageGRID; de lo contrario, el cliente podría rechazar el certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
```

El resultado contiene el certificado público que necesita el cliente API de gestión.

4. Seleccione y copie el certificado.

Incluya las etiquetas INICIAL Y FINAL en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`

6. Confirme que se configuró el certificado:

- Acceda a Grid Manager.
- Seleccione **Configuración > Seguridad > Certificados**
- En la ficha **Global**, seleccione **Certificado de interfaz de administración**.

7. Configure el cliente de administración para que utilice el certificado público que ha copiado. Incluya las etiquetas INICIAL Y FINAL.

Descargue o copie el certificado de la interfaz de gestión

Puede guardar o copiar el contenido del certificado de la interfaz de administración para utilizarlo en otro lugar.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

Descargue el certificado o el archivo del bundle de CA .pem. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

Si está descargando un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se descargan como un solo archivo.

b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

Copie el texto del certificado que se va a pegar en otro lugar. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM**.

Si va a copiar un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se copian al mismo tiempo.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Configure los certificados de API S3

Es posible reemplazar o restaurar el certificado de servidor que se utiliza para las conexiones de cliente S3 a los nodos de almacenamiento o para extremos de equilibrador de carga. El certificado de servidor personalizado de reemplazo es específico de su organización.



Se han eliminado los detalles de Swift de esta versión del sitio del documento. Consulte ["StorageGRID 11,8: Configure los certificados de API S3 y Swift"](#).

Acerca de esta tarea

De forma predeterminada, cada nodo de almacenamiento recibe un certificado de servidor X.509 firmado por la CA de grid. Estos certificados firmados por CA pueden sustituirse por un solo certificado de servidor personalizado común y una clave privada correspondiente.

Un único certificado de servidor personalizado se usa para todos los nodos de almacenamiento, por lo que debe especificar el certificado como comodín o certificado de varios dominios si los clientes necesitan verificar el nombre de host al conectarse al extremo de almacenamiento. Defina el certificado personalizado de forma que coincida con todos los nodos de almacenamiento de la cuadrícula.

Después de completar la configuración en el servidor, es posible que también necesite instalar el certificado de Grid CA en el cliente API S3 que utilizará para acceder al sistema, según la autoridad de certificación (CA) raíz que esté utilizando.



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor global para la API S3** se activa cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **Configuración > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado de API S3 en la pestaña Global.

Puede cargar o generar un certificado API personalizado de S3.

Agregue un certificado API S3 personalizado

Pasos

1. Seleccione **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **S3 certificado API**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor:** El archivo de certificado de servidor personalizado (codificado con PEM).
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado (.key).



Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

- **Paquete CA:** Un único archivo opcional que contiene los certificados de cada autoridad de certificación de emisión intermedia. El archivo debe contener cada uno de los archivos de certificado de CA codificados con PEM, concatenados en el orden de la cadena de certificados.

c. Seleccione los detalles del certificado para mostrar los metadatos y el PEM de cada certificado de API S3 personalizado que se cargó. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem.

Por ejemplo: storagegrid_certificate.pem

- Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

d. Seleccione **Guardar**.

El certificado de servidor personalizado se utiliza para las nuevas conexiones de cliente S3 posteriores.

Generar certificado

Genere los archivos de certificado de servidor.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.

Campo	Descripción
IP	Una o más direcciones IP que se incluirán en el certificado.
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado** para mostrar los metadatos y PEM para el certificado API S3 personalizado que se generó.

- Seleccione **Descargar certificado** para guardar el archivo de certificado.

Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

e. Seleccione **Guardar**.

El certificado de servidor personalizado se utiliza para las nuevas conexiones de cliente S3 posteriores.

5. Seleccione una pestaña para mostrar los metadatos del certificado de servidor StorageGRID predeterminado, un certificado firmado de una CA que se cargó o un certificado personalizado generado.



Tras cargar o generar un nuevo certificado, permita que se borren las alertas de caducidad de los certificados relacionados.

6. Actualice la página para garantizar que se actualice el explorador web.

7. Después de añadir un certificado de API S3 personalizado, la página de certificado de API S3 muestra

información de certificados detallada para el certificado de API S3 personalizado que está en uso. + puede descargar o copiar el certificado PEM según sea necesario.

Restaura el certificado API S3 predeterminado

Se puede revertir a utilizar el certificado de API S3 predeterminado para conexiones de cliente S3 a los nodos de almacenamiento. Sin embargo, no puede usar el certificado de API S3 predeterminado para un punto final de equilibrio de carga.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **S3 certificado API**.
3. Seleccione **utilizar certificado predeterminado**.

Cuando restaura la versión predeterminada del certificado de API global S3, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado de API S3 predeterminado se utilizará para las siguientes conexiones de cliente nuevos S3 a nodos de almacenamiento.

4. Seleccione **OK** para confirmar la advertencia y restaurar el certificado API S3 predeterminado.

Si tiene permiso de acceso raíz y se ha utilizado el certificado de API S3 personalizado para las conexiones de punto final del equilibrador de carga, se muestra una lista de puntos finales del equilibrador de carga a los que ya no se podrá acceder utilizando el certificado de API S3 predeterminado. Vaya a ["Configurar puntos finales del equilibrador de carga"](#) para editar o eliminar los puntos finales afectados.

5. Actualice la página para garantizar que se actualice el explorador web.

Descargue o copie el certificado API S3

Puede guardar o copiar el contenido del certificado API de S3 para utilizarlo en cualquier otro lugar.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **S3 certificado API**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

Descargue el certificado o el archivo del bundle de CA .pem. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

Si está descargando un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se descargan como un solo archivo.

b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

Copie el texto del certificado que se va a pegar en otro lugar. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM**.

Si va a copiar un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se copian al mismo tiempo.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Información relacionada

- ["USE LA API DE REST DE S3"](#)
- ["Configure los nombres de dominio de punto final S3"](#)

Copie el certificado de la CA de cuadrícula

StorageGRID utiliza una entidad de certificación (CA) interna para proteger el tráfico interno. Este certificado no cambia si carga sus propios certificados.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).

Acerca de esta tarea

Si se ha configurado un certificado de servidor personalizado, las aplicaciones cliente deben verificar el servidor mediante el certificado de servidor personalizado. No deben copiar el certificado de CA desde el sistema StorageGRID.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Grid CA**.
2. En la sección **Certificado PEM**, descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el archivo de certificado .pem.

- a. Seleccione **Descargar certificado**.
- b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem.

Por ejemplo: storagegrid_certificate.pem

PEM de certificado de copia

Copie el texto del certificado que se va a pegar en otro lugar.

- a. Seleccione **Copiar certificado PEM**.
- b. Pegue el certificado copiado en un editor de texto.
- c. Guarde el archivo de texto con la extensión .pem.

Por ejemplo: storagegrid_certificate.pem

Configure los certificados StorageGRID para FabricPool

Para los clientes S3 que realizan una validación estricta del nombre de host y no admiten la desactivación de la validación estricta del nombre de host, como los clientes ONTAP que usan FabricPool, puede generar o cargar un certificado de servidor al configurar el punto final del equilibrador de carga.

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).

Acerca de esta tarea

Al crear un extremo de equilibrador de carga, se puede generar un certificado de servidor autofirmado o cargar un certificado firmado por una entidad de certificación (CA) conocida. En los entornos de producción, se debe utilizar un certificado firmado por una CA conocida. Los certificados firmados por una CA se pueden rotar de forma no disruptiva. También son más seguros porque ofrecen una mejor protección contra los ataques de tipo "hombre en el medio".

En los siguientes pasos, se ofrecen directrices generales para clientes S3 que usan FabricPool. Para obtener más información y procedimientos, consulte ["Configure StorageGRID para FabricPool"](#).

Pasos

1. Opcionalmente, configure un grupo de alta disponibilidad (ha) para que lo utilice FabricPool.
2. Cree un extremo de equilibrador de carga de S3 para que se utilice FabricPool.

Cuando crea un extremo de equilibrio de carga HTTPS, se le solicita que cargue el certificado de servidor, la clave privada de certificado y el paquete de CA opcional.

3. Adjuntar StorageGRID como nivel de cloud en ONTAP.

Especifique el puerto de extremo de equilibrio de carga y el nombre de dominio completo utilizado en el certificado de CA que ha cargado. A continuación, proporcione el certificado de CA.



Si una CA intermedia emitió el certificado StorageGRID, debe proporcionar el certificado de CA intermedio. Si la CA raíz emitió directamente el certificado StorageGRID, debe proporcionar el certificado de CA raíz.

Configurar certificados de cliente

Los certificados de cliente permiten a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID, lo que proporciona una forma segura de que las herramientas externas supervisen StorageGRID.

Si necesita acceder a StorageGRID mediante una herramienta de supervisión externa, debe cargar o generar un certificado de cliente mediante el Gestor de cuadrícula y copiar la información de certificado a la herramienta externa.

Consulte ["Gestionar certificados de seguridad"](#) y ["Configurar certificados de servidor personalizados"](#).



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración de certificados de cliente configurados en la página Certificados** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **Configuración > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado del cliente en la pestaña Cliente.



Si utiliza un servidor de gestión de claves (KMS) para proteger los datos en nodos de dispositivos especialmente configurados, consulte la información específica sobre ["Cargando un certificado de cliente KMS"](#).

Antes de empezar

- Tiene permiso de acceso raíz.
- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Para configurar un certificado de cliente:
 - Tiene la dirección IP o el nombre de dominio del nodo de administrador.
 - Si configuró el certificado de interfaz de gestión StorageGRID, tiene la CA, el certificado de cliente y la clave privada utilizadas para configurar el certificado de interfaz de gestión.
 - Para cargar su propio certificado, la clave privada del certificado está disponible en su equipo local.
 - La clave privada debe haberse guardado o registrado en el momento de su creación. Si no tiene la clave privada original, debe crear una nueva.
- Para editar un certificado de cliente:
 - Tiene la dirección IP o el nombre de dominio del nodo de administrador.
 - Para cargar su propio certificado o un nuevo certificado, la clave privada, el certificado de cliente y la

CA (si se utiliza) están disponibles en su equipo local.

Añada certificados de cliente

Para agregar el certificado de cliente, use uno de estos procedimientos:

- [El certificado de interfaz de gestión ya está configurado](#)
- [CERTIFICADO de cliente emitido por CA](#)
- [Certificado generado desde Grid Manager](#)

El certificado de interfaz de gestión ya está configurado

Utilice este procedimiento para agregar un certificado de cliente si ya se ha configurado un certificado de interfaz de gestión mediante una CA proporcionada por el cliente, un certificado de cliente y una clave privada.

Pasos

1. En el Administrador de cuadrícula, seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
5. Seleccione **continuar**.
6. Para el paso **Adjuntar certificados**, cargue el certificado de la interfaz de administración.
 - a. Seleccione **cargar certificado**.
 - b. Seleccione **Examinar** y seleccione el archivo de certificado de la interfaz de gestión (.pem).
 - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.
 - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
 - c. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

7. [Configurar una herramienta de supervisión externa](#), Como Grafana.

CERTIFICADO de cliente emitido por CA

Utilice este procedimiento para agregar un certificado de cliente de administrador si no se ha configurado un certificado de interfaz de gestión y tiene previsto agregar un certificado de cliente para Prometheus que utilice un certificado de cliente emitido por CA y una clave privada.

Pasos

1. Realice los pasos a ["configure un certificado de interfaz de gestión"](#).
2. En el Administrador de cuadrícula, seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
3. Seleccione **Agregar**.

4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
6. Seleccione **continuar**.
7. Para el paso **Adjuntar certificados**, cargue el certificado de cliente, la clave privada y los archivos del paquete de CA:
 - a. Seleccione **cargar certificado**.
 - b. Seleccione **Examinar** y seleccione el certificado de cliente, la clave privada y los archivos del paquete de CA (.pem).
 - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.
 - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
 - c. Seleccione **Crear** para guardar el certificado en Grid Manager.

Los nuevos certificados aparecen en la ficha Cliente.

8. [Configurar una herramienta de supervisión externa](#), Como Grafana.

Certificado generado desde Grid Manager

Utilice este procedimiento para agregar un certificado de cliente de administrador si no se ha configurado un certificado de interfaz de gestión y planea agregar un certificado de cliente para Prometheus que utilice la función generar certificado en Grid Manager.

Pasos

1. En el Administrador de cuadrícula, seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
5. Seleccione **continuar**.
6. Para el paso **Adjuntar certificados**, selecciona **Generar certificado**.
7. Especifique la información del certificado:
 - **Tema** (opcional): X,509 Sujeto o nombre distinguido (DN) del titular del certificado.
 - **Días válidos**: El número de días que el certificado generado es válido, comenzando en el momento en que se genera.
 - **Agregar extensiones de uso de claves**: Si se selecciona (predeterminado y recomendado), el uso de claves y las extensiones de uso de claves extendidas se agregan al certificado generado.

Estas extensiones definen el propósito de la clave contenida en el certificado.



Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

8. Seleccione **generar**.

9. Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.



No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en una ubicación segura.

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
- Seleccione **Descargar certificado** para guardar el archivo de certificado.

Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar clave privada** para copiar la clave privada del certificado para pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como archivo.

Especifique el nombre del archivo de clave privada y la ubicación de descarga.

10. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

11. En el Administrador de cuadrícula, seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Global**.

12. Seleccione **Certificado de interfaz de administración**.

13. Seleccione **utilizar certificado personalizado**.

14. Cargue los archivos `certificate.pem` y `private_key.pem` desde el [detalles del certificado de cliente](#) paso. No es necesario cargar un paquete de CA.

- Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
- Cargar cada archivo de certificado (`.pem`).
- Seleccione **Guardar** para guardar el certificado en Grid Manager.

El nuevo certificado se muestra en la página del certificado de interfaz de gestión.

15. [Configurar una herramienta de supervisión externa](#), Como Grafana.

Configure una herramienta de monitorización externa

Pasos

1. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.

- Nombre:** Escriba un nombre para la conexión.

StorageGRID no requiere esta información, pero se debe proporcionar un nombre para probar la conexión.

- URL:** Introduzca el nombre de dominio o la dirección IP del nodo de administración. Especifique

HTTPS y el puerto 9091.

Por ejemplo: `https://admin-node.example.com:9091`

c. Activar **Licencia de cliente TLS y con CA Cert**.

d. En Detalles de autenticación TLS/SSL, copie y pegue:

- El certificado de CA de la interfaz de administración para **CA Cert**
- El certificado de cliente para **Cliente Cert**
- La clave privada de **clave de cliente**

e. **ServerName**: Introduzca el nombre de dominio del nodo Admin.

Servername debe coincidir con el nombre de dominio tal y como aparece en el certificado de la interfaz de gestión.

2. Guarde y pruebe el certificado y la clave privada que copió desde StorageGRID o un archivo local.

Ahora puede acceder a la métrica Prometheus desde StorageGRID con su herramienta de supervisión externa.

Para obtener información sobre las métricas, consulte la "[Instrucciones para supervisar StorageGRID](#)".

Editar certificados de cliente

Puede editar un certificado de cliente de administrador para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus, o cargar un nuevo certificado cuando el actual haya caducado.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de caducidad de los certificados y los permisos de acceso a Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará una alerta.

2. Seleccione el certificado que desea editar.

3. Seleccione **Editar** y, a continuación, seleccione **Editar nombre y permiso**

4. Introduzca un nombre de certificado.

5. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.

6. Seleccione **continuar** para guardar el certificado en Grid Manager.

El certificado actualizado se muestra en la ficha Cliente.

Adjunte un nuevo certificado de cliente

Puede cargar un nuevo certificado cuando el actual haya caducado.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de caducidad de los certificados y los permisos de acceso a Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y, a continuación, seleccione una opción de edición.

Cargue el certificado

Copie el texto del certificado que se va a pegar en otro lugar.

- a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
- b. Cargar el nombre del certificado de cliente (.pem).

Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.

- Seleccione **Descargar certificado** para guardar el archivo de certificado.

Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem.

Por ejemplo: storagegrid_certificate.pem

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
- c. Seleccione **Crear** para guardar el certificado en Grid Manager.

El certificado actualizado se muestra en la ficha Cliente.

Generar certificado

Genere el texto del certificado para pegarlo en otro lugar.

- a. Seleccione **generar certificado**.
- b. Especifique la información del certificado:

- **Tema** (opcional): X,509 Sujeto o nombre distinguido (DN) del titular del certificado.
- **Días válidos**: El número de días que el certificado generado es válido, comenzando en el momento en que se genera.
- **Agregar extensiones de uso de claves**: Si se selecciona (predeterminado y recomendado), el uso de claves y las extensiones de uso de claves extendidas se agregan al certificado generado.

Estas extensiones definen el propósito de la clave contenida en el certificado.



Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

- c. Seleccione **generar**.
- d. Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.



No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en una ubicación segura.

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en

otro lugar.

- Seleccione **Descargar certificado** para guardar el archivo de certificado.

Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar clave privada** para copiar la clave privada del certificado para pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como archivo.

Especifique el nombre del archivo de clave privada y la ubicación de descarga.

- e. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

Descargar o copiar certificados de cliente

Puede descargar o copiar un certificado de cliente para utilizarlo en otro lugar.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. Descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el archivo de certificado `.pem`.

- a. Seleccione **Descargar certificado**.
- b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado

Copie el texto del certificado que se va a pegar en otro lugar.

- a. Seleccione **Copiar certificado PEM**.
- b. Pegue el certificado copiado en un editor de texto.
- c. Guarde el archivo de texto con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

Quite certificados de cliente

Si ya no necesita un certificado de cliente de administrador, puede eliminarlo.

Pasos

1. Seleccione **Configuración > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea eliminar.
3. Seleccione **Eliminar** y, a continuación, confirme.



Para eliminar hasta 10 certificados, seleccione cada certificado que desee eliminar en la ficha Cliente y, a continuación, seleccione **acciones > Eliminar**.

Una vez que se elimine un certificado, los clientes que lo hayan usado deben especificar un nuevo certificado de cliente para acceder a la base de datos Prometheus de StorageGRID.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.