Configurar certificados de servidor

StorageGRID 11.8

NetApp
March 19, 2024

Tabla de contenidos

Configurar certificados de servidor

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 sea compatible con el certificado del servidor, puede hacerlo "vuelva temporalmente a la política de seguridad predeterminada".

Para obtener más información sobre cómo StorageGRID protege las conexiones de cliente, consulte "Seguridad para los clientes S3 y Swift".

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 interrumpan por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor para la interfaz de administración** se activa cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **certificados** y mirando la fecha de caducidad del certificado de interfaz de administración en la ficha 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 de certificado**: Archivo de clave privada de certificado de 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 personalizado se utiliza para todas las conexiones nuevas subsiguientes a Grid Manager, Tenant Manager, Grid Manager API o la API de Tenant 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 personalizado se utiliza para todas las conexiones nuevas subsiguientes a Grid Manager, Tenant Manager, Grid Manager API o la API de Tenant 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.

Restaure 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

- Ya tienes "permisos de acceso específicos".
- Usted tiene la `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 `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

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 Admin. Por ejemplo: `*.ui.storagegrid.example.com` utiliza el comodín * que se va a representar `admin1.ui.storagegrid.example.com` y.. `admin2.ui.storagegrid.example.com`.

- Configurado `--type` para `management` Para configurar el certificado de la interfaz de gestión, que utiliza el administrador de grid y el administrador de inquilinos.
- De forma predeterminada, los certificados generados son válidos durante un año (365 días) y deben volver a crearse antes de que expiren. Puede utilizar el `--days` argumento para anular el período de validez predeterminado.

> 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:
   a. Acceda a Grid Manager.
   b. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**
   c. 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 paquete de CA `.pem` archivo. 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 API S3 y Swift

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

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 CA de grid en el cliente API S3 o Swift que usará para acceder al sistema, según la entidad de certificación (CA) raíz que use.

Para garantizar que las operaciones no se interrumpan por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor global para S3 y Swift API** se activa cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **certificados** y mirando la fecha de caducidad del certificado API S3 y Swift en la ficha Global.

Puede cargar o generar un certificado API personalizado de S3 y Swift.

Añada un certificado API de S3 y Swift personalizado

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
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 de certificado**: Archivo de clave privada de certificado de 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 PEM de cada certificado API de S3 y Swift 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 usa para conexiones posteriores de clientes S3 y Swift.

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 de certificado** para mostrar los metadatos y PEM del certificado API de S3 y Swift 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 usa para conexiones posteriores de clientes S3 y Swift.

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 personalizado de S3 y Swift, la página de certificados de la API

de S3 y Swift muestra información detallada de los certificados API personalizados de S3 y Swift que está en uso.
Puede descargar o copiar el certificado PEM según sea necesario.

Restaure el certificado API S3 y Swift predeterminado

Puede revertir a utilizar el certificado de API S3 y Swift predeterminado para las conexiones de clientes S3 y Swift a los nodos de almacenamiento. Sin embargo, no puede usar el certificado de API S3 y Swift predeterminado para un extremo de balanceador de carga.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione **utilizar certificado predeterminado**.

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

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

   Si tiene permiso de acceso raíz y se utilizó el certificado de API Swift y S3 personalizado para conexiones de extremos de equilibrio de carga, se muestra una lista de extremos de equilibrio de carga que ya no se podrán acceder mediante el certificado API predeterminado S3 y Swift. 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 de la API S3 y Swift

Es posible guardar o copiar el contenido de los certificados API S3 y Swift para usarlos en otra parte.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
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 paquete de CA `.pem` archivo. 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"
- "Use la API DE REST de Swift"
- "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 un "navegador web compatible".
- Ya 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, a continuación, seleccione la ficha **CA** de cuadrícula.
2. En la sección **Certificado PEM**, descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el certificado `.pem` archivo.

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

- Ya tienes "permisos de acceso específicos".
- Ha iniciado sesión en Grid Manager mediante un "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 información más detallada 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.